Il routing (instradamento) è una funzione del livello Network del modello TCP/IP. Viene svolta da un dispositivo di rete chiamato router (o sistema intermedio), che per ottimizzare il percorso dei pacchetti deve conoscere ed eventualmente aggiornare una serie di informazioni. Solo sulla base di queste informazioni il router può avviare il processo di forwarding, stabilendo verso quale linea inviare il pacchetto.

Il Router

Un router è un dispositivo hardware dedicato a far comunicare reti differenti ed eterogenee, instradando i pacchetti nella giusta direzione. È connesso a due o più reti e decide il percorso che i dati devono seguire, basandosi sulle informazioni sullo stato delle reti collegate.

La funzione principale del router è quella di reindirizzare i messaggi tra reti di computer affinché possano raggiungere la destinazione finale. Le due attività fondamentali che svolge sono: la scelta del percorso migliore (routing) e l'invio dei pacchetti sull'interfaccia di uscita corretta (forwarding).

Un router, essendo un computer dedicato al routing, necessita di un sistema operativo. Dal punto di vista hardware deve avere almeno due schede di rete. Un router dotato di una scheda di rete verso la LAN e una verso la WAN può essere configurato come gateway, condividendo l'accesso a Internet per tutti i computer della rete locale. In questo caso, l'interfaccia del router che funge da gateway diventa la "via di uscita" degli host dalla LAN.

Routing Table

È fondamentale che il router costruisca nella propria memoria cache una tabella di instradamento (routing table), che gli consenta di memorizzare le informazioni necessarie a identificare il percorso ottimale verso le reti remote. Questa tabella è una lista di tutte le reti raggiungibili, con informazioni sulle modalità di instradamento.

Quando il router esegue il forwarding di un pacchetto, consulta la routing table per cercare l'indirizzo di rete corrispondente all'IP di destinazione.

Ogni riga (entry) della tabella di routing contiene quattro campi:

- l'indirizzo IP della rete raggiungibile (network address),
- l'indirizzo del router successivo (next hop),
- l'interfaccia del router a cui inoltrare il pacchetto (interface),
- la metrica, cioè un valore che rappresenta il costo del percorso. Il router sceglierà il percorso con il costo minore.

Routing Statico e Dinamico

Il funzionamento del router dipende da come viene creata la routing table. Se viene inserita manualmente dall'amministratore, si parla di routing statico, utilizzabile soprattutto in piccole reti. Se invece la tabella viene costruita automaticamente dal router in base alle informazioni ricevute tramite protocolli di routing, si parla di routing dinamico.

Protocolli di Routing

La gran parte dei protocolli che regolano il routing dinamico al giorno d'oggi utilizzano questi algoritmi:

- Distance Vector Routing
- Link State Routing

Distance Vector Routing

Il Distance Vector Routing è un algoritmo di routing usato dai router per trovare il percorso migliore verso le varie reti all'interno di una rete più grande

Ogni router mantiene una tabella di routing, dove annota:

- la distanza (in "hop", cioè il numero di router attraversati),
- e la direzione (cioè il router successivo) per raggiungere ogni rete.

Periodicamente, ogni router invia la propria tabella ai router vicini (i "vicini" sono quelli direttamente connessi). Quando un router riceve le tabelle dai vicini, confronta i percorsi e aggiorna la sua tabella se trova un percorso più breve.

Il Distance Vector Routing presenta diversi vantaggi. Prima di tutto, è un algoritmo semplice da implementare: ogni router ha bisogno solo di conoscere i suoi vicini e di scambiare con loro informazioni periodiche sulle distanze verso le varie reti. Questo lo rende adatto a reti di piccole dimensioni o con topologie stabili, dove le modifiche non sono frequenti. Inoltre, grazie alla sua bassa complessità, consuma poche risorse di calcolo e memoria, il che è vantaggioso per dispositivi con capacità limitate.

Tuttavia, ci sono anche alcuni svantaggi importanti. Uno dei principali è la lentezza nella convergenza: quando avviene un cambiamento nella rete, come il guasto di un collegamento, i router impiegano tempo per aggiornare le tabelle e trovare un nuovo percorso valido. Questo può portare a temporanei errori di instradamento. Un altro problema è il cosiddetto "count to infinity", dove i router continuano ad aumentare il numero di hop verso una destinazione irraggiungibile, senza accorgersi che il percorso non esiste più. Infine, il Distance Vector non ha una visione globale della rete, e questo lo rende meno efficiente in ambienti complessi o dinamici.

Link State Routing

Il Link State Routing è un tipo di algoritmo di routing che, a differenza del Distance Vector, si basa su una visione completa della rete. Ogni router non si limita a scambiare informazioni con i vicini, ma raccoglie dati sulla topologia dell'intera rete e costruisce una mappa completa, che usa per calcolare il percorso più breve verso ogni destinazione.

Ogni router scopre i propri vicini diretti (link state) ed invia queste informazioni a tutti gli altri router della rete tramite messaggi chiamati LSA (Link State Advertisements). Una volta che ogni router ha ricevuto tutte le LSA, può costruire un grafo della rete e applicare un algoritmo, di solito Dijkstra, per trovare i percorsi ottimali.

Il Link State Routing offre numerosi vantaggi, soprattutto in reti complesse o dinamiche. Uno dei principali è la velocità di convergenza: quando avviene un cambiamento nella rete, come un guasto o l'aggiunta di un nuovo collegamento, i router si aggiornano molto rapidamente grazie alla diffusione delle informazioni tramite i pacchetti LSA. Inoltre, ogni router ha una visione completa della rete, quindi può calcolare i percorsi migliori in modo molto, questo permette una gestione più efficiente del traffico, riducendo il rischio di loop o percorsi sbagliati. Un altro punto a favore è la maggiore stabilità e affidabilità, soprattutto in ambienti di grandi dimensioni o soggetti a frequenti cambiamenti.

Tuttavia, ci sono anche alcuni svantaggi. Il primo è la maggiore complessità: i router devono essere in grado di gestire più dati e di eseguire calcoli più complessi, quindi servono più risorse di memoria e CPU. Anche la configurazione e la manutenzione del protocollo possono essere più impegnative rispetto ad algoritmi più semplici come il Distance Vector. Inoltre, durante la fase di avvio o in caso di cambiamenti, la quantità di traffico di aggiornamento generata dai pacchetti LSA può essere elevata, soprattutto in reti molto estese.

