TSR: Concetti principali e nozioni ad alto livello

Indirizzi IPV6 privati:

- Indirizzi Link Local [FE80::/64]: usati solo all'interno della stessa rete privata (link)
- Indirizzi Site Local [FEC0::/10]: usati per comunicazioni fra diverse reti private
- Unique local address: indirizzi univoci a livello mondiale

Indirizzi IPV6 pubblici (GLOBAL UNICAST):

- IPV4 interoperability: [000….000IPV4] indirizzi con 96 bit a zero, seguiti dall'indirizzo IPV4

Headers IPV6: (TLV è il formato per definire delle opzioni custom per l'header)
Extension headers ipv6:se dopo tutte le estensioni/opzioni aggiuntive non arrivo ad un multiplo di 64bit, devo applicare un padding (usando l'opzione/estensione PAD1 o PADN)

- Hop by hop option (opzioni gestibili da qualsiasi router) *usa TLV*
- Routing option (fa il source routing, cioè la sorgente lista I nodi che deve attraversare)
- Fragment option (fa la frammentazione)
- Authentication option (gestisce autenticazione a livello 3)
- Encrypted security payload option (criptazione payload) Destination option (opzioni gestibili solo dalla destinazione) *usa TLV*

Mapping tra LV3 e LV2 (da IP a MAC) in IPV6 multicast&unicast (comunicazioni 1:1 o 1:N):
→ caso multicast IPV6 transmission: ricava il MAC di un IPV6 ["3333" in esadecimale][ultimi 32bit dell'indirizzo IPV6]
Neighbor discovery (ottenimento del MAC address di un nodo): il Solicited Node Multicast Address è un indirizzo IPV6 associato ad un qualsiasi nodo della rete, ed è generato in modo che sia abbastanza raro che faccia matching con più di un indrizzo. Per ottenere il MAC address di qualcuno devo creare un pacchetto Neighbor Solicitation che ha come destinazione il Solicited Node Multicast Address (viene scartato dai nodi che lo ricevono ma non matchano con l'IPV6 del destinatario desiderato), il nodo che riceve tale pacchetto deve rispondere con un Neighbor Advertisement che contiene il MAC address. **Anche i router ha un meccanismo analogo e omonimo.**

Configurazione delle interfacce: ogni indirizzo IPV6 ha una parte finale da 64bit che può essere configurata a mano, ottenuta dal DHCP o ottenuta dal MAC address. Se voglio usare il MAC di un indirizzo IPV4 (48bit) ma in IPV6, divido a metà il MAC e nel mezzo gli inserisco in esadecimale 0xFF seguito da 0xFE.

- Manual configuration (sconsigliata)
- Stateful configuration (automatica con DHCP server)
- Stateless configuration (automatica ma senza bisogno di server)
- Hybrid Stateless DHCP (ottengo alcuni dati dal router e altri dal DHCP server)

Gli indirizzi MAC univoci a livello mondiale hanno "0" al loro 7-mo bit (most significant, a sinistra)
Privacy Extension Algorithm: il MAC address è spesso fonte di problemi di sicurezza perché c'è un MAC address nella sua parte finale che può rivelare l'identità del possessore. Il Privacy Extension Algoritm permette di generare diversamente l'IPV6 in modo che al fondo non abbia più il MAC. Si prende l'IPV6 e se ne calcola l'MD5 hash, poi si mette a "0" il 7-mo bit per indicare che è un nuovo indirizzo univoco.
Duplicate Address Detection (DAD): prima di assegnare un indirizzo, il router manda una Neighbor Solicitation a "all-agents" (cioè a tutti i server della rete) per vedere se qualche host con l'indirizzo che sta per assegnare, gli risponde. Se qualcuno risponde, allora quell'indirizzo esisteva già e non si può assegnare.
Scoped Address: alcune stazioni/router hanno più interfacce connesse a reti locali *LINK LOCAL* diverse (le stazioni in questo caso si chiamano Dual Alone), quando devono inviare qualche messaggio agli host ad esse collegati, matchano tutte le reti. Ciò accade perché si usa il prefisso della rete per contattare l'host, ma le reti hanno tutte lo stesso prefisso. Quindi si usa lo SCOPE, cioè le reti gestiranno indirizzi da 17bit al posto di 16bit, così nell'ultimo bit si può segnare l' ID dell'interfaccia, evitando l'ambiguità al momento dell'invio.

