

VPN (Virtual Private Network): 2 tunnel end-points: macchina che si sta collegando, VPN Gateway.

Instaurazione 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 poichè 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).

Skype: Protocollo VoIP proprietario che usa molti concetti delle reti P2P (Peer To Peer). Si basa su nodi client e supernodi. Vantaggi: non è necessario avere indirizzi IP pubblici (i NAT non sono più un problema); come nelle

reti P2P il traffico è distribuito fra i vari nodi e non è necessario disporre di infrastrutture costose; la qualità del servizio (QoS) non è un prerequisito indispensabile in quanto la rete è abbastanza libera; la voce può essere trasmessa anche su TCP; buca i firewall grazie a TCP perchè la chiamata è spesso diretta e c'è una triangolazione attraverso relay (senza perdita della qualità); soppressione di pause ed eco; ottima gestione della voce; è free. Svantaggi: il codice è criptato; il debugging è impossibile; a livello aziendale si preferiscono soluzioni più sicure, aperte e gestibili come SIP; il singolo nodo può essere inaffidabile; problemi di intercettazione; overlay non influenzabile dall'utente (impossibile controllare chi sia il destinatario delle proprie informazioni).

Skype Overlay: Si basa su nodi client e supernodi (nodi client promossi che devono gestire circa 5Kbps di traffico aggiuntivo). I supernodi contengono l'indice dei nodi vicini e scambiano informazioni con loro. Il nodo client si collega ad uno o più supernodi salvati in un file locale. In mancanza di essi o in caso di connessione fallita ci si collega a un insieme di nodi predefiniti detti Bootstrap Servers. Il protocollo preferito è UDP, anche se in caso di rete con firewall si usa TCP e si cambiano spesso le porte.

H.323: VoIP. Protocollo di derivazione telefonica (per sistemi di comunicazione multimediali a pacchetto). Nato per estendere le videoconferenze alle LAN. Il Gatekeeper fa segnalazione e gestisce la comunicazione fra due o più client. La Multipoint Control Unit (MCU) gestisce i metodi di comunicazione e fa da mixer/switch dei flussi. I dati viaggiano su RTP affiancati da RTCP. H.323 fornisce la maggior parte dei servizi (autenticazione, localizzazione) ed è molto diffuso ma complesso, in via di abbandono a favore di SIP.

SIP (Session Initiation Protocol): VoIP. Protocollo di derivazione dati definito in ambito internet. Si utilizza un server SIP per l'autenticazione. Molto più semplice rispetto a H.323, nasce come protocollo di segnalazione (di tipo end-to-end, trasparente ai router) in grado di instaurare, modificare e terminare una sessione multimediale/dati. Il formato dei pacchetti è HTTP-like e la segnalazione può avvenire tramite TCP (per aggirare i firewall), UDP (molto semplice) e TLS (consente la cifratura). Sfrutta in modo identico a H.323 i protocolli RTP e RTCP e aggiunge una parte di controllo nella quale è importante SDP. Componenti SIP: Registrar Server; AAA Server; Location Server; Proxy Server; Redirect Server; Media Server; Media Proxy; MCU; Gateway.

RTP (Real-Time Protocol): Pensato per trasportare pacchetti audio/video. Non gestisce frammentazione e riassettaggio perchè i pacchetti sono molto piccoli. Non gestisce errori di trasmissione perchè la ritrasmissione non è necessaria. Non specifica il formato dei dati in modo da permettere un buon numero di codifiche. Completa il livello 4 insieme a UDP ed è usato solo dalle macchine alle estremità della comunicazione.

RTCP (Real-Time Control Protocol): Associato all'RTP per il monitoraggio e il controllo della comunicazione. Raccoglie informazioni sulla codifica.

SDP (Session Description Protocol): SIP. Definisce i parametri delle sessioni multimediali e in fase di INVITE trasporta diversi parametri utili (tipo media, codec, indirizzi, porte, ecc...).

Chiamata SIP (1 dominio): Struttura: Chiamante@dominio - Proxy SIP dominio - Ricevente@dominio. Messaggi: INVITE (Chiamante → Ricevente); 100 Trying (Proxy → Chiamante); 180 Ringing (Ricevente → Chiamante); 200 OK (Ricevente → Chiamante); ACK (Chiamante → Ricevente).

