Report: Homework 2 - Fondamenti di Comunicazioni ed Internet

Esercizio 1: Subnetting

L'obiettivo dell'esercizio è l'assegnazione di sottoreti contigue alle diverse sedi regionali, c vincolo di minimizzare lo spreco di indirizzi IP e prevenire la frammentazione dello spazio indirizzamento. Per ottenere questo risultato, è stato adottato il metodo VLSM (Variable Length Subnet Mask).

Come primo passo, le richieste delle sedi sono state riordinate in ordine decrescente (dalla sede con più host a quella con meno host). Questo approccio garantisce che i blocchi di indirizzi più grandi siano allocati per primi, permettendo ai blocchi successivi (più piccoli) di adattarsi perfettamente agli spazi di indirizzamento rimanenti contigui.

Per ogni sede, il calcolo della subnet mask è stato effettuato determinando la minima potenza di necessaria per contenere il numero di host richiesti più 2 indirizzi riservati (uno per l'indirizzo di rete e uno per il broadcast).

La formula utilizzata è:

$$Host_{richiesti} + 2 \leq 2^n$$

dove n rappresenta i bit dedicati agli host.

La maschera di sottorete (CIDR) si ottiene sottraendo questi bit alla lunghezza totale dell'indirizzo IPv4 (32 bit):

$$CIDR = /(32 - n)$$

Esempio: Per chiarire il procedimento applicato, riportiamo il calcolo dettagliato per la sede che richiede il maggior numero di host, la Puglia (8390 host richiesti). Essendo la prima sede in ordine di grandezza, le viene assegnato l'indirizzo base del blocco assegnato all'azienda 10.42.0.0.
Calcolo del numero di indirizzi IP: Servono almeno 8392 indirizzi. È necessario soddisfare la disuguaglianza $8390 + 2 \leq 2^n$. La potenza di 2 più vicina è $2^{14} = 16.384$, quindi questa sede occupa un blocco di 16.384 indirizzi e i bit dedicati all'host sono n = 14.
Maschera: / (32 - 14) = /18.

Una volta determinate le dimensioni dei blocchi, l'assegnazione degli indirizzi di rete segue una logica sequenziale rigorosa:

- Indirizzo di partenza:
  si stabilisce un IP di rete iniziale, nel nostro caso questo indirizzo IP è: 10.42.0.0/16.
- Sequenza:
  l'indirizzo di rete della regione successiva è calcolato sommando la dimensione del blocco della regione precedente al suo indirizzo di rete. Questo garantisce che non ci sian "buchi" di indirizzi inutilizzati tra una sottorete regionale e l'altra.

Dopo aver determinato l'indirizzo di rete (Network_Address) e la dimensione del blocco (Dimensione $\geq 2^n$), gli altri parametri della sottorete sono stati calcolati come segue:

- **Indirizzo di Broadcast**: Rappresenta l'ultimo indirizzo del blocco e si utilizza per comunicare con tutti gli host della sottorete. Si calcola sommando la dimensione del blocco all'indirizzo di rete e sottraendo 1:
  Broadcast = Network_Address + (Dimensione - 1)

- **Primo Indirizzo Host Utile**: È il primo indirizzo IP assegnabile a un dispositivo. Corrisponde all'indirizzo di rete più uno:
  Primo_Host = Network_Address + 1

- **Ultimo Indirizzo Host Utile**: È l'ultimo indirizzo assegnabile prima del broadcast. Corrisponde all'indirizzo di Broadcast meno uno:
  Ultimo_Host = Broadcast - 1

Esempio: Applicazione delle formule al caso della Puglia:
Indirizzo di Rete: 10.42.0.0
Indirizzo di Broadcast: 16.384 indirizzi corrispondono esattamente a 64 blocchi da 256 (ovvero 64 unità nel terzo ottetto), l'intervallo del terzo ottetto va da 0 a 63.
Broadcast = 10.42.(0 + 63).255 = 10.42.63.255
Primo Host Utile: *Rete + 1 = 10.42.0.1*
Ultimo Host Utile: *Broadcast - 1 = 10.42.63.254*

Di seguito viene mostrata la sequenza di assegnazione completa.

Nome sede	Numero host	Numero indirizzi IP nel blocco	Maschera	Primo - ultimo indirizzi host	Indirizzo di rete	Indirizzo di Broadcast
Puglia	8390	16384	/18	10.42.0.1 - 10.42.63.254	10.42.0.0	10.42.63.255
Marche	6727	8192	/19	10.42.64.1 - 10.42.95.254	10.42.64.0	10.42.95.255
Sicilia	4028	4096	/20	10.42.96.1 - 10.42.111.254	10.42.96.0	10.42.111.255
Calabria	3329	4096	/20	10.42.112.1 - 10.42.127.254	10.42.112.0	10.42.127.255
Veneto	1667	2048	/21	10.42.128.1 - 10.42.135.254	10.42.128.0	10.42.135.255
Sardegna	953	1024	/22	10.42.136.1 - 10.42.139.254	10.42.136.0	10.42.139.255
Toscana	700	1024	/22	10.42.140.1 - 10.42.143.254	10.42.140.0	10.42.143.255
Liguria	448	512	/23	10.42.144.1 - 10.42.145.254	10.42.144.0	10.42.145.255
Campania	98	128	/25	10.42.146.1 - 10.42.146.126	10.42.146.0	10.42.146.127

Per i collegamenti tra router P2P la logica di assegnazione cambia da quella delle sedi regionali poiché il requisito di indirizzi è fisso e minimo. Non è necessario applicare l'ordinamento dimensione, in quanto tutti i link hanno la stessa grandezza.

1. Analisi del Fabbisogno e Maschera:
ogni collegamento P2P richiede esattamente 2 indirizzi IP utilizzabili (uno per ciascuna interfaccia dei router ai capi del collegamento). A questi vanno aggiunti l'indirizzo di rete e l'indirizz broadcast, (*Totale_IP = 2(host) + 2 (rete/broadcast)*), portando il fabbisogno totale a 4 indirizzi per ciascun link:

- Dimensione del blocco: poiché il totale degli indirizzi richiesti è 4, si avrà $2^n = 4$ n = 2. Sono quindi necessari 2 bit dedicati alla parte host.
- Maschera: $/(32 - 2) = /30$.

2. Regole di indirizzamento
All'interno di ogni sottorete /30, l'assegnazione degli IP alle interfacce segue una convenz basata sull'identificativo numerico del router (es. R1 < R2):

- Indirizzo di Rete: primo indirizzo del blocco (Base).
- Primo Host Utile (Router Minore): assegnato al router con l'ID più basso. $IP_{min} = Rete + 1$
- Secondo Host Utile (Router Maggiore): assegnato al router con l'Id più alto. $IP_{max} = Rete + 2$
- Indirizzo di Broadcast: Ultimo indirizzo del blocco. $Broadcast = Rete + 3$

Applicazione pratica per il primo Link (R1-R2)
Le sottoreti P2P sono state allocate in modo contiguo immediatamente dopo l'ultimo indirizzo di broadcast utilizzato dalle sedi regionali.
L'ultima sede che nel nostro caso è la Campania termina con l'indirizzo di broadcast 10.42.146.127. Di conseguenza, lo spazio per i link P2P inizia dall'indirizzo successivo: 10.42.146.128.

Esempio: Consideriamo il primo link della lista, R1-R2:
Indirizzo di Rete: 10.42.146.128
Router R1 (ID più basso): Riceve il primo indirizzo utile, 10.42.146.128 + 1 = 10.42.146.129
Router R2 (ID più alto): Riceve il secondo indirizzo utile, 10.42.146.128 + 2 = 10.42.146.130
Indirizzo di Broadcast: 10.42.146.128 + 3 = 10.42.146.131

I link successivi (R1-R3, R2-R4, ecc.) seguono sequenzialmente incrementando l'indirizzo di rete di 4 unità alla volta.

Di seguito la tabella riassuntiva delle assegnazioni.