Gli Autonomous System

Nei primi anni Ottanta, Internet era considerata un'unica rete in cui ogni router possedeva una tabella di instradamento con una voce per ogni rete raggiungibile e l'indirizzo del router da contattare. Questo modello centralizzato non era più sostenibile con la crescita della rete. Si decise quindi di suddividere Internet in più domini chiamati Autonomous System (AS), ciascuno costituito da un insieme di router e LAN organizzati secondo criteri topologici o amministrativi.

Ogni AS è identificato da un numero unico assegnato dall'IANA. I router che collegano diversi AS vengono spesso chiamati gateway, poiché svolgono il compito di inoltrare pacchetti da una rete verso l'esterno.

Comunicazione In e Tra AS

All'interno di un AS, le informazioni di raggiungibilità vengono scambiate tramite uno o più protocolli adattivi, detti Interior Protocol. Gli AS tra loro si scambiano informazioni di raggiungibilità attraverso protocolli chiamati genericamente Exterior Protocol.

Se un router deve inoltrare un messaggio verso un altro router appartenente allo stesso AS, si parla di comunicazione tra Interior Router (IR), e nella sua tabella sarà presente l'informazione necessaria. Se invece il messaggio è destinato a un router in un altro AS, verrà inoltrato a una coppia di Exterior Router (ER), uno per ciascun AS coinvolto. Ogni ER conosce le reti raggiungibili tramite i link che lo collegano ad altri ER, ma non conosce la struttura interna degli AS esterni.

Gli accordi tra gestori di diversi AS per definire politiche di transito e raggiungibilità sono chiamati accordi di peering.

Il Routing Gerarchico

Le tabelle di routing di grandi dimensioni possono causare seri problemi: saturano la memoria del router e rallentano le trasmissioni, costringendo la CPU a elaborazioni complesse per calcolare i percorsi ottimali. Inoltre, gli aggiornamenti frequenti delle routing table, dovuti ai continui scambi di informazioni tra numerosi router, aumentano il traffico di rete e riducono le prestazioni complessive.

Quando una rete diventa troppo grande e non è più possibile inserire tutte le destinazioni nelle tabelle dei router, è necessario riorganizzarla. In questi casi si adotta il principio del "divide et impera". In pratica, invece di mantenere un'unica rete estesa, la si suddivide in più reti di

dimensioni più contenute (dette regioni). All’interno di ciascuna regione, la comunicazione avviene secondo protocolli standard. Le connessioni tra regioni sono garantite da router dedicati che, a loro volta, comunicano tra loro come se facessero parte di una rete separata.

Questo approccio prende il nome di routing gerarchico. Secondo questo modello, la rete viene suddivisa in regioni interconnesse. Ogni router conosce in dettaglio solo la topologia della propria regione, ma non quella delle altre. Questo comporta un peggioramento delle prestazioni globali, poiché i percorsi non sono ottimizzati a livello interregionale.

I Protocolli di Routing: Interior ed Exterior

Interior Gateway Protocol (IGP)

I protocolli IGP sono utilizzati all’interno di un AS per regolare l’instradamento dei pacchetti. Sono chiamati protocolli intradominio. Possono essere classificati in base all’algoritmo che utilizzano:

- Distance Vector:
  - RIP (Routing Information Protocol): usa come metrica il numero di hop.
  - IGRP (Interior Gateway Routing Protocol): protocollo Cisco, supera i limiti di RIP supportando più metriche (banda, ritardo, carico, affidabilità).
  - EIGRP (Enhanced IGRP): sempre di Cisco, migliora IGRP pur mantenendone le metriche.
- Link State:
  - OSPF (Open Shortest Path First)
  - Integrated IS-IS (Intermediate System to Intermediate System): standard ISO e poi adottato anche da IETF.

Exterior Gateway Protocol (EGP)

I protocolli EGP sono utilizzati tra diversi AS, per questo si definiscono protocolli extradominio. Il principale protocollo utilizzato su Internet è il BGP (Border Gateway Protocol), nella sua versione attuale BGP-4. BGP utilizza un algoritmo di tipo Path Vector, simile al Distance Vector, ma invece di contare semplicemente gli hop, costruisce un vettore contenente l’elenco degli AS da attraversare per raggiungere una destinazione.

Lo Stack TCP/IP

Lo stack TCP/IP è composto da quattro livelli. È stato sviluppato prima della definizione del modello OSI, che avrebbe dovuto sostituirlo, ma con il tempo si è imposto come lo standard de facto, specialmente su Internet.

I due protocolli principali della suite TCP/IP sono IP (Internet Protocol), che opera al livello rete, e TCP (Transmission Control Protocol), che appartiene al livello trasporto. Quest'ultimo è responsabile della comunicazione end-to-end tra processi che si trovano su host differenti.

Servizi del Livello Trasporto

Il livello di trasporto consente a due processi su host diversi di comunicare direttamente. Questo livello offre un controllo completo end-to-end. Un protocollo di trasporto può gestire più connessioni simultanee verso lo stesso host, distinguendo a quale processo inviare ciascun messaggio grazie a meccanismi basati su porte e socket.

Le Porte e le Socket

Poiché su un host possono essere attivi più processi che generano richieste, è necessario un sistema per identificare correttamente il destinatario di ogni pacchetto. Per questo vengono utilizzate le porte, numeri a 16 bit assegnati dall'IANA.

Le porte sono suddivise in tre categorie:

- Well Known Ports: da 0 a 1023
- Registered Ports: da 1024 a 49151
- Dynamic/Private Ports: da 49152 a 65535

Ogni connessione è identificata da una quintupla formata da: protocollo, indirizzo IP del client, indirizzo IP del server, numero di porta del client, numero di porta del server. Questa struttura è detta association. La parte locale dell'associazione (protocollo, IP e porta) è chiamata socket. Le socket permettono di distinguere le comunicazioni tra diversi processi su uno stesso host.

Multiplexing e Demultiplexing

Tutti i protocolli del livello trasporto forniscono funzionalità di multiplexing e demultiplexing. Il multiplexing consiste nel raccogliere dati da diverse applicazioni, aggiungere un header e inviarli al livello rete. Il demultiplexing è il processo inverso: ricevere un segmento, esaminarne l'header e consegnare i dati al processo corretto.

I Principali Protocolli di Trasporto

I protocolli più usati in questo livello sono UDP (User Datagram Protocol) e TCP (Transmission Control Protocol). Le unità dati per questi protocolli sono rispettivamente il datagramma (TPDU per UDP) e il segmento (TPDU per TCP).