Chiamata SIP (2 domini): Struttura: Chiamante@dominio1 - Proxy SIP dominio1 - DNS Server - Proxy SIP dominio2 - Ricevente@dominio2. Messaggi: INVITE (Chiamante → Proxy1); 100 Trying (Proxy1 → Chiamante); DNS 'NAPTR' Query (Proxy1 → DNS); DNS 'NAPTR' Response (DNS → Proxy1); DNS 'SRV' Query + Response (Proxy1, DNS); DNS 'A'/'AAAA' Query + Response (Proxy1, DNS); INVITE (Proxy1 → Proxy2); INVITE (Proxy2 → Ricevente); 180 Ringing (Ricevente → Chiamante); 200 OK (Ricevente → Chiamante); ACK (Chiamante → Ricevente).

SIP REGISTER: La registrazione permette di autenticare un utente che accede a un dominio SIP e permette di associare la URI SIP che identifica l'utente all'UA SIP (host) su cui si trova in quel momento. In questo modo l'utente può essere raggiunto conoscendo solamente la URI SIP. Se l'utente si sposta dovrà registrarsi nuovamente. Campi più importanti dell'header di un messaggio SIP REGISTER: Command (riga di comando); Via (indica i sistemi SIP già attraversati dal messaggio); Max-Forwards (numero massimo di sistemi SIP che possono essere attraversati dal messaggio); Contact (URI temporanea che identifica la posizione corrente

dell'utente: IP+porta); To e From (contengono entrambi la URI che identifica l'utente SIP); Call-Id (identifica univocamente la transazione); CSeq (permette di sapere a quale richiesta si riferisce questa risposta); Expires (periodo di validità della registrazione, in secondi); Allow (metodi utilizzabili dal chiamante nella sessione SIP); User-Agent (tipo di software usato dallo UA); Authorization (credenziali di autenticazione); Content-Lenght (lunghezza del corpo messaggio, 0).

NAPTR: SIP. Tipologia di entry nel DNS, non necessariamente presente, che definisce quale protocollo di trasporto debba essere preferito per accedere al servizio (TCP, UDP, TLS/TCP, SCTP). DNS 'NAPTR' Response = Nomi servizi

Formato: domain-name | TTL | class | NAPTR | order | preference | flags | service | regexp | target

Esempio: mydomain.org | 43200 | IN | NAPTR | 0 | 0 | "s" | "SIPS+D2T" | "" | _sips._tcp.mydomain.org

SRV: SIP. Tipologia di entry nel DNS che definisce i parametri per accedere a un determinato servizio. DNS 'SRV' Response = Nomi server

Formato: _service._proto.name | TTL | class | SRV | priority | weight | port | target

Esempio: _sips._tcp.mydomain.org | 43200 | IN | SRV | 0 | 0 | 5060 | sip1.mydomain.org

A/AAAA: SIP. Tipologia di entry nel DNS che contiene un indirizzo (A: IPv4, AAAA: IPv6). DNS 'A'/'AAAA' Response = IP server

Formato: domain-name | TTL | class | type | address

Esempio: sip1.mydomain.org | 43200 | IN | A | 10.0.0.30

UA (User Agent): SIP. End-point della rete logica, utilizzato per creare o ricevere messaggi SIP e gestire una sessione SIP. Macchina a stati che evolve in dipendenza di messaggi SIP e registra informazioni rilevanti di un dialogo. Può fungere da client o da server.

UAC (User Agent Client): SIP. UA che manda richieste SIP.

UAS (User Agent Server): SIP. UA che riceve richieste SIP e ritorna delle risposte SIP.

Dialogo SIP: ha inizio quando si risponde positivamente al messaggio di INVITE del chiamante e termina con un messaggio di BYE.

Messaggi SIP: REGISTER, INVITE, ACK, CANCEL, BYE, OPTIONS.

Frame Relay: Standard d'interfaccia DCE-DTE (Data Communication Equipment - Data Terminal Equipment) che mette in comunicazione reti dati con reti LAN. Necessità alte velocità di lavoro. E' concepita su L2 dove effettua la commutazione di frame. Prevede un meccanismo di correzione degli errori tramite ritrasmissione ma solo sull'edge (frontiera), è soggetto a jitter quindi non va bene per trasportare voce.

CIR (Committed Information Rate): valore entro il quale si possono trasmettere fino a Bc bit alla velocità del collegamento fisico in ogni intervallo di tempo di durata Tc (per non intasare la rete). Il traffico che eccede il valore CIR non è conforme alla rete e quindi non è garantito. Bc = numero di bit che si introducono in un lasso di tempo Tc (Committed Burst Time). $Tc = Bc / CIR$.