Routing IPV6: l'ON THE FLY ROUTING permette di leggere la routing table e instradare il pacchetto, mentre il PROACTIVE ROUTING permette di costruire la tabella stessa (in modo statico *gestito da un operatore*, o dinamicamente *in modo automatico*)
Routing Protocols: essi permettono di distribuire fra i vari router informazioni sulla topologia della rete. Abbiamo 2 tipologie:

- **Integrated Routing:** si usa un solo protocollo (sia per IPV4 che IPV6) per annunciare un pacchetto
- **Ships in the night:** si usano 2 protocolli (uno per IPV4 e uno per IPV6) per annunciare un pacchetto

Routing transizione da IPV4 a→ IPV6: il passaggio avverrà lentamente, nel mentre le stazioni devono supportare sia IPV4 che IPV6. Per attraversare una rete IPV4 only, si usa un tunneling che imbusta il pacchetto IPV6 dentro quello IPV4, sfrutta il protocollo "**GRE"** ([IPV4 [headerGRE+IPV6 packet]]) e quello "**IPV6 in IPV4"** (si usa un campo "protocol=41" nel pacchetto IPV4). Essi servono ad indicare che c'è un pacchetto IPV6 dentro uno IPV4, nel primo caso si usa un header GRE, nel secondo caso si modifica l'header IPV4.

- **Host Centered Solutions (far comunicare 2 host *dual stack* usando IPV6 in una rete IPV4):**
  - **IPV4 compatible addresses:** vengono usati indirizzi IPV6 da 96 zeri seguiti dall'IPV4, essi vengono mandati ad un'interfaccia virtuale che li processa/converte
  - **IPV4 compatible addresses with Static Router:** come sopra ma in mezzo ci sono dei router
  - **6over4:** i vari nodi IPV6 comunicano usando il MULTICAST IPV4 sulla rete IPV4, cioè una sorta di rete virtuale LAN dove al posto dei MAC si usano gli IPV4 (quindi il Neighbor Discovery avviene richiedendo l'IPV4).

