

## SUMMARY OF TOPICS

**VPN (Virtual Private Network):** 2 tunnel end-points: macchina che si sta collegando, VPN Gateway. Installazione VPN: 3 fasi: configurazione canale di controllo (PPTP), configurazione di livello 2 (PPP - LCP), configurazione di livello 3 (PPP - IPCP). Autenticazione (CHAP) fra PPP-LCP e PPP-IPCP.

**LCP (Link Control Protocol):** VPN. Protocollo per fare operazioni di controllo iniziali. Fa parte del PPP.

**CHAP (Challenge-Handshake Authentication Protocol):** VPN. Protocollo per l'autenticazione.

**IPCP (IP Control Protocol):** VPN. Protocollo per ottenere dal VPN Gateway un indirizzo IP interno alla VPN. Fa parte del PPP.

**Accesso Centralizzato:** VPN. Il traffico passa prima dal VPN Gateway il quale lo reindirizza verso le destinazioni (opzione di configurazione "Use Default Gateway on Remote Networks" = true).

**Accesso Distribuito:** VPN. Il traffico non passa necessariamente dal VPN Gateway ma viene indirizzato con le normali regole di routing (opzione di configurazione "Use Default Gateway on Remote Networks" = false).

**PPTP (Point-to-Point Tunneling Protocol):** Access VPN. Effettua il tunneling a livello 2. Per costruire tunnel direttamente dalla macchina utente.

**L2TP (Layer 2 Tunneling Protocol):** Access VPN. Effettua il tunneling a livello 2. Per reti VPN dial-up nella quale gli host si possono connettere da postazioni diverse.

**GRE (Generic Routing Encapsulation):** Site-to-site VPN. Effettua il tunneling a livello IP.

**IPsec:** Site-to-site VPN. Effettua il tunneling a livello IP.

**BGP (Border Gateway Protocol):** Site-to-site VPN, MPLS. Protocollo di routing inter-AS utilizzato per connettere tra loro più router gateway che appartengono a sistemi autonomi AS (Autonomous System) distinti fra loro. Protocollo a indicazione di percorso (Path Vector) che effettua il routing basandosi sulle regole determinate da ciascuna rete. Supporta il routing indipendente dalle classi (Classless InterDomain Routing) e aggrega gli instradamenti per diminuire la dimensione delle tabelle. Ideato per sostituire il protocollo EGP (legato alla filosofia dell'internet centralizzato dipendente dalla rete NSFNET) e rendere internet un sistema decentralizzato. Gli ISP sono obbligati a utilizzare BGP per stabilire i criteri di routing e lo rendono uno dei più importanti protocolli di internet.

**MPLS Label Distribution Protocols:** LDP, PIM, RSVP/CR-LDP, BGP.

**MPLS Routing Protocols:** OSPF, IS-IS, BGP-4, IGRP, RIP.

**LSP (Label Switched Path):** MPLS. Un LSP è un percorso virtuale basato su criteri FEC che parte da un Ingress Router verso un Egress Router attraverso una rete MPLS gestita da un protocollo di Label Distribution. Gli LSP sono dei tunnel MPLS poiché risultano opachi rispetto agli altri livelli. Sono unidirezionali pertanto per avere una comunicazione bidirezionale è necessario gestire un secondo LSP che va nella direzione opposta rispetto al primo. Funzionamento LSP: L'Ingress Router (LER) aggiunge una label (push) al pacchetto e determina l'LSP da seguire; uno o più LSR intermedi cambiano la label del pacchetto con un'altra (swap) e inoltrano il pacchetto al router successivo; l'Egress Router (LER) rimuove la label più esterna (pop) e inoltra il pacchetto basandosi sull'header del livello successivo (es. IPv4).

**LER (Label Edge Router):** LSP. Tramite le funzioni push/pop, aggiunge/toglie le label ai pacchetti IP entranti in base al FEC appropriato servendosi di una tabella.

**LSR (Label Switching Router):** LSP. Tramite la funzione swap cambia la label del pacchetto. Per ogni porta c'è una tabella che indica l'instradamento (data una label su una porta, viene indicata la porta ove smistare il pacchetto e la nuova label).

**FEC (Forwarding Equivalence Class):** LSP. E' la classe che distingue un LSP da un altro. Una FEC tende a corrispondere a un LSP e descrive un insieme di pacchetti con caratteristiche simili e/o identiche che possono essere spediti nella stessa maniera attraverso la stessa label. I criteri per attribuire una FEC possono essere: stessa destinazione (unicast/multicast); stesso tunnel VPN; ottimizzazione di alcune tipologie di pacchetti (traffic engineering); QoS o classe di servizio (VoIP/Web).

**Link-Local:** IPv6. Indirizzo privato valido solo su un segmento di rete locale (link fisico) oppure su una connessione point-to-point. Utile per l'autoconfigurazione stateless. Un pacchetto contenente un indirizzo Link-Local non viene mai inoltrato dai router. MAC\_H = 24 bit alti del MAC + settimo bit da sinistra a 1, MAC\_L = 24 bit bassi del MAC. Formato: fe80:MAC\_HFF:FEMAC\_L/10

**Site/Global:** IPv6. Indirizzo pubblico accessibile a tutta la rete internet. Formato: 2001:...

**Site Local:** IPv6. Indirizzo privato, utile solo nel Site scope. Formato: fec0::/10

**Prefix:** IPv6. Sostituisce il concetto di netmask di IPv4. E' un numero di bit posto dopo un indirizzo IPv6. Esempio: FEDC:0123:8700::/10. 10 e il prefix.