Link	IP router minore	IP router maggiore	Subnet assegnata
R1 - R2	10.42.146.129 (R1)	10.42.146.130 (R2)	10.42.146.128/30
R1 - R3	10.42.146.133 (R1)	10.42.146.134 (R3)	10.42.146.132/30
R2 - R4	10.42.146.137 (R2)	10.42.146.138 (R4)	10.42.146.136/30
R3 - R5	10.42.146.141 (R3)	10.42.146.142 (R5)	10.42.146.140/30
R4 - R6	10.42.146.145 (R4)	10.42.146.146 (R6)	10.42.146.144/30

R5 - R7	10.42.146.149 (R5)	10.42.146.150 (R7)	10.42.146.148/30
R6 - R7	10.42.146.153 (R6)	10.42.146.154 (R7)	10.42.146.152/30
R6 - R11	10.42.146.157 (R6)	10.42.146.158 (R11)	10.42.146.156/30
R7 - R9	10.42.146.161 (R7)	10.42.146.162 (R9)	10.42.146.160/30
R8 - R9	10.42.146.165 (R8)	10.42.146.166 (R9)	10.42.146.164/30
R8 - R10	10.42.146.169 (R8)	10.42.146.170 (R10)	10.42.146.168/30
R10 - R11	10.42.146.173 (R10)	10.42.146.174 (R11)	10.42.146.172/30

Esercizio 2: Routing Statico

L'obiettivo dell'esercizio è la configurazione dell'architettura di rete simulata in ambiente Kathará implementando un piano di routing statico in grado di garantire la connettività end-to-end tra tutt le sedi regionali e l'accesso alla rete Internet pubblica tramite il router di confine R1.

1. Architettura di Routing

L'architettura di routing è stata implementata manualmente utilizzando rotte statiche per soddisfare vincoli rigorosi di direzionalità del traffico.

La rete è divisa in due macro-aree:

Anello NORD: Configurato per instradare il traffico in senso orario

(R1 → R3 → R5 → R7 → R6 → R4 → R2 → R1).

Anello SUD: Configurato per instradare il traffico in senso antiorario

(R6 → R11 → R10 → R8 → R9 → R7 → R6)

Il router R6 rappresenta lo snodo cruciale della topologia, fungendo da gateway tra i due anelli.

2. Analisi e Valutazione sull'uso del Supernetting

Dall'analisi del piano di indirizzamento, emerge che non è possibile applicare un supernetting efficiente.

Motivazione:

L'assegnazione degli indirizzi è avvenuta per dimensione del blocco (VLSM) e non per posizione geografica. Di conseguenza, le subnet appartenenti all'anello Nord (es. Veneto, Liguria) e quelle dell'anello Sud (es. Puglia, Calabria) hanno indirizzi numerici intercalati e non separabili in due macro-blocchi distinti.

Conseguenza:

Aggregare le rotte causerebbe errori di instradamento per le sedi del Sud incluse in quel range. Pertanto, su R6 sono state configurate rotte statiche puntuali per le singole destinazioni (o piccoli gruppi contigui dove possibile).

3. Configurazione NAT per Accesso Internet

Per consentire l'accesso alla rete pubblica tramite l'ISP connesso a R1, è stata configurata una regola di Source NAT. Poiché l'intera rete utilizza indirizzi privati, R1 traduce gli indirizzi sorgente dei pacchetti in uscita sull'interfaccia eth2 con il proprio indirizzo pubblico.

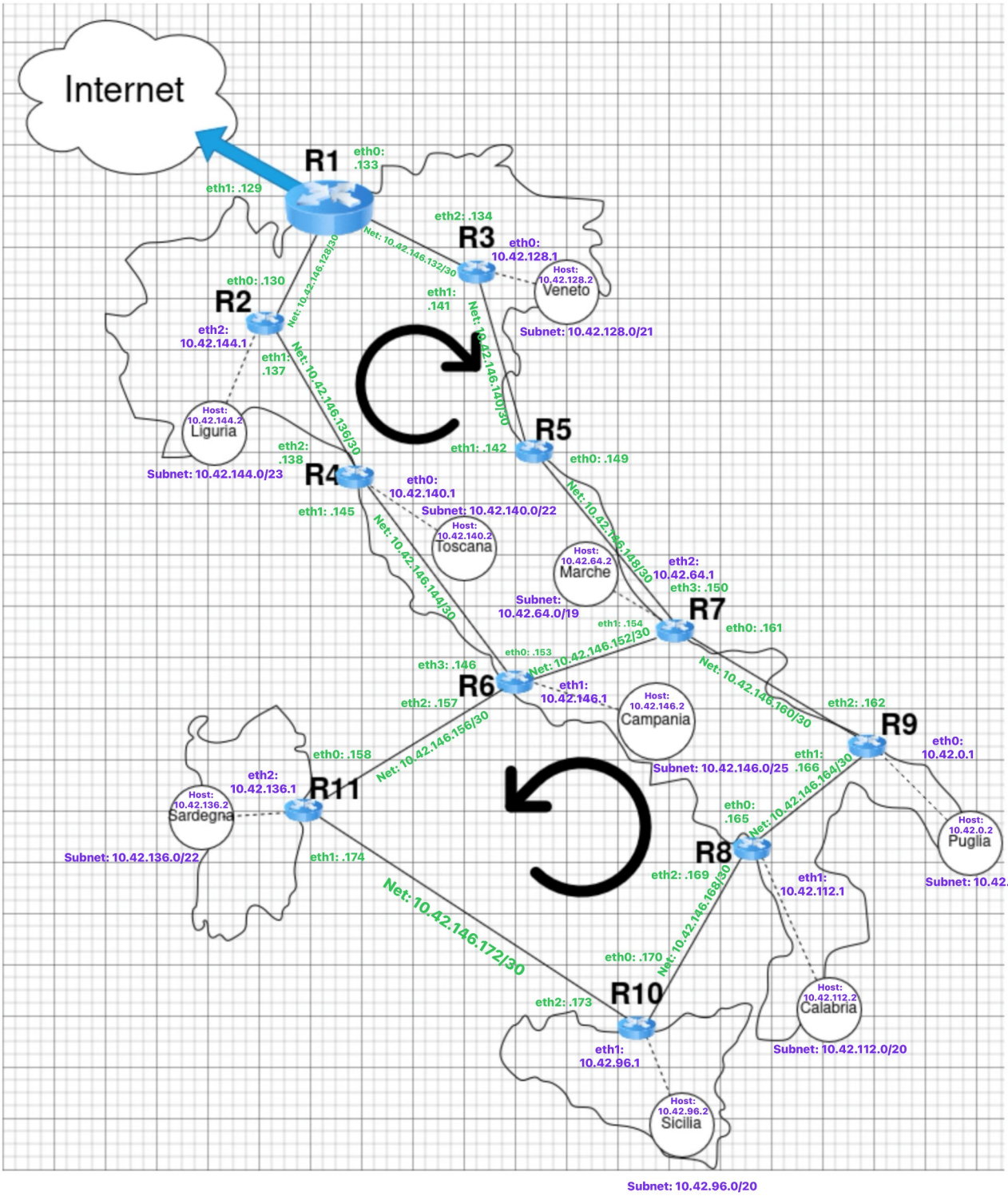
Comando implementato nel file r1.startup:

```
iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE
```

4. Configurazione dei Nodi e Topologia

Di seguito si riportano le evidenze grafiche e logiche della corretta implementazione. Mappa della Rete e Indirizzamento

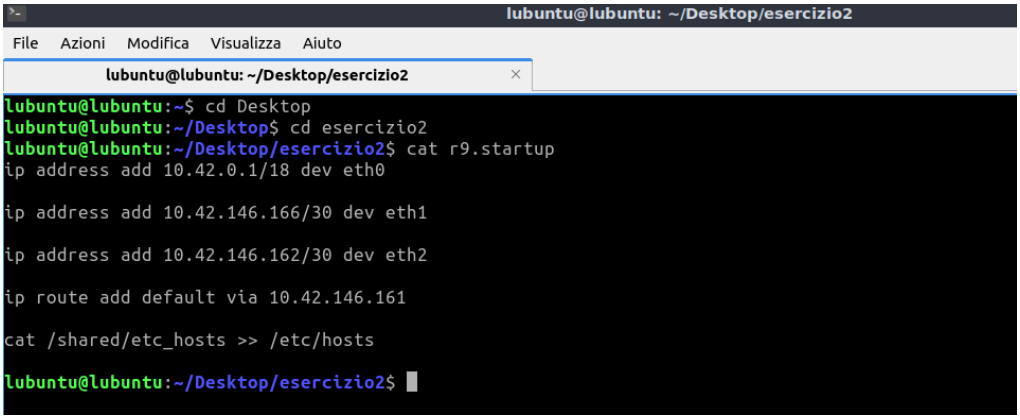
Topologia di rete iniziale e piano di indirizzamento



In viola sono indicati i nodi e le subnet assegnate alle sedi regionali; in verde sono riportati i collegamenti P2P tra i router con le relative interfacce.