    - **ISATAP:** come il 6over4 ma al posto del Neighbor Discovery si usa la PRL (una lista che contiene l'elenco dei router ISATAP presenti nel percorso fra la sorgente e la destinazione), essa è distribuita dal DHCP o dal DNS.
- **Network Centered Solutions (2 host IPV6 sono nelle loro reti IPV6, e li facciamo comunicare attraverso una rete IPV4 che collega le due reti IPV6):**
    - **6to4:** il router di confine nella rete IPV4 fornisce l'accesso verso la rete IPV6, tale router ha un indirizzo IPV6 con dentro l'indirizzo IPV4
    - **Mixed 6to4:** come il 6to4 classico, ma una rete IPV6 è connessa, attraverso una rete IPV4, alla rete globale (internet) IPV6.
    - **Teredo:** come 6to4 ma i pacchetti sono incapsulati dentro UDP, cioè [UDP[IPV4[IPV6]]]
    - **Tunnel Broker:** poiché i primi 16 bit del 6to4 sono fissi "2002", non si possono usare tutti i bit disponibili nell'indirizzo. Allora si usa un server dedicato (Tunnel Broker Server), così quando lo contattiamo per chiedergli di raggiungere una destinazione IPV6, non c'è bisogno di leggere i primi 16bit perché esso implementa solo il protocollo Tunnel Broker. Il Tunnel Broker Server invia l'indirizzo IPV4 del Tunnel Server a chi lo contatta. Quando si raggiunge il Tunnel Server, viene instaurato un Tunnel and Point (con IPV6 dentro a IPV4, come il 6to4) verso la destinazione IPV6 richiesta.
- **Scalable Carrier-Grade Solutions (tanti host in reti IPV6 connesse da una IPV4 o vice versa):**
    - **DS-Lite:** abbiamo una rete IPV4+IPV6 (del cliente) con degli host di un tipo e altri dell'altro, che tramite un CPE (configurato dal provider, conosce la posizione del LARGE SCALE NAT) è connessa ad una rete IPV6 (a questa rete IPV6 sono connesse tante di queste reti IPV4+IPV6) che infine tramite un LARGE SCALE NAT (nat che gestisce grandi numeri, detto anche AFTR, esso possiede una tabella estesa che ha sia l'IPV4 sorgente che l'IPV6 della rete sorgente) è connessa all'internet IPV4 (vedi *). Quindi un pacchetto privato IPV4 viene mandato alla CPE che lo imbusta in un IPV6 con destinazione LARGE SCALE NAT, dove viene estratto, viene cambiato l'IPV4 sorgente da privato a pubblico e mandato su internet.
    - **Address Plus Port (A+P):** come il DS-Lite (vedi *), ma ad ogni rete IPV4+IPV6 dei clienti viene assegnata una porta TCP/UDP (così si mantiene uno stato di ogni device, ovvero si tratta di una *soluzione statefull*), inoltre il NAT si sposta dove c'è il CPE e quindi non è più large scale perché gestisce solo la rete del cliente.
    - **Mapping Address and Port (MAP):** come A+P (vedi *) ma viene cercata una *soluzione stateless* cioè viene usato solo IPV6 per capire la provenienza del pacchetto, le reti dei clienti sono IPV4, e porte che vengono associate ad ogni IPV4 sono un SET (non contigue) detto PSID. Il CPE crea il suo indirizzo esterno usando il PSID, il prefisso IPV6 della rete intermedia (fra cliente e internet) e "EA" bit.
    - **NAT64+DNS64:** le reti sono così→la rete del cliente è solo IPV6 che può contenere il DNS64, poi abbiamo una rete IPV4+IPV6 che contiene il NAT64 (e il DNS64, se non c'era nella IPV6), e infine abbiamo la rete internet IPV4. Il pc del cliente crea un pacchetto IPV6 con dentro uno IPV4, chiede al DNS64 l'ip della destinazione, esso chiede a server IPV4 o IPV6 (perché non sa dov'è la destinazione) e manda indietro l'ip destinazione imbustato dentro un IPV4 embedded al NAT64. Esso lo traduce in IPV4 o IPV6 e lo manda alla destinazione.

Tecnologie di LV 1:

- **Repeter:** amplifica il segnale e lo forwarda su un'altra porta
- **Hub:** amplifica il segnale e lo forwarda a tutte le sue porte (è un repeter ma con più di una porta)

Tecnologie di LV 2:

- **Bridge:** ricevo una trama, riesco a leggerla e la invio su una diversa tecnologia (wifi/eth). Essi accumulano i pacchetti in un buffer, quindi non è possibile che ci siano collisioni.
- **Trasparent Bridge (switch):** sono dei bridge ma usati nelle reti ethernet. Esso deve essere plug and play, non deve mai modificare i frame che invia, ma possono essere ricevuti in ordine diverso o con qualche frame mancante (a causa della rete). La sua tabella di forwarding si chiama Filtering Database, essa può non essere aggiornata o popolata correttamente e quindi può causare problemi di pacchetti non ricevuti. Si possono fare attacchi di MAC flooding o Packet storming per saturare la memoria della Filtering Database (soluzione: porre un limite massimo nel buffer), o Broadcast Storm per creare cicli infiniti di invio di pacchetti dove c'è un anello di Bridges (soluzione: staccare un link per spezzare l'anello).

Tecnologie di LV3:

- **Router:** permettono la separazione dei domini di broadcast. Posso inoltre gestire via software le porte di un router in modo da associare una o più VLAN (lan virtuali) ad ogni porta del router, e cambiarle le VLAN associate alle porte quando voglio, senza dover spostare i cavi dei dispositivi. Così posso effettuare il One Hub Router, cioè assegnare ad una porta tutte le VLAN, in essa inserisco il router e faccio gestire ad esso tutte le VLAN degli altri dispotivi. I pacchetti che passano vengono "colorati" cioè si applica un valore al campo "VLAN" del pacchetto (0=fa la user priority, 1=vlan default, 4094=max vlan).
    - **Link di tipo Access:** se configuriamo 2 porte di un link in modalità access, tutto il traffico nel link si colora
    - **Link di tipo Trunk:** è un link fra due switch che collega le due lan in modo da poter far passare nel link tutte le diverse VLAN colorate