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 è 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'invviare 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. E' 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:FFultime 6 cifre IP.

1)

Nel meccanismo del secchiello a gettoni si riesce a controllare:

- Il tempo di attraversamento massimo di un router.
- La gestione interna delle code con WFQ.
- La velocità minima di immissione dei dati.
- **IL burst size massimo e la velocità media di immissione dei dati.**

2)

Nell'architettura DiffServ, il PHB permette di:

- **Trattare in modo differenziato le varie classi di servizio.**
- Tenere sotto controllo il tempo di attraversamento massimo di singolo router per ciascun flusso che lo attraversa.
- Fornire la garanzia end-to-end della QoS richiesta da ciascun flusso.
- Garantire la QoS richiesta da ciascun flusso che lo attraversa un router.

3)

L'algoritmo RED (Random Early Access):

- Gestisce le code interne dei router trasmettendo a rotazione pacchetti delle varie code.
- Permette la marcatura in ingresso di traffici appartenenti a diverse classi
- **Gestisce le code interne dei router, iniziando a scartare i pacchetti con probabilità crescente quando la coda raggiunge una lunghezza minima.**
- Permette il controllo del massimo burst size.

4)

La telefonia su IP prevede:

- **L'uso di voice gateway per consentire la comunicazione con utenti collegati a reti tradizionali (POTS).**
- L'aggiornamento del cablaggio della rete IP in modo da collegare ogni utente telefonico tramite fibra ottica.
- Di dotare il calcolatore di ogni utente di voce su IP di un software di telefonia per comunicare con altri utenti di telefonia su IP e di un telefono tradizionale per comunicare con utenti di telefonia tradizionale.
- il protocollo SIP.

5)

Nel protocollo RTP, quando è possibile cambiare la codifica dei dati trasportati da un flusso?

- Una volta iniziata la trasmissione del flusso audio/video, non è più possibile cambiare la codifica
- é possibile cambiare la codifica, quando si effettua una opportuna segnalazione di controllo utilizzando RTCP.
- **é possibile cambiare la codifica ad ogni pacchetto inviato.**
- è possibile cambiare la codifica, solo se si sta utilizzando un RTP Mixer.

6)

La mobilità dell'utente viene trattata nel protocollo SIP?

- Non viene trattata
- Sì, all'utente non viene imposta nessuna limitazione sulla mobilità.
- Sì, a patto però che l'utente si ricollegli sempre con un indirizzo IP interno allo stesso provider.
- **Sì, a patto però che l'utente non cambi indirizzo IP durante una sessione SIP.**

(**APPROFONDIMENTO:** attraverso il Name Mapping è possibile riconoscere un utente SIP indipendentemente dal suo indirizzo IP)

7)

In un sistema VOIP basato su SIP, cosa può avvenire se effettuo una chiamata verso un destinatario non collegato a internet

- **Si può chiedere di essere avvertiti quando l'utente desiderato ritorna ad essere noto al sistema.**
- Si può solo tornare a provare più tardi.
- Si può essere avvertiti dell'apparizione dell'utente desiderato, solo se entrambi siamo nello stesso dominio SIP (abbiamo lo stesso operatore).
- Si può essere avvertiti dell'apparizione dell'utente desiderato, solo se lo stesso si ricollega da uno degli indirizzi IP noti al dominio SIP

(**APPROFONDIMENTO:** attraverso il Media Server, contenente le caselle vocali che fungono da segreterie telefoniche, è possibile lasciare un messaggio anche se il client destinatario non è collegato a internet. Egli riceverà il messaggio non appena si riconnetterà)
Umberto Actis Perino 05/07/10 15.14

8)

L'architettura MPLS (Multi Protocol label Switching) è caratterizzata da

- Un supporto particolarmente evoluto per fornire servizi a qualità garantita
- **Un diverso meccanismo (rispetto all'IP puro) per decidere l'interfaccia di uscita verso cui un pacchetto debba essere inoltrato**
- Protocolli di routing particolarmente veloci ad aggiornare le tabelle di routing in seguito a cambiamenti topologici in modo da recuperare molto velocemente i guasti.
- Terminali di rete intelligenti in grado di personalizzare i servizi ricevuti dalla rete.