Il diagramma mostra i due anelli. Le interfacce dei router sono state configurate coerentemente con la tabella VLSM. Ogni router possiede un'interfaccia simulata che rappresenta la LAN regionale, e interfacce seriali per i link P2P.

Esempio: Riprendendo come esempio la regione Puglia, si riporta il procedimentodi compilazione del file.startup di R9 (Router connesso alla Puglia).



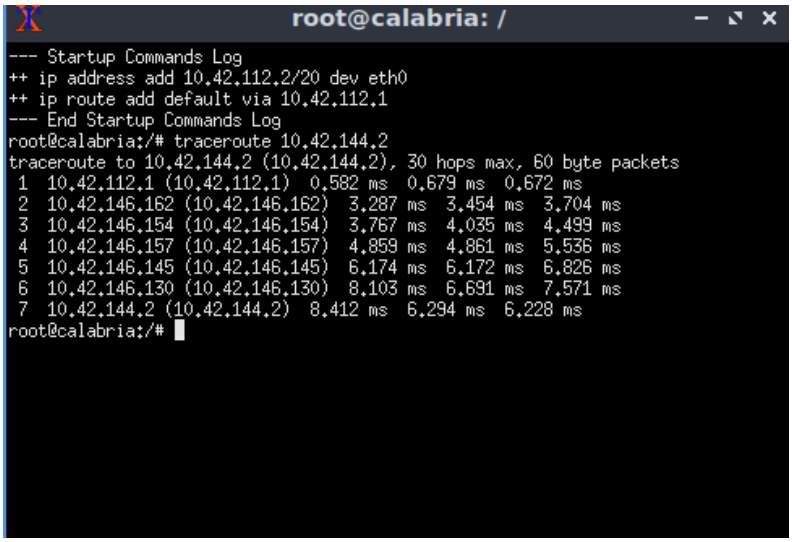
Dove vengono aggiunti sia l'indirizzo IP di R9 nel collegamento con la regione direttamen connessa al router, sia gli indirizzi IP con cui R9 si connette ai router (R8 e R7) tramite i rispettivi link. Inoltre viene aggiunto un IP di default (R7 per il senso antiorario) al quale R9 trasm informazioni.

5. Verifica della Connettività

Per verificare il rispetto delle regole di direzionalità (Nord Orario / Sud Antiorario), è stato eseguit un test di tracciamento pacchetti.

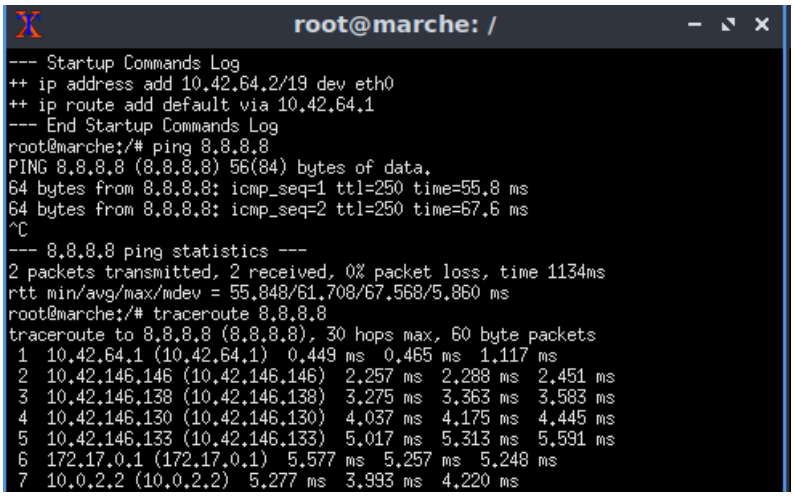
Scenario di Test:

A) Host in Calabria (Sud) → Host in Liguria (Nord)



Come evidenziatodal comando traceroutelanciato dalla sede Calabria verso la Liguria (10.42.144.2), il pacchetto attraversa l'anello Sud in senso antiorario (passando per R8, R9, R7, R6) fino al router ponte R6, per poi percorrere l'anello Nord in senso orario (R6, R4, R2) come richiesto dalle specifiche.

B) Host in Marche (Nord/Sud) → Internet (8.8.8.8)



Nello scenario Marche (Anello Nord) verso Internet, si osserva il rispetto del vincolo orario pacchetto, invece di percorrere la tratta breve verso R1 (senso antiorario), viene instradato lungo l'intero anello (R6, R4, R2) fino a giungere al gateway R1. L'ultimo hop verso l'IP pubblico 8.8.8.8 conferma inoltre il corretto funzionamento della regola di Source NAT su R1, permettendo l'uscita verso la rete esterna.

6. Tabelle di Routing Statico

Di seguito si riportano le tabelle di routing statico implementate sui nodi rappresentativi, fondamentali per garantire la logica descritta.

Router	Interfaccia e indirizzo	# Static route	Subnet destinazione	Gateway	Interfaccia
R1	Eth0: 10.42.146.133/30 Eth1: 10.42.146.129/30	1 2 3 4 5 6 7 8 9 10	10.42.128.0/21 10.42.64.0/19 10.42.146.0/25 10.42.140.0/22 10.42.144.0/23 10.42.136.0/22 10.42.112.0/20 10.42.96.0/20 10.42.0.0/18 Default	10.42.146.134 10.42.146.134 10.42.146.134 10.42.146.134 10.42.146.134 10.42.146.134 10.42.146.134 10.42.146.134 10.42.146.134 Connessa	Eth0 Eth0 Eth0 Eth0 Eth0 Eth0 Eth0 Eth0 Eth0 Eth2
R2	Eth0: 10.42.146.130/30 Eth1: 10.42.146.137/30 Eth2: 10.42.144.1/23	1 2 3 4 5 6 7 8 9 10	10.42.128.0/21 10.42.64.0/19 10.42.146.0/25 10.42.140.0/22 10.42.144.0/23 10.42.136.0/22 10.42.112.0/20 10.42.96.0/20 10.42.0.0/18 Default	10.42.146.129 10.42.146.129 10.42.146.129 10.42.146.129 Connessa 10.42.146.129 10.42.146.129 10.42.146.129 10.42.146.129 10.42.146.129	Eth0 Eth0 Eth0 Eth0 Eth2 Eth0 Eth0 Eth0 Eth0 Eth0