TCP

Il TCP è il protocollo più diffuso per il livello trasporto. È connection-oriented e affidabile, ed è utilizzato da applicazioni che necessitano di una trasmissione sicura, come FTP (trasferimento file), SMTP (posta elettronica) e HTTP (pagine web).

Il Segment TCP è composto da un header (20 byte) con al suo interno:

- Numero porta sorgente
- Numero porta destinazione
- Sequenza di numeri
- Acknowledgement number
- Lunghezza header
- Checksum, window size
- Urgent pointer

Poi troviamo il parametro options e data.

Instaurazione e Abbattimento Sessione TCP

Instaurazione di una Connessione TCP – Three-Way Handshake

Affinché possa essere instaurata una connessione TCP tra due host, è necessario che l'host ricevente acconsenta mediante una sequenza composta da tre fasi, nota come Three-Way Handshake:

1. Host 1 invia un segmento TCP con il flag SYN impostato a 1. Viene inoltre generato un numero di sequenza iniziale (sequence number) scelto in modo casuale, indicato con X.
2. Host 2, se accetta di stabilire la connessione, risponde con un segmento in cui:
   - il flag SYN è impostato a 1
   - il flag ACK è impostato a 1
   - l'Ack Number è posto a X + 1
   - viene generato un nuovo numero di sequenza Y
3. Host 1 risponde con un segmento contenente:
   - flag ACK impostato a 1
   - l'Ack Number impostato a Y + 1

A questo punto la connessione è considerata stabilita e si può procedere con la trasmissione dei dati.

Trasferimento Dati: Affidabilità e Controlli

Durante la fase di trasmissione:

- TCP garantisce una trasmissione affidabile e ordinata dei dati
- sono attivi meccanismi di controllo degli errori, controllo del flusso (flow control) e controllo della congestione (congestion control)
- ogni segmento ricevuto viene confermato (ACK) e i numeri di sequenza aiutano a mantenere l'ordine dei dati ed evitare duplicazioni o perdite

Chiusura della Connessione TCP – Double-Way Handshake

Poiché la connessione TCP è bidirezionale, la chiusura avviene in maniera indipendente per ciascuna direzione. La procedura di chiusura prende il nome di Double-Way Handshake:

1. Un host (es. Host 1) invia un segmento TCP con il flag FIN impostato a 1
2. Host 2 risponde con un segmento contenente:
   - flag ACK = 1
   - l'Ack Number = X + 1
3. Se Host 2 ha ancora dati da trasmettere, continua a farlo. Quando termina, invia un segmento con FIN = 1 e numero di sequenza Y
4. Infine, Host 1 conferma con ACK = 1 e Ack Number = Y + 1

Controllo della Congestione in TCP

Per individuare una congestione il TCP utilizza dei timer per misurare il tempo trascorso tra l'invio di un segmento e la ricezione del relativo ack. Se questo non arriva entro un determinato tempo si genera un timeout.

TCP ipotizza che la perdita di dati sia per una congestione della rete e agisce di conseguenza. Tuttavia, esistono versioni di TCP che tengono conto anche di errori di trasmissione.

TCP implementa una serie di algoritmi, specificati nella RFC 5681, per il controllo della congestione. Tutti fanno uso della finestra di congestione, che indica il massimo numero di byte non confermati che possono trovarsi ancora nella rete.

```
maxWindow = min(FinestraDiCongestione, FinestraDiRicezione)
```

Dove:

- FinestraDiCongestione: max numero di byte che la rete può trasmettere
- FinestraDiRicezione: quanti byte il destinatario è in grado di ricevere
- maxWindow: minimo tra i due valori, usato per decidere quanti byte trasmettere

Dei 4 algoritmi utilizzati, si analizzano:

- Slow Start: la finestra di congestione cresce esponenzialmente fino al threshold (es. 64KB)
- Congestion Avoidance: oltre il threshold, la crescita è lineare
- In caso di timeout: la soglia viene dimezzata e la finestra torna al valore iniziale

Controllo di Flusso e degli Errori

Il protocollo Sliding Window è un meccanismo usato da TCP per garantire un controllo efficiente del flusso dei dati tra mittente e destinatario.

Permette di inviare più byte consecutivi senza attendere un ACK per ognuno, entro una finestra.

La dimensione della finestra dipende dallo spazio disponibile nel buffer del ricevente. In caso di buffer pieno, la finestra si restringe; se c'è spazio, si allarga.

Ogni segmento ha un numero di sequenza, così TCP può rilevare l'ordine dei pacchetti e accorgersi di eventuali perdite, ritrasmettendo solo i dati mancanti.

UDP

UDP (User Datagram Protocol) offre solo le funzionalità di multiplexing/demultiplexing. Il servizio è connectionless e non affidabile.

Il datagram UDP si compone di:

- source port number
- destination port number
- length (o checksum coverage length per UDP-Lite)
- checksum
- data

UDP-Lite

UDP-Lite è una versione modificata di UDP che accetta pacchetti anche se parzialmente corrotti.

Permette di proteggere con il checksum solo una parte del pacchetto. Utile per applicazioni come streaming video, audio o VoIP, dove è meglio ricevere qualcosa, anche se imperfetto, piuttosto che perdere tutto.

Confronto tra UDP e TCP

TCP e UDP condividono:

- le funzionalità di multiplexing/demultiplexing
- l'uso delle porte

TCP è da preferire quando serve affidabilità e integrità dei dati. UDP è indicato quando le prestazioni sono più importanti dell'assenza di perdite.

Il principale protocollo usato per la configurazione degli host è il DHCP (Dynamic Host Configuration Protocol). Per la gestione della rete si usa invece il protocollo SNMP (Simple Network Management Protocol).

Il DHCP

Quando nelle reti si diffusero la tecnologia wireless e l'uso di computer portatili, in ambito IETF fu definito il protocollo DHCP (Dynamic Host Configuration Protocol), la cui specifica si trova in RFC 2131.

Tramite DHCP, oltre all'indirizzo IP, un host può ricevere altri parametri di configurazione:

- subnet mask
- default gateway: per esempio l'indirizzo IP del router che connette la subnet alla rete Internet. A questo sono inviati i pacchetti IP aventi indirizzo di rete del destinatario diverso da quello del mittente
- DNS Server preferito
- DNS Server alternativo

Configurazione Modalità

L'amministratore di rete può configurare, per ogni subnet e per ogni host, la modalità con cui il DHCP Server risponderà alle richieste dei client scegliendo fra 3 diversi tipi di configurazione.