9)

Gli LSP (Label Switch Path) nell'architettura MPLS (multi protocol label switching)

- Sono ottenuti riservando risorse nei nodi di rete in modo da garantire opportuna qualità del servizio alle applicazioni che li hanno creati.
- Costituiscono il percorso più breve verso una destinazione.
- Vengono creati (Set-Up) dalle applicazioni per il trasporto di pacchetti appartenenti ad una classe di equivalenza di inoltro (Forwarding Equivalence Class FEC)**
- **Vengono creati dai nodi di rete che si accordano sulle etichette da utilizzare per i pacchetti appartenenti ad una classe di equivalenza di inoltro (Forwarding Equivalence Class FEC)**

10)

Le soluzioni di VPN (virtual private network) di livello 3 attraverso una dorsale MPLS sono caratterizzate da:

- Livelli particolarmente alti di sicurezza grazie all'utilizzo di tecniche crittografiche
- **Buon livello di automatizzazione e integrazione tra la dorsale pubblica e le reti private.**
- Meccanismi di tunnelling di livello 3, ovvero all'interno di pacchetti IP.
- Gestione diretta da parte dell'utente, senza intervento dell'operatore.

11)

Il protocollo GRE serve per:

- **Incapsulare i pacchetti in altre intestazioni IP, in modo da poterle inviare su un tunnel**
- Garantire la riservatezza delle comunicazioni.
- Garantire l'autenticità dei pacchetti.
- Riservare della banda per la comunicazione.

12)

La caratteristica di una VPN di accesso centralizzata è che:

- **Il traffico non diretto alla VPN viene fatto passare comunque attraverso il VPN Gateway.**
- L'autenticazione dell'utente per l'accesso alla VPN viene delegato all'ISP.
- Il traffico non diretto alla VPN non è costretto a passare attraverso il VPN Gateway
- L'autenticazione dell'utente non viene fatta dal VPN Gateway

13)

Una delle caratteristiche principali delle linee Sonet/SDH è che:

- L'allocazione degli slot di trasmissione avviene secondo le esigenze del momento delle varie stazioni.
- **Le varie frequenze di trasmissione sono una multipla dell'altra.**
- La trasmissione avviene previa esecuzione di un meccanismo di contesa del canale che stabilisce chi ha diritto di trasmettere
- La trasmissione avviene a divisione di lunghezza d'onda

14)

In una rete Frame Relay, la minima unità di trasmissione è:

- **La trama del livello 2.**
- Il circuito virtuale
- Il pacchetto IP
- La cella da 53 bytes

15)

Nel protocollo IPV6:

- I protocolli di routing (ad esempio il formato dei pacchetti) non cambiano rispetto ad IPV4
- Il protocollo ARP viene inglobato in ICMPv6, ma mantiene esattamente lo stesso schema di funzionamento (richiesta broadcast, risposta unicast) precedente.
- **Esiste la possibilità, per una stazione su un segmento di rete, di autoconfigurarsi attraverso l'ascolto di messaggi di Router Advertisement.**
- Come in IPV4, IPV6 non prevede meccanismi di riconfigurazione dei router.

16)

Nell'IPV6 cosa sparisce dalle intestazioni, rispetto a IPV4?

- Il tempo di del pacchetto
- Gli indirizzi mittente e destinatario
- L'indicazione su quale sia l'intestazione successiva
- **Il checksum dell'intestazione**

17)

Lo schema di indirizzamento IPV6:

- Prevede esclusivamente indirizzi assegnati in modo univoco da un ente preposto.
- Prevede che ogni entità (es. azienda) si faccia assegnare globalmente un insieme di indirizzi, che diventano di sua proprietà a tempo illimitato.
- **Prevede che i primi 64 bit di un indirizzo siano normalmente identificati come il prefisso di rete, almeno sulle LAN.**
- Non prevede l'esistenza di indirizzi multicast.

18)

Gli indirizzi Link-local

- Sono validi all'interno di una organizzazione che li può utilizzare per assegnare indirizzi alle macchine

nelle varie sottoreti della propria internet (sono gli omologhi degli indirizzi privati di IPv4)

- Non possono essere assegnati ai router
- **Sono normalmente costruiti automaticamente dalla stazione a partire dall'indirizzo MAC della propria scheda, a cui si pre-pende un prefisso predefinito**
- Vengono utilizzati per identificare macchine che svolgono un certo servizio (ad esempio i server DNS)