Algoritmi di Routing (determina percorso dei pacchetti nella routing table) and Forwarding (legge la routing table e invia i pacchetti):

- **Algoritmi di On The Fly Routing (forwarding):**
    - **Routing by Network Address:** legge la destinazione dentro il pacchetto per sapere dove spedirlo
    - **Label Swapping:** un'etichetta sul pacchetto indica la strada che deve percorrere
    - **Source Routing:** Nell'intestazione del pacchetto viene scritta la strada che deve fare il pacchetto, quindi non bisogna mai leggere la routing table per conoscere il next hop
- **Algoritmi di Routing Proattivo:**
    - **Non adattivo:** non si adatta alla rete, e usa delle Fixed directory cioè delle tabelle di routing pre-costruite che non cambiano

- **Adattivo:** si adatta alla rete

Algoritmi Dynamic Routing:

- **Algortmi centralizzati:** un'entità distribuisce le informazioni di routing da inserire nella tabella di routing
- **Algoritmi Isolati**
- **Algoritmi distribuiti:** il calcolo delle informazioni di routing è distribuito ma non vi è più un single point of failure

Algoritmo Distance Vector Routing:
Il Distance Vector è un vettore che contiene tutte le destinazioni che il mittente sa raggiungere, e tutte le distanze per ogni destinazione. Ogni router manda ai suoi vicini il distance vector, i quali fanno il merge dei distance vector e calcolano la tabella di routing. Se due percorsi hanno la stessa distanza si può usare l'ECMR (equal cost multiple routing) cioè dividere i pacchetti equamente fra tutti i rami equivalenti.
I problemi sono → il *Black Hole* (router che dice di saper raggingere una destinazione, invece non può), il *Count To Infinity* (router che conta all'infinito per calcolare una destinazione), il *Bouncing Effect* (pacchetti che vanno vanti e indietro fra vari router in loop infinito)
Le soluzioni parziali sono → *Split Horizon* (se un router1 pensa di poter raggiungere una destinazione tramite un altro router2, eviterà di includere la destinazione nel distance vector che manderà al router2, così che il router2 non proverà nemmeno a raggiungere la destinazione tramite router1. Risolve il Count To Infinity ma ricalcolare il distance vector ad ogni nodo è dispendioso e ogni router deve aspettare tempo per essere certo che un nodo non sia raggiungibile), *Split Horizon With Poison Reverse* (al posto di non comunicare che un nodo è raggiungibile, comunichiamo che è raggiungibile ma a costo infinito, così eliminiamo le attese)
Algoritmo Path Vector Routing: come il distance vector ma oltre a indicare la distanza viene messa anche la lista di nodi attraversati per ogni distanza
Algoritmo Link State: ogni router manda ai suoi vicini dei messaggi per dire a quali nodi è collegato, quindi ogni router accumula e mette insieme queste informazioni (dette Link State) al fine di avere una visione dell'intera rete. Il Selective Flooding permette di leggere nella propria tabella se il Link State da inviare è presente, se lo è, allora non devo inviarlo perché l'ho già fatto. Inoltre in tabella si usano anche numerazioni e timer al fine di distinguere le diverse repliche dei Link State inviati.

Protocolli di Routing: la rete internet è suddivisa in domini che a loro volta sono raggruppati in Autonomous Systems. I router che si trovano sul bordo di un Autonomous System sono i Border Gateway. Le Neutral Access Point(NAP) o Internet Exchange Point(IEP) sono delle stanze create da terzi, dove gli ISP possono lasciare i loro router in collegamenti a velocità altissime.