- Configurazione manuale: è possibile assegnare un indirizzo IP specifico a un host, inserendolo manualmente nel DHCP Server; di regola si utilizza per macchine come router e server che si trovano stabilmente in una rete o per host che necessitano di un indirizzo permanente
- Configurazione automatica: il DHCP Server assegna in modo automatico un indirizzo IP permanente a ogni host che si collega alla rete (si differenzia dalla configurazione dinamica per l'assenza del tempo di lease)
- Configurazione dinamica: il DHCP Server assegna un indirizzo IP a un host per un tempo limitato (tempo di lease) in base alla lease length policy stabilita. Allo scadere del tempo di lease il client può richiederne il rinnovo o richiedere l'assegnazione di un nuovo indirizzo

L'Architettura Client Server DHCP

Un solo DHCP Server è solitamente in grado di soddisfare le esigenze operative relative all'assegnazione degli indirizzi IP e al setting dei parametri di configurazione sui client della rete locale. In condizioni normali il carico che deriva da queste attività non è particolarmente pesante.

Un DHCP Server può anche essere configurato per servire più subnet, per due scopi:

- fault-tolerance: per cui in genere è opportuno inserire un secondo DHCP Server come backup, così da mantenere il servizio sempre attivo
- bilanciamento del carico di lavoro: così da diminuire i tempi di risposta del server. In tal caso, alla richiesta di un client per l'assegnazione di un indirizzo IP possono rispondere più di un DHCP Server

Quando un DHCP Server è responsabile dell'indirizzamento su una subnet diversa dalla propria è necessario introdurre un relay agent (agente di ritrasmissione), ossia una macchina che non è né un server né un client, ma svolge un ruolo di intermediario occupandosi di facilitare la comunicazione tra client e server attraverso più reti.

La Comunicazione tra DHCP Client e DHCP Server

I messaggi di trasporto tra DHCP Client e DHCP Server sono di due tipi: richieste (request) e risposte (reply). Il protocollo di trasporto utilizzato è UDP e utilizza le porte 67 per il server e 68 per il client.

Il Pacchetto DHCP

- op (operation code)
- htype (hardware type)
- hlen (Hardware address length)
- hops (Hops count)
- Transaction ID (xid)
- Seconds (secs)
- Flags (flags)
- Client IP address (ciaddr)
- 'Your' (client) IP address (yiaddr)
- Server IP address (siaddr)
- Gateway IP address (giaddr)

- Client hardware address (chaddr)
- Server host name (sname)
- Boot file name (file)
- Options

Assegnazione degli Indirizzi

La comunicazione tra il nuovo host e il server, al fine di ottenere i dati per la configurazione di rete, avviene in 4 fasi:

1. Ricerca del DHCP Server: quando un nuovo host si connette alla rete, per ottenere un IP, invia un messaggio di broadcast chiamato DHCP Discover. Questo messaggio viene inviato a tutti i dispositivi sulla rete locale, perché l'host non conosce ancora l'indirizzo del server DHCP che possa assegnargli una configurazione IP
2. Offerta al DHCP Client: quando il server DHCP riceve il messaggio di Discover, risponde con un messaggio chiamato DHCP Offer che contiene una proposta di configurazione per il client: un indirizzo IP disponibile, la subnet mask, il gateway, i DNS e altre informazioni utili
3. Richiesta al DHCP Server: dopo aver ricevuto le offerte, il client sceglie una delle proposte e invia un messaggio chiamato DHCP Request, con cui il client comunica al server DHCP che ha accettato l'offerta. Anche questo messaggio è un broadcast, così che anche gli altri server DHCP sappiano che la loro offerta è stata rifiutata
4. Conferma al DHCP Client: infine, il server DHCP riceve la richiesta e risponde con un messaggio chiamato DHCP ACK, con cui il server conferma l'assegnazione dell'indirizzo IP al client e ribadisce tutte le informazioni necessarie per la configurazione della rete

Problematiche di Sicurezza

Il DHCP utilizza i protocolli UDP e IP che sono intrinsecamente insicuri. Sono due i principali problemi di sicurezza:

- DHCP Server non autorizzati: un DHCP Server abusivo potrebbe inserirsi e inibire gli host o configurarli per azioni fraudolente
- DHCP Client non autorizzati: un host potrebbe danneggiare la rete, oppure esaurire gli indirizzi a disposizione e bloccare nuovi accessi

Per ovviare al problema si possono implementare meccanismi di sicurezza ai livelli più bassi, inoltre si potrebbe usare IPsec per rendere sicuro il livello Network.

Il DNS

Il DNS consente agli utenti della rete di usare dei nomi al posto dell'indirizzo IP. È un database distribuito usato dagli applicativi del TCP/IP per il mapping tra nomi e indirizzi IP. Il DNS è formato da 3 componenti principali:

- Domain Name Space, specifica la struttura ad albero dei nomi di dominio ed è suddiviso in 3 tipi di domini:
  - domini radice
  - domini intermedi
  - domini foglia
- Name Server, un processo applicativo con il ruolo di server che contiene informazioni su alcune parti del Name Space chiamate zone
- Resolver, un programma con il ruolo di client che ottiene informazioni dal Name Server

Come Funziona il DNS

L'albero gerarchico del DNS è realizzato mediante base di dati distribuita, cosa che garantisce il funzionamento della rete. Se tutte le informazioni fossero memorizzate su un unico server e questo si guastasse si fermerebbe infatti tutta la rete Internet.

Lo spazio dei nomi del DNS è stato suddiviso in zone disgiunte, ognuna con un Name Server principale (DNS primario) e dei Name Server secondari (DNS secondario) che attingono al principale.

I client che accedono ai Name Server sono i resolver. Se il Resource Record è authoritative per la zona richiesta, il DNS Server risponderà direttamente, in caso contrario farà una ricerca nello spazio dei nomi. Questo processo si chiama risoluzione dei nomi.

Problematiche di Sicurezza del DNS

Il DNS dal punto di vista della sicurezza è critico sotto vari punti di vista:

- non è autenticato: l'informazione richiesta potrebbe arrivare non dal DNS Server corretto ma da un'altra macchina
- è molto lento, quindi è possibile che qualcuno intercetti la richiesta destinata a un DNS Server e risponda al suo posto (spoofing)
- non offre meccanismi per proteggere l'integrità delle informazioni distribuite

Proprio per il ruolo critico che il DNS ricopre nell'internet, l'ICANN ha evidenziato la necessità di stabilire metriche e modalità per il controllo del DNS, individuando 5 indicatori importanti: coerenza, integrità, velocità, disponibilità e robustezza

Internet Security

Con la diffusione di Internet, la sicurezza delle informazioni è diventata una questione fondamentale. È essenziale proteggere i dati sia a livello fisico che durante la loro trasmissione da un nodo all'altro. Per garantire questa protezione, sono state sviluppate diverse misure di sicurezza, note complessivamente come Internet Security.