Router	Interfaccia e indirizzo	# Static route	Subnet destinazione	Gateway	Interfaccia
R3	Eth0: 10.42.128.1/21	1	10.42.128.0/21	Connessa	Eth0
	Eth1: 10.42.146.141/30	2	10.42.64.0/19	10.42.146.142	Eth1
	Eth2: 10.42.146.134/30	3	10.42.146.0/25	10.42.146.142	Eth1
		4	10.42.140.0/22	10.42.146.142	Eth1
		5	10.42.144.0/23	10.42.146.142	Eth1
		6	10.42.136.0/22	10.42.146.142	Eth1
		7	10.42.112.0/20	10.42.146.142	Eth1
		8	10.42.96.0/20	10.42.146.142	Eth1
		9	10.42.0.0/18	10.42.146.142	Eth1
		10	Default	10.42.146.142	Eth1
R4	Eth0: 10.42.140.1/22	1	10.42.128.0/21	10.42.146.137	Eth2
	Eth1: 10.42.146.145/30	2	10.42.64.0/19	10.42.146.137	Eth2
	Eth2: 10.42.146.138/30	3	10.42.146.0/25	10.42.146.137	Eth2
		4	10.42.140.0/22	Connessa	Eth0
		5	10.42.144.0/23	10.42.146.137	Eth2
		6	10.42.136.0/22	10.42.146.137	Eth2
		7	10.42.112.0/20	10.42.146.137	Eth2
		8	10.42.96.0/20	10.42.146.137	Eth2
		9	10.42.0.0/18	10.42.146.137	Eth2
		10	Default	10.42.146.137	Eth2
R5	Eth0: 10.42.146.149/30	1	10.42.128.0/21	10.42.146.150	Eth0
	Eth1: 10.42.146.142/30	2	10.42.64.0/19	10.42.146.150	Eth0
		3	10.42.146.0/25	10.42.146.150	Eth0
		4	10.42.140.0/22	10.42.146.150	Eth0
		5	10.42.144.0/23	10.42.146.150	Eth0
		6	10.42.136.0/22	10.42.146.150	Eth0
		7	10.42.112.0/20	10.42.146.150	Eth0
		8	10.42.96.0/20	10.42.146.150	Eth0
		9	10.42.0.0/18	10.42.146.150	Eth0
		10	Default	10.42.146.150	Eth0
R6	Eth0: 10.42.146.153/30	1	10.42.128.0/21	10.42.146.145	Eth3
	Eth1: 10.42.146.1/25	2	10.42.64.0/19	10.42.146.158	Eth2
	Eth2: 10.42.146.157/30	3	10.42.146.0/25	Connessa	Eth1
	Eth3: 10.42.146.146/30	4	10.42.140.0/22	10.42.146.145	Eth3
		5	10.42.144.0/23	10.42.146.145	Eth3
		6	10.42.136.0/22	10.42.146.158	Eth2
		7	10.42.112.0/20	10.42.146.158	Eth2
		8	10.42.96.0/20	10.42.146.158	Eth2
		9	10.42.0.0/18	10.42.146.158	Eth2
		10	Default	10.42.146.145	Eth3
R7	Eth0: 10.42.146.161/30	1	10.42.128.0/21	10.42.146.153	Eth1
	Eth1: 10.42.146.154/30	2	10.42.64.0/19	Connessa	Eth2
	Eth2: 10.42.64.1/19	3	10.42.146.0/25	10.42.146.153	Eth1
	Eth3: 10.42.146.150/30	4	10.42.140.0/22	10.42.146.153	Eth1
		5	10.42.144.0/23	10.42.146.153	Eth1
		6	10.42.136.0/22	10.42.146.153	Eth1
		7	10.42.112.0/20	10.42.146.153	Eth1
		8	10.42.96.0/20	10.42.146.153	Eth1
		9	10.42.0.0/18	10.42.146.153	Eth1
		10	Default	10.42.146.153	Eth1

Router	Interfaccia e indirizzo	# Static route	Subnet destinazione	Gateway	Interfaccia
R8	Eth0: 10.42.146.165/30 Eth1: 10.42.112.1/20 Eth2: 10.42.146.169/30	1 2 3 4 5 6 7 8 9 10	10.42.128.0/21 10.42.64.0/19 10.42.146.0/25 10.42.140.0/22 10.42.144.0/23 10.42.136.0/22 10.42.112.0/20 10.42.96.0/20 10.42.0.0/18 Default	10.42.146.166 10.42.146.166 10.42.146.166 10.42.146.166 10.42.146.166 10.42.146.166 Connessa 10.42.146.166 10.42.146.166 10.42.146.166	Eth0 Eth0 Eth0 Eth0 Eth0 Eth0 Eth1 Eth0 Eth0 Eth0
R9	Eth0: 10.42.0.1/18 Eth1: 10.42.146.166/30 Eth2: 10.42.146.162/30	1 2 3 4 5 6 7 8 9 10	10.42.128.0/21 10.42.64.0/19 10.42.146.0/25 10.42.140.0/22 10.42.144.0/23 10.42.136.0/22 10.42.112.0/20 10.42.96.0/20 10.42.0.0/18 Default	10.42.146.161 10.42.146.161 10.42.146.161 10.42.146.161 10.42.146.161 10.42.146.161 10.42.146.161 10.42.146.161 Connessa 10.42.146.161	Eth2 Eth2 Eth2 Eth2 Eth2 Eth2 Eth2 Eth2 Eth0 Eth2
R10	Eth0: 10.42.146.170/30 Eth1: 10.42.96.1/20 Eth2: 10.42.146.173/30	1 2 3 4 5 6 7 8 9 10	10.42.128.0/21 10.42.64.0/19 10.42.146.0/25 10.42.140.0/22 10.42.144.0/23 10.42.136.0/22 10.42.112.0/20 10.42.96.0/20 10.42.0.0/18 Default	10.42.146.169 10.42.146.169 10.42.146.169 10.42.146.169 10.42.146.169 10.42.146.169 10.42.146.169 Connessa 10.42.146.169 10.42.146.169	Eth0 Eth0 Eth0 Eth0 Eth0 Eth0 Eth0 Eth1 Eth0 Eth0
R11	Eth0: 10.42.146.158/30 Eth1: 10.42.146.174/30 Eth2: 10.42.136.1/22	1 2 3 4 5 6 7 8 9 10	10.42.128.0/21 10.42.64.0/19 10.42.146.0/25 10.42.140.0/22 10.42.144.0/23 10.42.136.0/22 10.42.112.0/20 10.42.96.0/20 10.42.0.0/18 Default	10.42.146.173 10.42.146.173 10.42.146.173 10.42.146.173 10.42.146.173 Connessa 10.42.146.173 10.42.146.173 10.42.146.173 10.42.146.173	Eth1 Eth1 Eth1 Eth1 Eth1 Eth2 Eth1 Eth1 Eth1 Eth1

Si nota che R6 ha rotte specifiche per ogni destinazione proprio perché funge da smistat centrale e non può aggregare (questo dimostra che non è possibile usare il supernetting).

Esercizio 3: Connettività Internet

L'obiettivo dell'esercizioè la gestione di uno scenario di guasto critico che ha causato l'isolamento parziale della sede Sicilia (R10), interrompendone il collegamento diretto con dorsale continentale (R8), rimanendo connesso fisicamente solo al router R11 (Sardegna).

1. Diagnosi del Guasto: Isolamento di R10

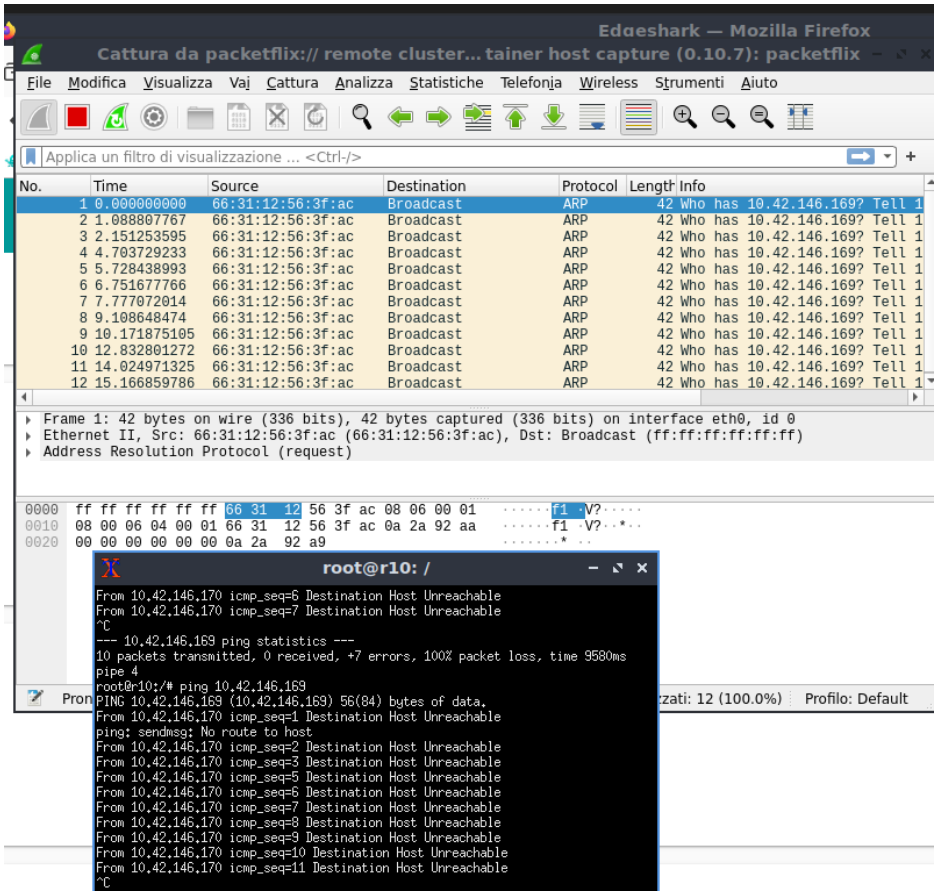
Analisi tramite Edgeshark:

Per diagnosticare il punto esatto del guasto, si è analizzato il traffico sull'interfaccia di R1 connessa verso R8. Come richiesto, il guasto è stato simulato ponendo le interfacce in domini di collisione differenti.