- **IBGP o IGP (Interior Border Gateway Protocol):** protocolli usati dai router interni allo stesso Autonomous System
  - **RIP (Routing Information Protocol):** può contare il numeri di hop per raggiungere la destinazione, in modo settare un valore massimo per evitare hop infiniti. Scambia i Distance Vector periodicamente a prescindere dal fatto che la routing table sia cambiata o no.
  - **IGRP (Interior Gateway Routing Protocol):** come il RIP ma ottimizzato per le grandi reti, inoltre ogni LINK ha delle caratteristiche come Delay, Bandwidth, Reliability, Load, Max Packet Length. Se ci sono path equivalenti, i pacchetti vengono smistati a seconda della velocità di ogni link equivalente.
  - **OSPF (Open Shortest Path First):** gestisce grandi reti con il routing gerarchico dividendo i domini in aree. Quindi il router manda i link state a tutti i router della sua area, le info di ogni area vengono scambiate e aggregate. Purtroppo se un'area si "spegne" si avranno problemi di comunicazione fra le aree, inoltre i percorsi fra aree non sono simmetrici e la visibilità dei percorsi fra aree è limitata.
- **EBGP o EGP (Esterior Border Gateway Protocol):** protocolli usati dai router sul bordo o fra due Autonomous System diversi
  - **BGP (Border Gateway Protocol):** nella tabella di routing, oltre al numero di hop per raggiungere la destinazione, c'è anche l'elenco di Autonomous Systems da attraversare. Solamente se c'è un cambiamento topologico vengono scambiati i Distance Vectors (usando TCP).
  - **IDRP (Inter Domain Protocol):** miglioria del BGP, poi integrata in BGP
  - **Static Routing**

Tecnologia MPLS (Multi Protocol Label Switching): si basa su una rete che ha un core centrale in fibra ottica e un guscio di router MPLS al suo esterno. MPLS mette un'etichetta davanti al pacchetto, così che non sia necessario leggere dentro di esso per capire dove instradarlo. MPLS è connection oriented (cioè i pacchetti sono instradati grazie all'etichetta) e connectionless (non devo aprire una connessione verso un indirizzo per poterlo raggiungere). Non dovendo basare il routing su un indirizzo, è possibile fare ingegnerizzazione del traffico.
- La rete MPLS (nuovla) ha dei router Label Switch Router (LSR) divisi in LSR Ingress (riceve il traffico in entrata nella nuvola e gli assegna etichette → "push") e in LSR Egress (fa uscire il traffico dalla nuvole e toglie le etichette → "pull").
- I link MPLS (LSP Label Switch Path) sono dei percorsi a commutazione di etichetta, cioè dove i pacchetti viaggiano.
- I pacchetti MPLS hanno un Header (Shim) che contiene l'etichetta (20bit), i pacchetti vengono gestiti da protocolli identici al protocollo IP (così da mantenere l'integrazione con l'esterno della rete MPLS) ma con info aggiuntive per l'MPLS. Fra l'header di LV2 e quello di LV3 si possono inserire vari moduli. Si può inserire l'header MPLS dentro l'header LV2 così da poter usare MPLS con i vecchi ATM

Etichetta & Creare un LSP (un link in MPLS): i FEC sono gruppi di pacchetti che vengono trattati allo stesso modo dalla LSR, hanno lo stesso percorso LSP e stessa etichetta. Per creare un LSP i router associano un'etichetta ad un FEC: se abbiamo un link che collega il nodo (1) al nodo (2), il nodo a valle (2) sceglie l'etichetta del pacchetto e lo comunica al nodo a monte (1), infine il nodo a monte (1) indirizzerà il traffico secondo l'etichetta.

- **Binding Statico (modalità On-Demand):** persone fisiche configurano i device per scegliere le etichette volute a priori, ciò non è interoperabile perché esistono vari protocolli diversi
- **Binding Dinamico (modalitrà Unsolicited):** etichetta assegnata automaticamente dal router sulla base del traffico che arriva (Data/Traffic Driven) oppure sulla base di un altro router/nodo che comunica l'etichetta da usare (Control Driven)

Protocolli di distribuzione delle etichette:

- **BGB:** se il router scopre (gli viene annunciata) una nuova destinazione, viene associata automaticamente anche un'etichetta

- **Label Distribution Protocol (LDP):** viene usato apposta per la distribuzione delle etichette
- **Resource reservation protocol (RSVP):** permette di riservare le richieste di etichetta, così da propagare una scelta di etichetta

Protocolli di routing: per MPLS vengono usati delle versioni modificate dei protocolli classici cioè OSPF-TE e IS-IS-TE. Essi implementano il Constraint Based Routing cioè un routing basato su vincoli (carico dei link, capacità dei link, percorsi alternativi..) che permette di effettuare il traffic engineering.