**Neighbor Solicitation:** IPv6. Significato: "Esiste qualcuno che abbia un certo indirizzo Link-Local all'interno della mia sottorete?" Un host può fare una richiesta per vedere se il suo Link-Local è univoco. Se riceve una Neighbor Advertisement c'è già qualcun altro con quell'indirizzo e deve generare un altro Link-Local (altri 64 bit bassi). Se non riceve risposte può mandare un Group Membership Report. Può usare il NS anche per chiedere chi ha un certo Link-Local per poi generare pacchetti ICMP verso quella destinazione. Formato: [Eth] MAC\_Source → 3333FF-MAC\_Searched\_L | [IPv6] :: → FF02::1:FFMAC\_Searched\_L | [ICMP6] N.S.: Who has Link\_Local\_del\_MAC\_Searched?

**Neighbor Advertisement:** IPv6. Significato: "Sì, ho questo Link-Local e questo MAC" Formato: [Eth] MAC\_Source → MAC\_Dest | [IPv6] Link\_Local\_Source → Link\_Local\_Dest | [ICMP6] N.A.: I am Link\_Local\_Source at MAC\_Source

**Group Membership Report:** IPv6. Significato: "Ho questo indirizzo IPv6 ed è mio" Formato: [Eth] MAC → 3333FF-MAC\_L | [IPv6] Link\_Local → FF02::1:FFMAC\_L | [ICMP6] G.M.R. (Link\_Local)

**Router Solicitation:** IPv6. Significato: "Uno dei router che si affacciano sulla mia sottorete può darmi un indirizzo IPv6 pubblico Aggregatable oppure un Site Local?" Se uno dei router ha abilitato il Router Advertisement risponde. Formato: [Eth] MAC → 3333FF-000002 | [IPv6] Link\_Local → FF02::2 | [ICMP6] R.S.

**Router Advertisement:** IPv6. Se abilitato, permette al router di rispondere ai messaggi Router Solicitation mandati dagli host e di dare agli host degli indirizzi Site/Global o Site Local. Il pacchetto contiene informazioni come il prefix annunciato, il Valid Lifetime, il MAC del router (salvato dagli host nella cache). Formato: [Eth] MAC\_Router → 3333FF-000001 | [IPv6] Link\_Local\_Router → FF02::1 | [ICMP6] R.A.

**DAD (Duplicate Address Detection):** IPv6. Consiste nell'inviare in multicast un pacchetto Neighbor Solicitation per verificare che il Link-Local appena generato sia univoco nella propria sottorete. Si attende almeno un secondo. Se qualcun altro possiede quel Link-Local, arriverà una risposta tramite pacchetto Neighbor Advertisement e dovrà essere generato un altro Link-Local. In caso contrario si considera l'indirizzo Link-Local come valido ed è possibile iniziare la fase di Router Discovery.

**Autoconfigurazione Stateless:** IPv6. Al boot un nodo crea automaticamente un indirizzo Link-Local, esegue la procedura DAD. Se il Link-Local è valido il nodo può parlare con tutte le macchine della propria LAN anche senza router.

**Router Discovery:** IPv6. È la fase successiva all'autoconfigurazione stateless. Se esiste un router il nodo rimane in ascolto dei messaggi Router Advertisement oppure manda un pacchetto Router Solicitation. Se un router risponde a quest'ultimo con un pacchetto Router Advertisement, il nodo ottiene anche un indirizzo globale.

**Neighbor Discovery:** IPv6. Serve a una stazione per scoprire l'indirizzo MAC di un'altra stazione conoscendone l'IPv6. Consiste in un pacchetto Neighbor Solicitation con [MAC destinazione] = 3333FF-ultime 6 cifre IPv6 e [IPv6 destinazione] = FF02::1:FF ultime 6 cifre IP.

## Indirizzi IPv6

Ipv4 compatibile con ipv6 -> ::/96

6to4 -> 2002::/48 (parto da dopo 2002 per avere IP)

Tutti i nodi (multicast) -> FF02::1

Tutti i router (multicast) -> FF02::2

Mappato ipv4 -> 0:0:0:0:FFFF::/96

MAC da ipv6(esempio) -> FE80::0201:06FF:FEA5:3A4C diventa 00:01:06:A5:3A:4C

Multicast solicited node -> FF02:1:FF:24\_bit\_meno\_significativi\_ipv6/104

Tunnel broker -> 2002::/16

MAC multicast ipv4 -> 01-00-5E-0(bit) + 23\_bit\_meno\_significativi\_IP

MAC multicast ipv6 -> 33:33+32\_bit\_ipv6

ULA -> FC00::/7 (FC00::/8 in futuro FD00::/8 privati)

Multicast -> FF00::/8 - FFFF:[...]:FFFF