Alla base dell'Internet Security vi è la Raccomandazione X.800, che definisce un insieme di requisiti di sicurezza che ogni sistema deve soddisfare:

- Autenticazione: assicurare l'identità dei soggetti coinvolti nella trasmissione
- Controllo degli Accessi: proibizione dell'uso di una risorsa da parte di soggetti non autorizzati
- Confidenzialità: protezione della riservatezza dei dati, poiché nessun soggetto terzo vi deve accedere durante la trasmissione
- Integrità: certezza che i dati non siano stati alterati da soggetti non autorizzati
- Non ripudiabilità: protezione contro la negazione di un soggetto coinvolto nella trasmissione

La strategie di sicurezza principali nella trasmissione dei dati si incentrano o sull'oscurazione o sul confinamento. Qualsiasi sia quella adottata, nella progettazione del servizio di sicurezza si deve:

1. Utilizzare un algoritmo per trasformare i dati in chiaro in dati crittografati
2. Generare le chiavi da utilizzare per crittografare e decrittografare
3. Sviluppare un metodo per la condivisione sicura delle chiavi
4. Specificare un protocollo che permetta di utilizzare sia l'algoritmo che le chiavi in modo sicuro

La Crittografia

La crittografia è l'insieme di tutte le procedure che hanno lo scopo di nascondere il significato di un messaggio tranne che al legittimo destinatario. Alla base vi è un cifrario, che ci permette di trasformare ogni carattere del testo in chiaro. Per cifrare un testo occorrono un algoritmo di cifratura e una chiave per decifrarlo.

Uno dei cardini della teoria della crittografia è il principio di Kerckhoffs, secondo il quale la sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave.

Esistono molti sistemi di crittografia, si possono classificare in vario modo:

1. Tipo di operazioni usate per cifrare il testo:
   - Crittografia a sostituzione
   - Crittografia a trasposizione
2. Modo in cui il testo in chiaro viene elaborato:
   - Crittografia a blocchi
   - Crittografia a flusso
3. Numero di chiavi distinte utilizzate:
   - Crittografia a chiave simmetrica
   - Crittografia a chiave asimmetrica

Crittografia Simmetrica e Asimmetrica

La crittografia a chiave simmetrica si basa sull'utilizzo di una sola chiave usata sia per cifrare che per decifrare. La crittografia a chiave asimmetrica utilizza due chiavi per ciascun soggetto, una privata e una pubblica.

A seconda dell'uso delle chiavi:

- Confidenzialità: viene utilizzata la coppia di chiavi del destinatario
- Autenticazione: viene utilizzata solo la coppia di chiavi del mittente
- Tutte: utilizzando entrambe le coppie di chiavi

Le due chiavi devono essere matematicamente correlate ma non ricavabili l'una dall'altra.

Gli Algoritmi DES e Triple DES

Il DES (Data Encryption Standard) è un algoritmo sviluppato negli anni '70 e basato su:

- Confusion: rende confusa la relazione tra testo in chiaro e testo cifrato
- Diffusion: altera la struttura del testo in chiaro

Funzionamento:

- Input: blocchi da 64 bit, chiave a 56 bit
- Permutazione iniziale
- Suddivisione in due semiblocchi da 32 bit (L_0, R_0)
- Generazione di 16 chiavi da 48 bit
- Operazioni di espansione, XOR, compressione con S-box
- Permutazione finale
- Inversione dei semiblocchi e decrittazione simmetrica (DES^{-1})

Triple DES:

- Applica il DES tre volte con tre chiavi diverse (Crypt → Decrypt → Crypt)
- Usa chiavi da 192 bit (128 effettivi)

Altri algoritmi derivati:

- IDEA: blocchi da 64 bit, chiave da 128
- AES: blocchi da 128 bit, chiavi da 128, 192, 256
- CAST: blocchi da 64 o 128 bit, chiavi da 128 o 256

L'algoritmo RSA

RSA è un algoritmo a chiave pubblica, sicuro grazie alla difficoltà della fattorizzazione.

Generazione chiavi:

- Scegliere p e q
- Calcolare n = p × q e φ(n) = (p − 1)(q − 1)
- Scegliere e coprimo con φ(n)
- Calcolare d tale che d × e ≡ 1 mod φ(n)
- Pubblica: (e, n), Privata: (d, n)

Crittografia:

- c = m^e mod n

Decrittografia:

- m = c^d mod n

RSA è sicuro ma lento. Oggi è usato soprattutto per lo scambio della chiave simmetrica.

La Firma Digitale e gli Enti Certificatori

La firma digitale ha valore legale e si basa su un sistema a chiavi asimmetriche. Per garantire l'identità del firmatario intervengono i certificatori, che rilasciano un certificato digitale.

Formati riconosciuti:

- pkcs#7 (p7m): usato dalla PA
- PDF: accordo Adobe–CNIPA del 2006 (RFC 3778)
- XML: molto usato in ambito bancario e sanitario

Il processo di firma digitale:

- Si crea un'impronta (message digest) con una funzione di hash
- Si firma questa impronta con la chiave privata del mittente

Per firmare serve un kit composto da:

- Dispositivo sicuro

- Software di firma

Spanning Tree Protocol

Le reti locali moderne sono suddivise in segmenti più piccoli collegati tramite switch o router. Questo permette di isolare il traffico, ridurre i domini di collisione e migliorare la banda disponibile per ogni dispositivo. Per garantire affidabilità, spesso si introducono collegamenti ridondanti, ma questi possono causare loop nella rete e generare broadcast storm, cioè un sovraccarico di traffico che rallenta o blocca la rete. Per evitare questi problemi si usa il protocollo STP (Spanning Tree Protocol), definito dallo standard IEEE 802.1.

STP costruisce una topologia logica ad albero che lascia attivi solo i collegamenti necessari tra due dispositivi e di conseguenza disattiva quelli ridondanti a livello logico (ma non fisico), da usare solo in caso di guasto.