Modalità di routing:

- **Hop by hop routing:** ogni router sceglie dove mandare il pacchetto autonomamente
- **Explicit routing:** ogni router decide dove mandare il pacchetto e impone agli altri il percorso dei pacchetti
- **Explicit constraint routing:** poiché i vincoli cambiano molto velocemente, non si può sempre usare un protocollo come l'hop by hop, quindi con l'explicit constraint si fa scegliere il percorso ad 1 solo router che lo impone a tutta la rete

Ingegneria del traffico: vengono raccolti molti dati sui link carichi della rete e il traffico viene distribuito di conseguenza. Consideriamo che i link rimangano statici nel loro carico di rete. Quando nuovi LSP vengono aggiunti, il vecchio carico rimane sempre sui vecchi link ma il nuovo si spalma nei nuovi link. Periodicamente vengono fatti controlli sui vecchi LSP troppo carichi in modo da abbatterli e ribilanciare il carico.

Recupero Guasti:

- **Link Rerouting:** per ogni link della rete viene creato un link alternativo. Quanto un link si rompe, il nodo davanti a lui fa push dell'etichetta del link rotto e poi manda i pacchetti nel percorso alternativo. Il processo è molto rapido, non bisogna ricalcolare nessun percorso ma se dei pacchetti avevano la priorità su altri, questa priorità si perde.
- **Edge to Edge Rerouting:** per ogni link della rete è presente un intero LSP alternativo. Quando un link si rompe, il nodo davanti ad esso manda un messaggio al nodo precedente, e così via fino al primo nodo dell'LSP che sposta tutti i pacchetti su un nuovo LSP. Il nuovo LSP è stato settato per priorità di carico, così i pacchetti che avevano priorità non la perdono.

Qualità del servizio (QoS): le reti che supportano la QoS fanno classificazione del traffico, scheduling routing (gestione delle code dei pacchetti), controllo di accesso alla rete (limitazione della quantità di traffico entrante). Vengono quindi utilizzate delle code multiple per accodare i pacchetti, e c'è uno Scheduler che preleva da una coda il pacchetto da inviare. Vi sono vari algoritmi per prelevare il pacchetto:

- **Priority Queuing:** si divide per priorità, ma se ho troppi pacchetti a priorità alta, si rischia lo starving di alcune code.
- **Round Robin:** prende un pacchetto da ogni coda, ma li prende pesati
- **Deadline Queuing:** ogni pacchetto in coda ha un conto alla rovescia per l'invio

Algoritmi Controllo del traffico:

- **A priori:** l'ISP deve assicurarsi che la rete sia adeguatamente dimensionata e ingegnerizzata per servire il traffico atteso
- **Call/Flow level:** gli host devono notificare alla rete le operazioni che stanno per fare così che la rete allochi le risorse
- **Policing & Shaping:** il Policing è la limitazione del traffico, lo Shaping è il controllo e la modifica del traffico affinché esso rientri nei limiti imposti dal Policing

Protocolli Controllo del Traffico:

- **Leaky Bucket:** il fornitore del servizio (es streaming) dichiara quanta banda dovrà usare e il BURST (massima quantità di bit inviabili in un certo lasso di tempo molto breve). Quindi ogni router ha un Bucket pieno di crediti che vengono usati proporzionalmente alla richiesta dal fornitore. La grandezza del Bucket è il BURST. L'operatore della rete può decidere cosa fare del traffico che non rispetta i limiti.
  Se questo controllo è applicato dalla stazione del fornitore, prende il nome di SHAPING, se invece è usato dal nodo successivo alla stazione del fornitore prende il nome di POLICING.

Framework per garantire la qualità del servizio:

- **Integrated Services (IntServ):** tramite la Resource Reservation Protocol (RSVP), l'applicazione può prenotare nella rete le risorse che gli servono, così i nodi della rete comunicano fra di loro e propagano la richiesta. La rete risponderà usando RSVP per comunicare se può soddisfare o meno la richiesta.
- **Differentiated Services (DiffServ):** si creano delle classi di traffico e viene garantito il servizio alla classe, non all'intera applicazione.

VPN: le Intranet VPN sono reti private basate su IP, le Extranet VPN sono reti (pubbliche/private) che comprendono organizzazioni diverse. I VPN Gateway router che implementano la rete VPN, cioè sono i router usati dalla VPN.