Tentando un ping da R10 verso l'interfaccia di R8 (IP 10.42.146.169), si è osservato il seguente comportamento:

1. Il ping restituisce "Destination Host Unreachable". Questo indica che R10 possiede una rotta per la destinazione (sa che è sulla sua stessa sottorete), ma non riesce a contattare il vicino a livello 2.
2. L'analisi con edgeshark mostra continue richieste ARP (Address Resolution Protocol) di tipo "Who has 10.42.146.169? Tell 10.42.146.170".
3. Non arrivano mai risposte ARP (ARP Reply).

Questo conferma che il collegamento logico è attivo (IP configurato), ma il collegamento fisico/ livello 2 è interrotto (i pacchetti non raggiungono l'altro capo).



Analisi edgeshark su R10: si notano le richieste ARP senza risposta verso R8 e l'errore "H Unreachable".

2. Risoluzione: Nuovo Link R6-R8

Per ripristinare la piena connettività garantendo al contempo la ridondanza dell'infrastruttu creando un nuovo anello sud, è stato istituito un nuovo collegamento P2P tra R6 (Campania) e R8 (Calabria).

Modifiche alla Topologia:

- Link Guasto: R10 - R8 (isolato).
- Nuovo Link: R6 - R8.
- Indirizzamento IP: È stata assegnata la prima subnet /30 libera disponibile (seguendo la logica sequenziale dell'Esercizio 1) al nuovo collegamento R6-R8.

Esempio: Subnet 10.42.146.176/30.
R6 interfaccia nuova: .177
R8 interfaccia nuova: .178

Questa operazione ha permesso di ricreare l'anello Sud, fornendo un percorso alternativo per il traffico, permettendo al traffico di fluire nonostante l'interruzione in Sicilia.

3. Aggiornamento del Routing (Rotte Statiche)

L'obiettivo è ripristinare la connettività alterando il meno possibile la direzione del traffico (senso antiorario per l'anello sud). Tuttavia, essendo R10 ora un nodo "stub" (terminale) dietro R flusso per la Sicilia deve necessariamente cambiare.

Strategia di Instradamento:

1. R10 (Sicilia): Non può più inviare traffico a R8. La sua rotta di default (o verso il resto della ret deve puntare a R11.
2. R11 (Sardegna): Riceve il traffico da R10 e lo instrada verso R6.
3. R6 (Campania): Diventa il punto di snodo. Instrada verso R11 il traffico diretto a R10/R11, e usa il nuovo link verso R8 per mantenere il flusso antiorario verso la Puglia (R8 -> R9 -> R7), se necessario, oppure usa R8 come backup.

Di seguito le tabelle di routing aggiornate per i nodi critici.

Router	Interfaccia e indirizzo	# Static route	Subnet destinazione	Gateway	Interfaccia
R6	Eth0: 10.42.146.153/30	1	10.42.128.0/21	10.42.146.145	Eth4
	Eth1: 10.42.146.1/25	2	10.42.64.0/19	10.42.146.158	Eth2
	Eth2: 10.42.146.177/30	3	10.42.146.0/25	Connessa	Eth1
	Eth3: 10.42.146.157/30	4	10.42.140.0/22	10.42.146.145	Eth4
	Eth4: 10.42.146.146/30	5	10.42.144.0/23	10.42.146.145	Eth4
		6	10.42.136.0/22	10.42.146.158	Eth3
		7	10.42.112.0/20	10.42.146.178	Eth2
		8	10.42.96.0/20	10.42.146.158	Eth3
		9	10.42.0.0/18	10.42.146.178	Eth2
		10	Default	10.42.146.145	Eth4
R8	Eth0: 10.42.146.165/30	1	10.42.128.0/21	10.42.146.166	Eth0
	Eth1: 10.42.112.1/20	2	10.42.64.0/19	10.42.146.166	Eth0
	Eth2: 10.42.146.169/30	3	10.42.146.0/25	10.42.146.166	Eth0
	Eth3: 10.42.146.178/30	4	10.42.140.0/22	10.42.146.166	Eth0
		5	10.42.144.0/23	10.42.146.166	Eth0
		6	10.42.136.0/22	10.42.146.166	Eth0
		7	10.42.112.0/20	Connessa	Eth1
		8	10.42.96.0/20	10.42.146.166	Eth0
		9	10.42.0.0/18	10.42.146.166	Eth0
		10	Default	10.42.146.166	Eth0
R10	Eth1: 10.42.96.1/20	1	10.42.128.0/21	10.42.146.174	Eth2
	Eth2: 10.42.146.173/30	2	10.42.64.0/19	10.42.146.174	Eth2
		3	10.42.146.0/25	10.42.146.174	Eth2
		4	10.42.140.0/22	10.42.146.174	Eth2
		5	10.42.144.0/23	10.42.146.174	Eth2
		6	10.42.136.0/22	10.42.146.174	Eth2
		7	10.42.112.0/20	10.42.146.174	Eth2
		8	10.42.96.0/20	Connessa	Eth1
		9	10.42.0.0/18	10.42.146.174	Eth2
		10	Default	10.42.146.174	Eth2

Router	Interfaccia e indirizzo	# Static route	Subnet destinazione	Gateway	Interfaccia
R11	Eth0: 10.42.146.158/30 Eth1: 10.42.146.174/30 Eth2: 10.42.136.1/22	1 2 3 4 5 6 7 8 9 10	10.42.128.0/21 10.42.64.0/19 10.42.146.0/25 10.42.140.0/22 10.42.144.0/23 10.42.136.0/22 10.42.112.0/20 10.42.96.0/20 10.42.0.0/18 Default	10.42.146.157 10.42.146.157 10.42.146.157 10.42.146.157 10.42.146.157 Connessa 10.42.146.157 10.42.146.173 10.42.146.157 10.42.146.157	Eth0 Eth0 Eth0 Eth0 Eth0 Eth2 Eth0 Eth1 Eth0 Eth0