Ogni switch invia messaggi chiamati BPDU (Bridge Protocol Data Unit) per:

- selezionare lo switch root (radice dell'albero)
- calcolare il percorso più breve verso la root
- eleggere il designated switch (quello più vicino alla root su ogni segmento)
- scegliere la root port per ogni switch (la porta con il percorso migliore verso la root)

Le porte coinvolte nello Spanning Tree sono le designated port (attive nel traffico) e le altre porte bloccate per prevenire i loop. Gli stati possibili di una porta STP sono:

- blocking: riceve solo BPDU
- listening: partecipa alla costruzione della topologia
- learning: impara gli indirizzi MAC
- forwarding: invia e riceve traffico
- disabled: disattivata manualmente

Il problema principale dell'STP classico è il tempo di convergenza (30–50 secondi), troppo lungo per le moderne LAN. Per migliorarlo, nel 2001 è stato introdotto il Rapid Spanning Tree Protocol (RSTP), standard IEEE 802.1w, che riduce significativamente i tempi di riconfigurazione della rete.

Le Reti Locali Virtuali

Per migliorare l'efficienza e la gestione delle reti, oltre a separare i domini di collisione, è utile anche dividere la rete in più domini di broadcast. Un dominio di broadcast è un gruppo di dispositivi che riceve un messaggio broadcast inviato da uno di essi. In una configurazione base, tutti gli host collegati a uno switch appartengono allo stesso dominio di broadcast. Tuttavia, in reti con molti dispositivi, i messaggi broadcast possono generare traffico eccessivo. Per evitare questo problema, si utilizzano due soluzioni:

- VLAN (Virtual LAN): creano sottoreti logiche all'interno della rete fisica, permettendo di suddividere i domini di broadcast senza modificare la topologia fisica
- Switch Layer 3: integrano funzionalità di routing, permettendo la comunicazione tra VLAN diverse senza bisogno di router esterni

Le VLAN offrono vari vantaggi come migliorare le prestazioni e la sicurezza della rete, semplificano l'aggiunta, lo spostamento e la gestione degli host e riducono i costi.

Una VLAN può essere creata in vari modi:

- per gruppi di porte: in base alla porta dello switch a cui è collegato un dispositivo (metodo più comune)
- per indirizzi MAC: in base all'indirizzo fisico del dispositivo (meno usato perché difficile da gestire)
- per protocolli: in base al protocollo di rete utilizzato

Esistono due tipi di collegamenti nelle VLAN:

- access link: collegamento che fa parte di una sola VLAN, usato per connettere dispositivi finali
- trunk link: collegamento punto-punto tra switch o altri apparati, trasporta traffico di più VLAN (fino a 4096)

In una configurazione con VLAN e trunking, le porte di uno switch possono essere configurate come:

- Access port
  - Collegate a dispositivi finali (PC, stampanti, telefoni IP)
  - Appartengono a una sola VLAN
- Trunk port
  - Collegate ad altri switch, router o server
  - Trasportano traffico di più VLAN contemporaneamente

In alcuni casi, è possibile configurare le porte con modalità dinamiche (es. Dynamic Trunking Protocol su switch Cisco), ma per motivi di sicurezza e controllo si preferisce la configurazione manuale.

Per semplificare la gestione centralizzata delle VLAN in reti complesse si usa il VTP (VLAN Trunking Protocol), che sincronizza le configurazioni tra switch. Gli switch VTP possono operare in tre modalità:

- VTP server: gestisce e distribuisce le configurazioni VLAN
- VTP client: riceve e applica le configurazioni dai server
- VTP transparent: inoltra le informazioni VTP ma non modifica la propria configurazione

Firewall

Il firewall è una linea di difesa che filtra tutti i pacchetti sia in entrata che in uscita da una rete, secondo regole prestabilite che contribuiscono alla sicurezza della rete stessa. Questo si può comunemente realizzare tramite un PC, l'apposito software e le Access Control List che servono per configurarlo. I firewall si possono distinguere in 3 categorie in base al livello dello stack TCP/IP in cui operano:

- Application Level Firewall: intercetta le trasmissioni a livello Application valutando il contenuto applicativo dei pacchetti, come i Proxy;
- Packet Filter Firewall: lavora a livello Network e Transport, è più veloce dell'Application perché controlla solo l'header;
- Stateful Packet Inspection Firewall: agisce solo a livello Transport, controlla e analizza tutto il pacchetto dati, compila una tabella con lo stato delle connessioni;

ACL

L'Access Control List o ACL è un insieme di istruzioni da applicare alle interfacce di un router allo scopo di gestire il traffico. Le ACL forniscono un livello base di sicurezza, aumentano le performance della rete e stabiliscono quali tipi di traffico possono essere trasmessi.

Le ACL vengono elaborate in ordine, e appena una condizione è soddisfatta il pacchetto viene eliminato o inoltrato. L'ultima istruzione di ogni ACL è una negazione implicita 'deny ip any any'.

Le ACL si applicano specificando la direzione (in ingresso o uscita):

- Ingresso: traffico che arriva al router prima della tabella di routing;
- Uscita: traffico già elaborato per l'inoltro;

Tipi di ACL:

- Standard ACL (1-99): controllano solo l’indirizzo IP sorgente;
- Extended ACL (100-199): controllano indirizzi sorgente/destinazione, protocolli TCP/UDP, numeri di porta;

ACL possono essere:

- Numbered: identificativo numerico;
- Named: identificativo con nome;

Ogni router può avere una ACL per ogni protocollo, interfaccia logica e direzione.

Posizionamento:

- Extended ACL: vicino alla sorgente;
- Standard ACL: vicino alla destinazione;

Configurazione di ACL standard numeriche

```
Router(config)#access-list numero_ACL deny|permit ip_sorgente maschera_wildcard
```

Configurazione di ACL extended numeriche

```
Router(config)#access-list numero_ACL [deny|permit] protocollo ip-sorgente wildcard ip-destinazione wildcard
condizione
```

Configurazione di ACL standard con nome

```
Router(config)#ip access-list standard nome_ACL
```

```
Router(config-std-nacl)# [deny|permit] ip-sorgente
```

Configurazione di ACL extended con nome

```
Router(config)#ip access-list extended nome-ACL
Router(config-ext-nacl)# deny|permit protocollo ip_sorgente wildcard_mask ip_destinazione wildcard_mask condizione
```

Proxy

Un proxy è un programma che si interpone tra client e server. Riceve la richiesta dal client, la inoltra al server e poi ritorna la risposta al client. Lavora a livello Application e utilizza tecniche come NAT e PAT. Collocato vicino al client, migliora le prestazioni e riduce il consumo di banda.