Accesso a internet da una VPN:

- **Centralizzato:** prima si raggiunge la sede della VPN e poi si accede a internet dalla sede.
- **Distribuito:** l'accesso ad internet per i nodi avviene con l'IP e la rete del nodo, senza passare per la sede della VPN

Modelli di fornitura:

- **Overlay Model:** l'internet pubblico non sa nulla del VPN costruito sopra e non vi partecipa
- **Peer Model:** l'internet pubblico partecipa alla VPN comunicando con i Gateway VPN
- **Customer Provisioned:** alla rete VPN che collega le varie sedi dell'azienda partecipano anche i router dell'azienda stessa. I VPN gateway sono realizzati con solo i dispositivi del cliente. Per aprire una connessione col servizio VPN, il cliente deve rispondere (criptare) una "sfida" mandata dal VPN. L'accesso ad internet può essere solo centralizzato.
- **Provider Provisioned:** il provider VPN gestisce tutto, non solo la rete VPN ma anche i collegamenti con le varie aziende

Topologie VPN: nella topologia Hub and Spoke la rete VPN esce verso tutti gli endpoint delle varie sedi dell'azienda, passando tramite un unico endpoint finale, dove c'è un sovraccarico della rete. Nella topologia Mesh ogni endpoint delle sedi dell'azienda è collegato con ogni altro ndpoint, quindi esistono tutte le combinazioni e i pacchetti si recapiteranno sempre end-to-end. Rete più complessa ma link meno carichi.

Protocolli VPN:

- **PPP (non nato per vpn):** protocollo che collega due nodi alla rete. LCP è un protocollo usato nel PPP per negoziare i parametri a livello datalink. Invece l'LCP è un protocollo usato dal NAS e client per accordarsi sui parametri da usare a livello IP.

- **L2TP (nato per Provider Provision) :** usato per creare un tunnel fra cliente e VPN così da effettuare la negoziazione.
  Il LAC è il dispositivo che gestisce i pacchetti LCP mandati da vari utenti (anche in diverse aziende) e apre il tunnel L2TP che arriva fino all'LNS dell'azienda VPN. Il LAC si trova nel NAS (soluz. Provider provision) o nella stazione dell'utente (soluz. Customer provision).
  Ogni tunnel L2TP può contenere diverse sessioni per diversi utenti (Session ID), inoltre vengono contati i pacchetti totali e inviati nel tunnel così da renderlo affidabile. L2TP può essere imbustato anche dentro pacchetti diversi da IP, come UDP.
- **PPTP (nato per Customer Provision):** le trame PPP sono imbustate in pacchetti IP usando GRE.

Protocolli per Sicurezza IPSEC:

- **Authentication Header Protocol (AH):** l'header AH è un'intestazione aggiuntiva che contiene Digest e info varie, si inserisce in un pacchetto IP ("protocol=51") per autenticarlo. Se il pacchetto viene modificato, l'AH se ne accorge.
- **Encapsulating Security Payload (ESP):** ricevitore e trasmettitore si mettono d'accordo su algortmi e chaivi da usare, per poi avviare una sessione SECURITY ASSOCIATION a cui è associato un Security Parameter Index (SPI). Tale protocollo cripta e autentica il payload dei pacchetti.

Modalità di IPSEC:

- **Transport mode:** viene messo un IPSEC header e un IPSEC trail per rendere sicuro il payload a livello trasporto
- **Tunnel mode:** viene messo un IPSEC header e un IPSEC trail per rendere sicuro il payload e l'header a livello IP

Protocolli negoziazione chiavi IPSEC:

- **Security Associacion (SA):** insieme di dati che 2 stazioni usano per comunicare in modo sicuro. Per ogni comunicazione sono scelte 3 chiavi e 3 algoritmi (2 di autenticazione e 1 di cifratura) usando AH. Ogni SA è identificata da un numero Security Parameter Index (SPI) necessario per capire gli algoritmi da usare.
- **Internet Key Exchange (IKE):** insieme di protocolli per negoziare le chaivi e i SA