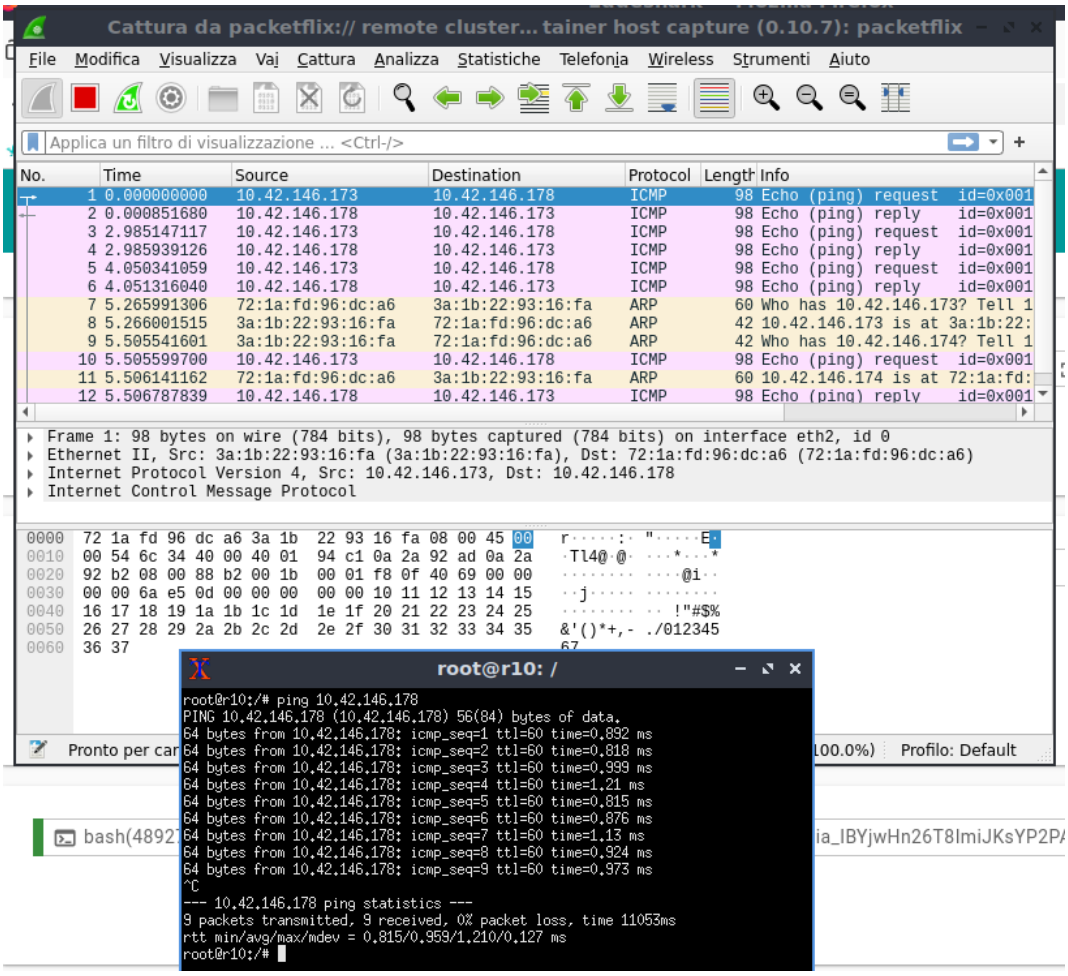
4. Verifica della Connettività

Dopo aver configurato il nuovo link e aggiornato le tabelle di routing, si è verificata la connettività

Test Effettuato:
Ping da R10 verso un indirizzo remoto.

Come mostrato nello screenshot sottostante, il ping ha successo.

- Il TTL = 60 suggerisce che il pacchetto ha attraversato vari hop, confermando che il routing è stato corretto e R10 non è più isolato.

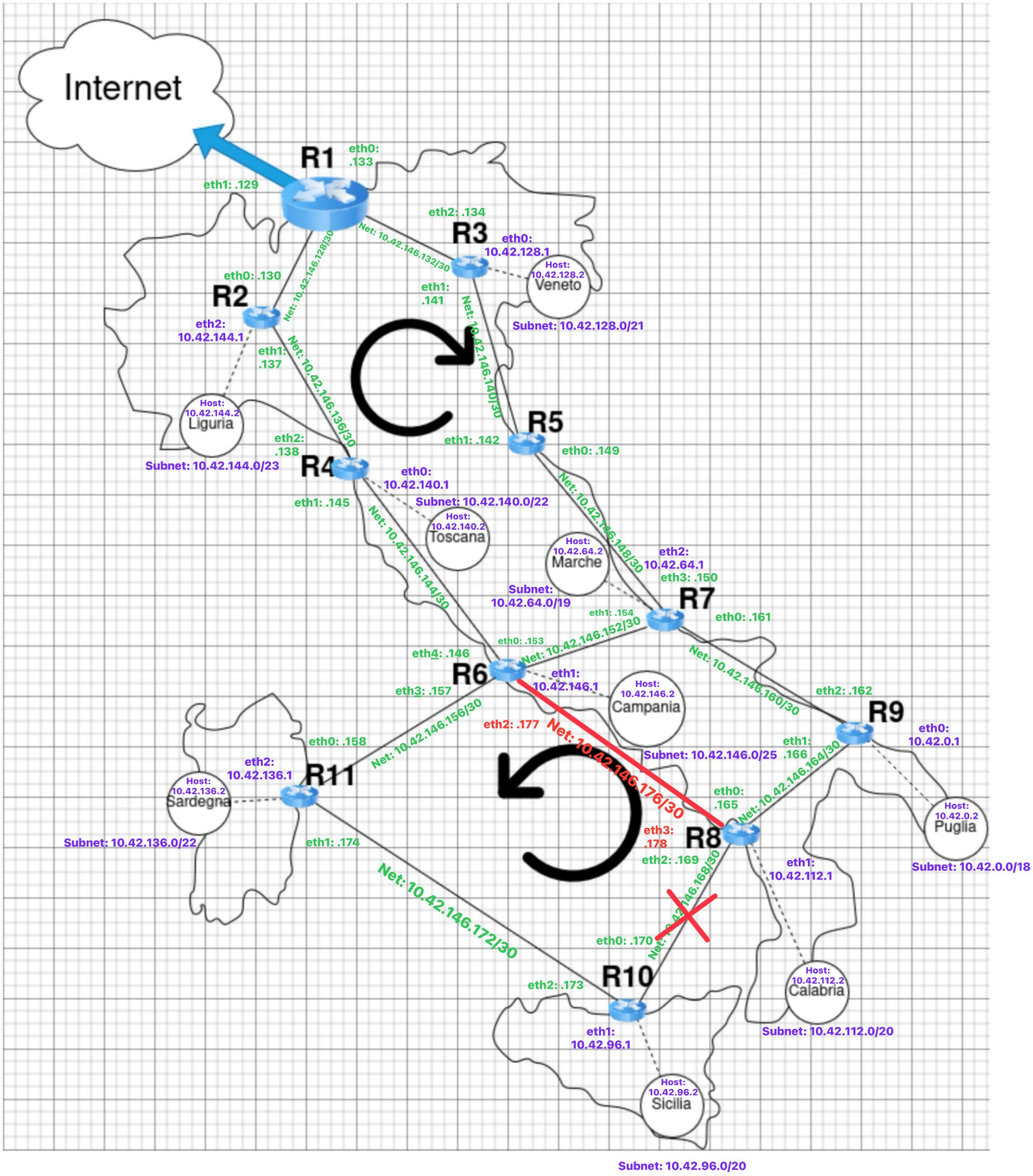


Verifica connettività:
R10 riesce a pingare correttamente attraverso la rete ripristinata. Le statistiche mostrano packet loss.

Conclusione

Il guasto sul link R10-R8 è stato aggirato con successo tramite l'implementazione del nuo collegamento R6-R8 e la modifica delle rotte statiche su R10 e R11, forzando il traffico siciliano a risalire attraverso la Sardegna (R11) verso il continente (R6).

Riconfigurazione della rete a seguito del guasto



Una X rossa evidenzia l'interruzione del collegamento R8-R10 e mostra il nuovo link di ripristino attivato direttamente tra R6 ed R8 per garantire la continuità del servizio.

Esercizio 4: Traffico Anomalo

L'obiettivo dell'esercizio è isolare il traffico diretto verso un server specifico situato nella s
Puglia, identificato come bersaglio di traffico anomalo. Per scopi di analisi e sicurezza, si richiede
che solo i pacchetti diretti a questo server vengano instradati obbligatoriamente attraverso
router di confine R1, mentre il resto del traffico per la regione Puglia deve continuare a seguire i
percorsi standard definiti in precedenza.

1. Configurazione del Server e Topologia

Come richiesto, è stato identificato un indirizzo IP situato al centro del blocco assegnato
Puglia (10.42.0.0/18) per rappresentare il server compromesso.

• Subnet Puglia: 10.42.0.0/18 (Range: 10.42.0.1 - 10.42.63.254)
• IP Server Selezionato (Target): 10.42.32.0 (Centro matematico del range).

È stato creato un nuovo nodo server e stabilito un collegamento P2P diretto ed esclusivo con R1.
Per questo collegamento è stata utilizzata la prima subnet /30 disponibile, successiva a q
utilizzate nell'Esercizio 3.

Dettagli Nuovo Link (R1 - Server):

- Subnet: 10.42.146.180/30
- R1 (eth2): 10.42.146.181
- Server (eth0): 10.42.146.182
- Interfaccia Loopback Server: 10.42.32.0/32 (L'IP target da raggiungere).