Funzioni principali:

- Connettività;
- Privacy;
- Caching;
- Monitoraggio;
- Amministrazione;
- Filtraggio;
- Restrizioni (DMZ);

Topologie di utilizzo:

- Single Proxy Topology: un solo proxy per tutta la rete;
- Multiple Proxy Vertically Topology: proxy secondari si collegano a uno primario;
- Multiple Proxy Horizontally Topology: bilancia il carico tra proxy di pari livello;

NAT e PAT

NAT (Network Address Translation) è una tecnica con cui il router sostituisce l'indirizzo IP del pacchetto. Permette a reti private con indirizzi locali di accedere a Internet tramite un unico IP pubblico.

Vantaggi del NAT:

- Riduce il numero di IP pubblici necessari;
- Mantiene la configurazione degli host;
- Offre sicurezza e flessibilità;

Tipi di NAT:

- Static NAT: un solo IP pubblico usato per tutte le connessioni
- Dynamic NAT: scelta dinamica di un IP pubblico tra un insieme disponibile
- PAT (Port Address Translation): utilizza un solo IP pubblico con porte diverse

NAT in IPv6:

- Dual-stack: doppio stack IP per supportare IPv4 e IPv6;
- Conversion: traduzione tramite NAT-PT;
- Tunneling: incapsulamento IPv6 in IPv4;

Tipi di tunneling:

- 4to6: pacchetti IPv6 incapsulati in IPv4;
- 6to6: tunnel IPv6 attraverso rete IPv4, usato in reti locali;

Il PAT permette di usare un solo IP pubblico per oltre 64.000 connessioni private. Cambia la porta, mantenendo lo stesso IP.

DeMilitarized Zone

Per migliorare la sicurezza, le reti si dividono in zone:

- Zona LAN: rete privata interna;
- Zona WAN: parte esterna collegata a Internet;

DMZ (DeMilitarized Zone) è una terza zona che separa LAN e WAN, limitando il traffico tra loro. Usata per pubblicare servizi all'esterno (SMTP, Webmail, Application Server) senza esporre la LAN.

Tipi di DMZ:

- Vicolo cieco: un firewall con tre interfacce (LAN, WAN, DMZ);
- Zona cuscinetto: due firewall, uno tra WAN e DMZ, l'altro tra DMZ e LAN;

VPN – Virtual Private Network

Esistono sia reti private vere e proprie che collegano più sedi in una rete aziendale tramite canali dedicati, sia reti private virtuali. I vantaggi delle reti private sono:

- Larghezza di banda sempre disponibile;
- Nessun problema di accesso;
- Nessuna congestione del traffico;
- Sicurezza e prestazioni ottimali;

Abbiamo anche numerosi svantaggi:

- Alti costi ricorrenti di gestione;
- Lunghi tempi di configurazione;
- Mancanza di scalabilità;
- Rischio di blocco del canale in caso di guasto;

Per ovviare a questi problemi si ricorre alle reti private virtuali. Una VPN (Virtual Private Network) è una rete privata creata all'interno di un'infrastruttura di rete pubblica come Internet. Il rischio di blocco della rete è minimo grazie all'alto grado di ridondanza offerto dalla rete pubblica. Purtroppo vi sono anche delle problematiche, le principali sono 3:

- variabilità di tempo di trasferimento;
- controllo degli accessi;
- sicurezza delle trasmissioni;

Il primo problema viene affrontato tramite l'utilizzo delle WAN, il secondo e il terzo grazie ai fattori di autenticazione, cifratura e tunneling. Esistono due tipi di VPN in commercio, le Remote-access VPN e le Site-to-site VPN.

Remote-Access VPN

Una remote-access VPN consente ai singoli utenti di stabilire connessioni sicure con la LAN aziendale remota, vi sono due componenti indispensabili per la sua realizzazione, il Server NAS (Network Access Server) è il primo, esso può essere o un server dedicato o un'applicazione software in esecuzione su un server condiviso. Attraverso esso l'utente si connette a Internet e può utilizzare una VPN, richiede all'utente di fornire le credenziali per accedere alla VPN e per autenticare queste ultime il NAS utilizza il proprio processo di autenticazione o si avvale di un server di autenticazione separato in esecuzione sulla rete, come il RADIUS AAA Server (AAA sta per i servizi: Authentication, Authorization, Accounting).
L'altro componente di un accesso remoto VPN è un software VPN client, inoltre è necessario un firewall che faccia da barriera tra la rete privata e Internet. In genere le aziende esperte decidono di implementare e gestire in proprio la VPN ad accesso remoto, anche se le aziende possono decidere di esternalizzare (outsourcing) i propri servizi VPN tramite il provider dei servizi enterprise. Tirando le somme una Remote-access VPN è adatta per i singoli dipendenti/utenti o per aziende con filiali costituite da piccoli uffici.

Site-to-Site VPN

Una Site-to-site VPN permette di stabilire connessioni sicure attraverso una rete pubblica, anche ad aziende con tante soldi, ognuna con la sua LAN, ne esistono due tipi:

- Intranet-based, se si desidera unire le reti delle sedi remote in un'unica rete privata;
- Extranet-based, se si desidera unire in un ambiente sicuro le LAN di aziende diverse, in modo da condividere risorse senza l'accesso preventivo alla propria intranet;

Anche se gli scopi della Site-to-site VPN sono diversi da quelli della Remote-access VPN, è possibile utilizzare parte dello stesso software e gli stessi dispositivi, in genere la Site-to-site dovrebbe eliminare la necessità di eseguire il software VPN client come se l'host fosse una Remote-access VPN.

La Sicurezza delle Reti

Ovviamente le VPN devono affrontare seri problemi nell'ambito sia della sicurezza dei dati che della riservatezza delle trasmissioni. In questo campo i fattori su cui bisogna concentrare la nostra attenzione sono 3:

Autenticazione dell'Identità = il processo con cui il sistema informatico, un applicativo o un utente verifica l'identità di un altro sistema che vuole comunicare attraverso una connessione per poi concedergli l'autorizzazione ad usufruire dei relativi servizi associati. Bisogna autenticarsi prima di connettersi alla VPN, questa procedura è nota come MultiFactor Authentication, per esempio dopo il login viene chiesto di inserire un codice generato tramite una chiave elettronica. Ad oggi questa pratica è però superata dall'uso di applicazioni che associano alla generazione di una sequenza di caratteri da usare una volta sola. L'amministratore deve definire delle apposite autorizzazioni per

ciascun utente per l'accesso ai servizi della rete, la maggior parte delle VPN garantisce anche l'integrità, l'autenticità dei dati e prevede dei meccanismi di accounting. Con accounting si intendono tutte le azioni volte a misurare e documentare le risorse concesse a un utente durante un accesso, ciò può includere la durata della sessione di lavoro, o il quantitativo di traffico di dati in una sessione di lavoro. Le informazioni ottenute dalla trascrizione possono poi essere usate per un controllo per le autorizzazioni.

