Risposte multiple:

1. B
2. D
3. A
4. A
5. B
6. D
7. A
8. C
9. C
10. C
11. A
12. A
13. C
14. D
15. A
16. C
17. D
18. A
19. Assunzioni:

47.120.0.12 -> Indirizzo IP pubblico dell’host che si connette alla VPN del Politecnico o eventualmente indirizzo pubblico associato all’host per mezzo di un NAT

130.192.18.253 -> Indirizzo IP del VPN Gateway

130.192.55.240 -> Indirizzo del server Web del Politecnico

130.192.20.45 -> Indirizzo VPN privato assegnato al client

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L2 Header** | **IP**  S: 130.192.18.253  D: 47.120.0.12  Next Protocol: 47 (GRE) | **GRE**  Protocol PPP | **PPP**  Protocol  IP | **IP**  S: 130.192.55.240  D: 130.192.20.45  Next Protocol  TCP | **TCP** | **HTTP** | **L2 Trailer** |

1. Al fine di individuare l’indirizzo MAC corrispondente ad un indirizzo IPv6 appartenete alla medesima sottorete, è necessario avviare la procedura di Neighbor Discovery equivalente per certi versi alla procedura effettuata in IPv4 per mezzo del protocollo ARP, con l’unica differenza consistente nella mancanza in IPv6 di indirizzi di broadcast. In sostanza l’host interessato a scoprire l’indirizzo MAC di un certo indirizzo IPv6 noto, invia un messaggio ICMPv6 in multicast a tutti gli host connessi alla propria sottorete il cui indirizzo IPv6 abbia i 24 bit meno significativi pari ai 24 bit meno significativi dell’indirizzo IPv6 dato:

(sia A l’host di origine e B l’host di destinazione)

[Eth] MAC host A -> 3333FF: 24 bit bassi dell’indirizzo IPv6 di B

[Ipv6] IPv6 di A -> FF02::1:FF + 24 bit bassi dell’indirizzo IPv6 di B

[ICMPv6] Neighbor Solicitation: who has “indirizzo IPv6 di B”?

A tale messaggio risponderà unicamente l’host B con il seguente messaggio:

[Eth] MAC host B -> MAC host A

[Ipv6] IPv6 di B -> IPv6 di A

[ICMPv6] Neighbor Advertisment: I am “indirizzo IPv6 di B” at “indirizzo MAC di B”!

Nel caso in cui l’host B non appartenga alla stessa sottorete di A, il che viene determinato semplicemente confrontando i prefissi di rete di entrambi gli indirizzi, deve essere determinato l’indirizzo MAC del Default Gateway, e dunque la stessa procedura di Neighbor Discovery viene effettuata nei confronti del Default Gateway.

1. Avendo supposto che il Recond Routing non sia abilitato lo schema relativo allo scambio dei pacchetti necessari ad instaurare la comunicazione risulta essere il seguente:

ACK

200 OK

200 OK

200 OK

180 Ringing

180 Ringing

100 Trying

180 Ringing

INVITE sip:chiamato@dominio2.org

100 Trying

INVITE sip:chiamato@dominio2.org

DNS Response

Query NAPTR SRV – A/AAAA

INVITE sip:chiamato@dominio2.org

sip:chiamante  
@dominio1.org

Server SIP @dominio1.org

D

Server DNS

D

Server SIP @dominio2.org

D

sip:chiamato  
@dominio2.org

DATA FLOW