2. Strategia di Routing: Longest Prefix Matching

Per ottenere la deviazione selettiva del traffico, è stato sfruttato il principio del Longest P
Matching (LPM). I router, quando devono decidere dove inoltrare un pacchetto, confrontan
l'indirizzo di destinazione con le voci nella tabella di routing e scelgono quella con la maschera di
sottorete più lunga, ovvero quella con il maggior numero di bit corrispondenti.

Nella configurazione si è introdotta una "collisione deliberata" nelle tabelle di routing:

1. Rotta Generale (Puglia): Esiste una rotta per 10.42.0.0/18 che punta verso l'anello Sud
   (percorso standard).
2. Rotta Specifica (Server): È stata aggiunta una rotta per 10.42.32.0/32 che punta verso R1.

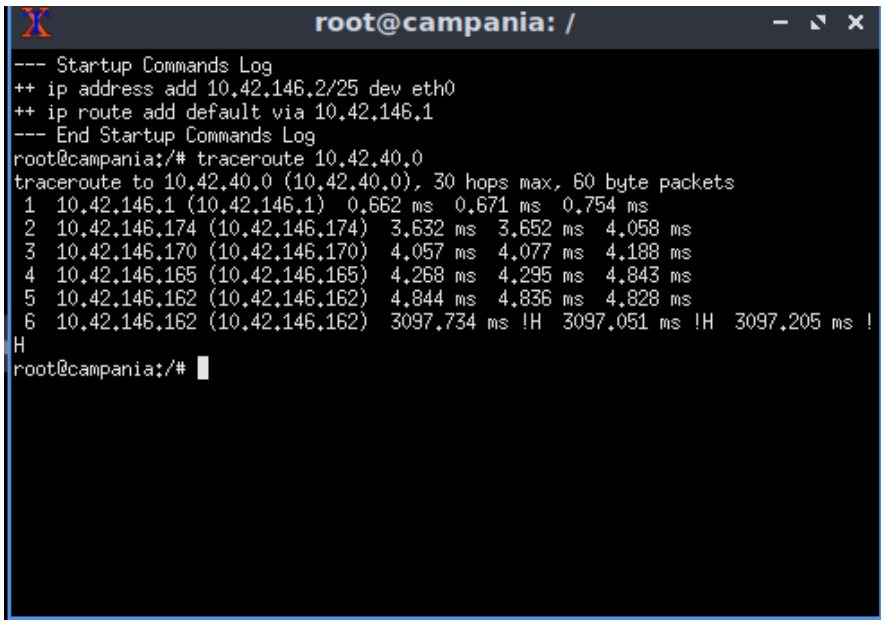
Poiché /32 è più specifico di /18, qualsiasi pacchetto diretto al server (10.42.32.0) userà la rotta
verso R1. Qualsiasi altro pacchetto per la Puglia (es. 10.42.40.1) non corrisponderà alla /3
userà la /18.
Per garantire che il traffico venga dirottato verso R1 da qualsiasi punto della rete, è stata aggiunt
la rotta specifica /32 sui router di transito.

3. Analisi del Traffico e Verifica

Per dimostrare l'efficacia della soluzione, sono stati eseguiti due traceroute comparativi.

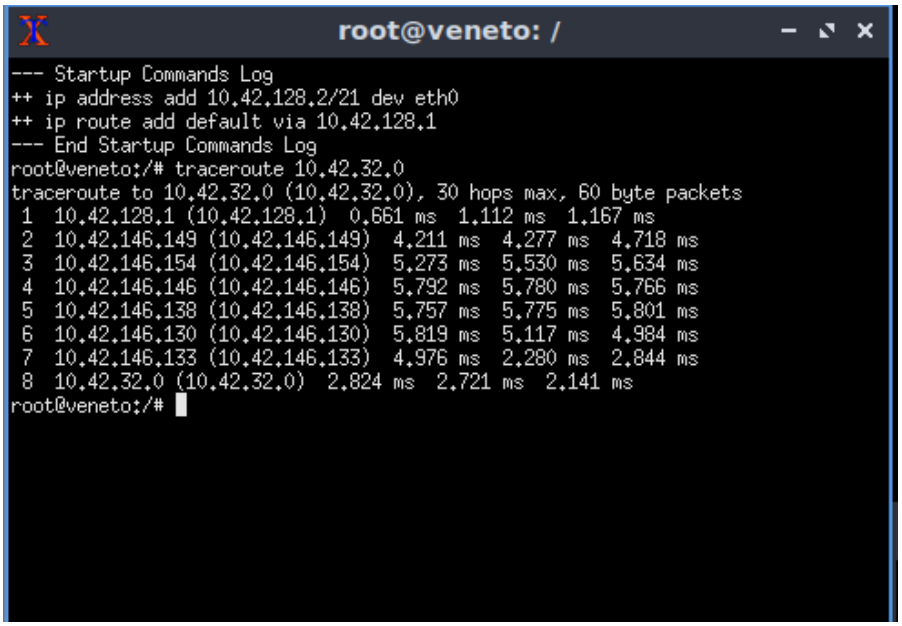
Caso A: Traffico Normale (Campania → Puglia Generica)
È stato inviato traffico dalla Campania verso un IP casuale della Puglia (10.42.40.0), diverso dall'I
del server.

Come mostra lo screenshot, il traffico segue il percorso standard dell'anello Sud:
(R6→R11→ R10→ R8→ R9), ignorando R1.



Il traffico verso un host generico della Puglia (10.42.40.0) segue il normale instradamento tramite l'anello Sud, rispettando la regola generale.

Caso B: Traffico Anomalo (Veneto → Server Anomalo)
È stato inviato traffico dal Veneto verso l'IP del Server (10.42.32.0).
In questo caso, il router applica la regola del Longest Prefix Matching. Riconoscendo la destinazione /32, il pacchetto non viene inviato direttamente verso il Sud, ma viene instra lungo l'anello Nord fino a raggiungere R1, che poi lo consegna al server tramite il link dedicato.



Il traffico verso il Server (10.42.32.0) viene identificato dalla rotta /32.
Il traceroute mostra che il pacchetto non scende verso la Puglia, ma risale o attraversa l'anello (R → R5 → R7 → R6 → R4 → R2 → R1) fino ad essere processato da R1, soddisfacendo il requisito di sicurezza.

Conclusione

L'implementazione della rotta statica con maschera /32 ha permesso di isolare chirurgicamente il traffico destinato al server "vittima", costringendolo a passare per R1 per l'ispezione, senz interrompere o rallentare il normale flusso di dati verso il resto della sede regionale Puglia. Quest conferma la corretta applicazione del principio di Longest Prefix Matching.

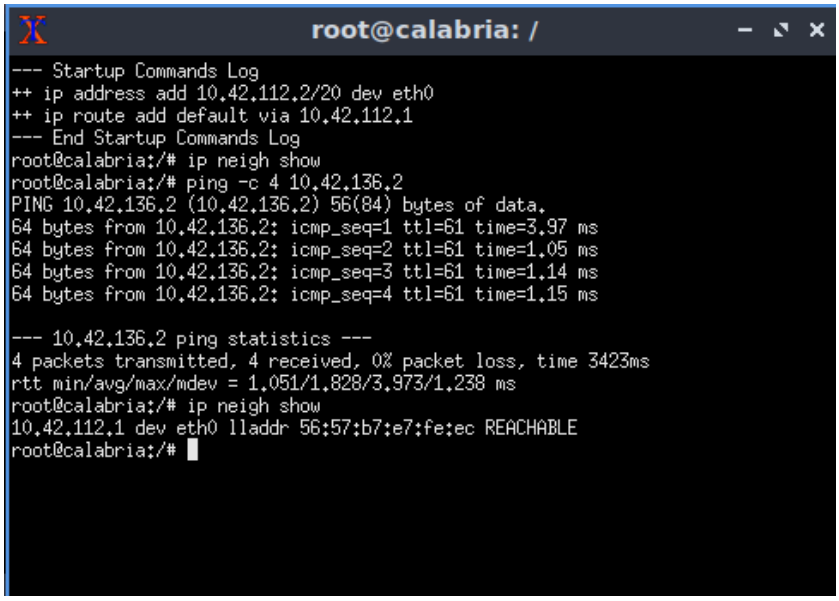
Esercizio 5: ARP e NAT

L'obiettivo dell'ultimo esercizio è l'analisi dei protocolli fondamentali per la comunicazione a livell 2 (ARP) e per l'accesso alla rete pubblica (NAT), verificando come i nodi risolvono gli indirizzi fisic e come il router di confine gestisce la traslazione degli indirizzi.