VPN Gateway Poisoning: viene messo un firewall prima del VPN Gateway (per assicurare l'accesso solo a certi utenti e in certe porte) e un firewall dopo (per vedere il traffico decriptato e proteggere la rete da virus e minacce).
IP based VPN: alcune di queste VPN usano dei Router dedicati a fornire il servizio solo per un cliente, oppure dei router e/o link condivisi/virtuali.
MPLS based VPN: tali reti permettono di creare connessioni tra i router che forniscono l'accesso alla VPN. I dispositivi di un utente che è connesso alla rete si chiamano Customer Edge (CE), i dispositivi del provider VPN che è al bordo della rete VPN si chiamano Provider Edge (PE) e mantengono info di routing su tutte le reti delle varie aziende collegate alla VPN. I PE costruiscono delle tabelle contenenti le etichette di tutte le destinazioni delle "Corporate Network" collegate al PE stesso. Per ogni nuova VPN aziendale che si connette ai PE bisogna annunciare il colore dell'etichetta da associargli.

- **Layer 2 VPN Pseudo Wire Emulatiuon End-to-end (PWE3):** tale rete configura degli LSP (link) fra i router della rete stessa tramite Hub And Spoke. Spesso vengono creati tanti LSP nello stesso percorso che collega 2 nodi (perché la rete VPN possiede tante reti aziendali in uno stesso tratto di strada), in questi casi i vari LSP vengono tutti incapsulati dentro un altro LSP dello stesso percorso.
- **Layer 3 VPN Virtual Router o RFC2547bis (BGP):** i nodi del service provider comunicano direttamente con i nodi delle reti aziendali (PE comunicano con CE)

BGP-based protocol: i PE scoprono i propri vicini solo perché gli vengono comunicati dai CE. Quindi i router PE sono configurati con delle liste di peer chiamate Peering Session e i protocolli BGP-based permettono di scambiare queste informazioni.

SSL: protocollo che prende in ingresso connessioni TCP e le rende TCP criptate. Dopo aver creato una connessione TCP fra client e destinatario, avviene un Handshake, cioè il destinatario manda un certificato al client, il client verifica tramite una certification authority che sia valido e genera una chiave simmetrica da mandare criptata (con la chiave inviata precedentemente dal server) al server.
SSL VPN: esso è migliore di IPSEC perché se vengono sfruttati bug ci si ritrova a livello utente e non kernel (come IPSEC), e peggiore perché se si sfruttano bug a livello 3 o 4 con IPSEC sono protetto mentre con SSL no. Il Port Forwarder è un apparato che riceve da un client sicuro dei dati tramite un protocollo con SSL (es: SPOP3) e poi li manda ad un suo server in zona protetta tramite un protocollo senza SSL (es: POP3) per elaborarli.

Reti Ottiche
Wavelength Division Multiplexing (WDM): consiste nel prendere diversi segnali e multiplexarli sulla stessa fibra.

- **DWDM:** prende tantissimi segnali sulla stessa fibra e li separa/demultiplexa
- **CWDM:** prende dei segnali a frequenze poco attenuate e li multiplexa

Lambda Switching: è un commutatore di segnali ottici che utilizzando degli specchi riesce a separare i segnali ottici basandosi sulla loro frequenza (principio fisico). Ci sono vari tipi di commutatori:

- **Core Ottico:** essi permettono di commutare il segnale, cioè spostarlo da una fibra in ingresso ad una in uscita senza trasformarlo in segnale elettrico, sfruttano proprietà fisiche. Essi introducono un po' di attenuazione.
- **Core Elettronico:** essi permettono di convertire il segnale ottico in elettrico e poi di mandarlo su un altra porta in uscita
- **Cross Connect** (commutano lentamente): essi sono dispositivi statici, la loro "configurazione" cambia solo in rari casi
- **Switch** (commutano velocemente): la loro "configurazione" cambia molto spesso
- **Wavelength Conversion:** convertono la lunghezza d'onda e permettono di raggiungere posti diversi usando pochi cavi, poiché normalmente ogni cavo sarebbe disposto a portare un segnale di 1 sola lunghezza d'onda e senza le Wavelength Conversion saremmo costretti ad usare tantissimi cavi, uno per ogni lunghezza d'onda. Quindi per brevi tratti (link) viene cambiata la lunghezza d'onda del saegna le ottico usando le camere di risonanza.