1. Analisi del protocollo ARP

Come richiesto, sono stati eseguiti i test di connettività tra sedi diverse.

Caso A: Calabria→ Sardegna
È stato eseguito un ping dalla sede Calabria (Host: 10.42.112.2) verso la sede Sardegna (Host: 10.42.136.2).



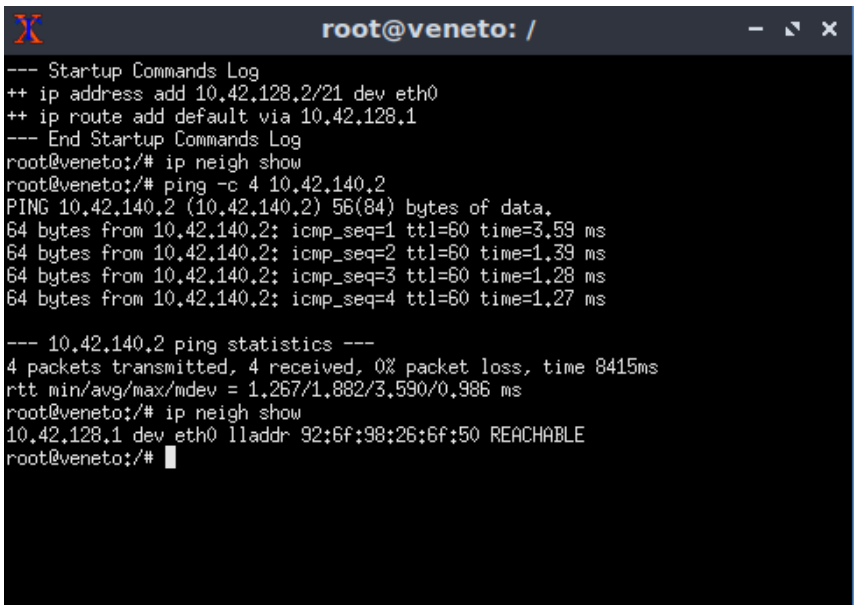
Osservazioni sulla tabella ARP:

1. Stato Iniziale: Il comando *ip neigh show* eseguito prima del ping non restituisce alcun risultato, confermando che la cache ARP è vuota.

2. Esecuzione del Ping: Il ping ha successo (0% packet loss), confermando la connettività end-to-end attraverso la rete.

3. Stato Finale: Eseguendo nuovamente *ip neigh show* dopo il ping, compare una singola entry: 10.42.112.1 dev eth0 lladdr ... REACHABLE
   Questo conferma il funzionamento teorico dell'ARP in reti routate:
   - Poiché la destinazione (Sardegna) si trova in una subnet diversa da quella sorgente (Calabria), l'host non cerca di risolvere direttamente il MAC address della destinazio finale.
   - L'host risolve invece il MAC address del suo Default Gateway (R8, interfaccia 10.42.112.1), che è il next hop necessario per inoltrare il pacchetto fuori dalla rete locale.

Caso B: Veneto↛ Toscana
È stato eseguito un ping dalla sede Veneto (Host: 10.42.128.2) verso la sede Toscana (H
10.42.140.2).

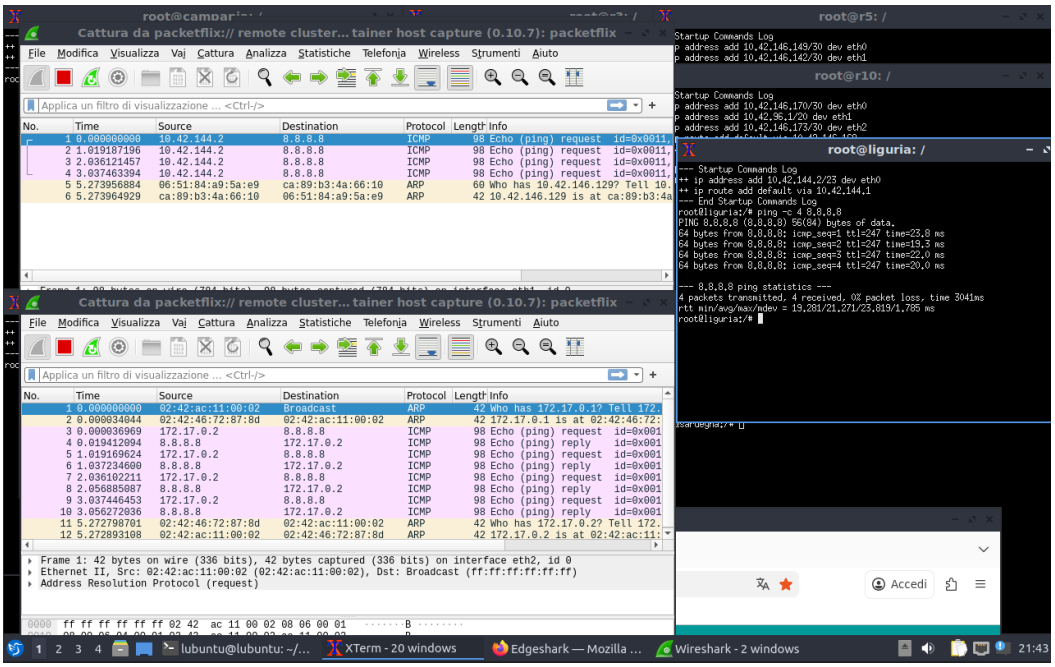


Osservazioni:
Anche in questo caso, il comportamento è analogo. L'host del Veneto, dovendo comunicare con una rete remota, invia una richiesta ARP in broadcast solo per ottenere l'indirizzo fisico del propri router di riferimento (R3, 10.42.128.1). Una volta ottenuta la risposta, incapsula il pacchetto IP in un frame Ethernet indirizzato al router e lo invia. La tabella ARP finale mostra quindi sol l'associazione IP-MAC del gateway locale.

2. Analisi del NAT

L'ultima parte dell'esercizio richiedeva di testare la connettività verso l'esterno (Internet) e analizzare il ruolo del NAT configurato sul router di confine R1.

È stato eseguito un ping dalla sede Liguria (10.42.144.2) verso l'indirizzo pubblico di Goo (8.8.8.8).



Analisi del Funzionamento:
Lo screenshot mostra sia il terminale della Liguria che riceve le risposte ICMP, sia le catture del traffico tramite wireshark.

1. Il Problema: L'intera rete aziendale utilizza lo spazio di indirizzamento privato 10.42.0.0 Questi indirizzi non sono instradabili sulla rete Internet pubblica. Se un pacchetto uscisse con sorgente 10.42.144.2, i router di Internet lo scarterebbero o, comunque, il server di destinazione (8.8.8.8) non saprebbe come rispondere a un IP privato.

2. La Soluzione (NAT/Masquerading):
   Sul router R1 è stata configurata la regola di MASQUERADE (Source NAT) tramite iptables3.

   - In Uscita (POSTROUTING): Quando il pacchetto ICMP proveniente dalla Liguria giunge a R1 e sta per uscire verso l'ISP, R1 modifica l'header IP. Sostituisce l'indirizzo IP sorgente originale (10.42.144.2) con il proprio indirizzo IP pubblico (assegnato all'interfaccia esterna connessa all'ISP). R1 memorizza questa associazione nella sua tabella di traduzione NAT.

   - In Entrata: Quando 8.8.8.8 risponde, invia il pacchetto all'indirizzo pubblico di R1. R consulta la tabella NAT, riconosce che quella risposta è associata alla connessione iniziata dalla Liguria, sostituisce l'IP destinazione con 10.42.144.2 e inoltra il pacchetto nella rete interna.

Le catture wireshark nello screenshot confermano questo flusso: si vedono le richieste ICMP e le risposte ARP relative al next hop verso l'esterno, permettendo la comunicazione bidirezion trasparente per l'host interno.