Cifratura = le VPN utilizzano diversi algoritmi di crittografia come il 3DES, CAST o IDEA per cifrare il traffico di rete. Nello specifico nelle VPN viene utilizzato il protocollo Internet Key Exchange (IKE), che implementa lo scambio delle chiavi per cifrare i pacchetti, esso automatizza la gestione delle chiavi.

Tunneling = i protocolli di tunneling aggiungono un livello di sicurezza al fine di proteggere ogni pacchetto nel suo viaggio su Internet, le VPN possono essere protette sia in modalità trasporto che in modalità tunneling. In caso di modalità trasporto hanno un ruolo importante i software impiegati. Nel caso di modalità tunneling hanno un ruolo fondamentale gli apparati router e firewall. In questa modalità l'intero pacchetto viene posto all'interno di un altro pacchetto passeggero che andrà su Internet, proteggendo il contenuto dalla vista del pubblico e facendo viaggiare il pacchetto passeggero all'interno di un tunnel virtuale. Tale stratificazione dei pacchetti viene definita incapsulamento, gli host alle estremità del tunnel possono incapsulare i pacchetti in uscita e riaprire i pacchetti in entrata.

I principali protocolli usati per garantire la sicurezza della rete sono :

- IPsec;
- SSLTLS;
- BGP/MPLS (Border Gateway Protocol / Transport Layer Security);

IPsec

L'IPsec è la scelta più frequente per realizzare sia le Site-to-site VPN con topologia a maglia completa che le Remote-access VPN con topologia a stella. Questo non è un singolo protocollo, ma piuttosto un'intera infrastruttura di sicurezza a livello Network composta da 3 protocolli:

- Authentication Header (AH): garantisce l'autenticazione e l'integrità del messaggio, ma non offre confidenzialità. Viene definito nell'RFC 4302;
- Encapsulating Security Payload (ESP): fornisce autenticazione, confidenzialità e integrità del messaggio. Viene definito nell'RFC4303;
- Internet Key Exchange (IKE): implementa lo scambio delle chiavi per il flusso crittografico. Viene definito nell'RFC 7296;

IPsec utilizza il protocollo **ESP** per l'invio sicuro dei datagrammi, poiché fornisce confidenzialità rispetto ad **AH**. In **IPv4**, AH ed ESP sono header di protocollo, mentre in **IPv6** sono extension header. Il protocollo **IKE**, invece, opera a livello Application sia in IPv4 che in IPv6. IPsec può funzionare in due modalità:

- **Trasporto**: aggiunge gli header AH/ESP tra l'header IP e il protocollo di trasporto (TCP/UDP);
- **Tunnel**: incapsula completamente il pacchetto IP originario;

Per garantire la sicurezza, due host stabiliscono una **Security Association (SA)** tramite **IKE**. Poiché le SA sono unidirezionali, ne servono due per una comunicazione bidirezionale. Le SA attive sono memorizzate nel **SAD (SA Database)**, mentre le politiche di sicurezza sono nel **SPD (Security Policy Database)**. L'elaborazione dei pacchetti distingue il **traffico in uscita (outbound)** da quello **in entrata (inbound)**:

- **Outbound**: si verifica lo SPD, si associa il pacchetto a una SA esistente (o si crea con IKE), si applica IPsec e si inoltra;
- **Inbound**: si ricompone il datagramma IP (se frammentato), si identifica il pacchetto tramite il campo protocollo e il valore **SPI**, si eseguono le operazioni IPsec, si controlla lo SPD e si inoltra il pacchetto alla destinazione o al livello superiore;

Ora andiamo a dare uno sguardo più specifico ai 3 protocolli principali dell'IPsec:

- AH: fornisce servizi di autenticazione, integrità e protezione da attacchi di tipo replay, in cui un intruso immette nella rete un pacchetto autentico precedentemente intercettato. Il campo più interessante dell'AH è Security Parameters Index SPI, che contiene un valore numerico che insieme all'indirizzo IP di destinazione e il protocollo, identifica l'SA utilizzata;
- ESP: fornisce servizi di confidenzialità, autenticazione, integrità e protezione da attacchi di tipo replay. È possibile utilizzare solo alcuni servizi o tutti i servizi insieme. Per quanto riguarda la confidenzialità differisce dall'AH in quanto essa non copre l'header esterno. ESP aggiunge anche un campo Authentication che contiene i dati usati per autenticare il pacchetto;
- IKE: realizza un collegamento peer-to-peer in due fasi, in primis i due host creano una Security Association per IKE stesso, ovvero un canale sicuro per la condivisione dei messaggi. In secundis, utilizzano l'SA appena creata per negoziare Security Association per altri protocolli (IPsec SA);

SSL/TLS

Una valida alternativa all'IPsec è rappresentata dai protocolli SSL/TLS (Security Sockets Layer/Transport Layer security). Le differenze tra SSL e TLS sono minime, in genere vengono implementati entrambi rendendoli interoperabili, Il TSL è un protocollo del livello Session ed è uno standard IETF e deriva dal SSL.

Il protocollo SSL/TLS è composto da due livelli:

- Record Protocol, che opera subito sopra un protocollo di livello Transport (come TCP) ed è utilizzato per incapsulare protocolli di livello superiore;
- Handshake Protocol, che rappresenta il livello superiore e si occupa della fase di negoziazione in cui si autentica l'interlocutore e si stabilisce la crittografia comune;

Per realizzare un SSL/TSL bisogna utilizzare tale protocollo al posto di IKE nell'IPsec, per la fase di autenticazione degli estremi del tunnel e la creazione delle chiavi. Per definizione, SSL/TLS è un semplice protocollo Client/Server che ha lo scopo di autenticare il server da parte del client e, opzionalmente, anche il client da parte del server, e di creare un canale cifrato sicuro per la comunicazione tra i due.

L'autenticazione si basa su **certificati digitali** firmati da una **Certification Authority (CA)**. Il server invia il proprio certificato al client, che ne verifica la validità controllando la firma digitale. Se valida, il server viene autenticato, altrimenti la connessione fallisce. I passaggi per una connessione sicura sono:

- **Client → Server**: invia la richiesta di connessione con gli algoritmi di crittografia supportati e un valore random per la pre-master key;
- **Server → Client**: invia il certificato digitale, la scelta degli algoritmi e il proprio valore random;
- **Client → Server**: verifica il certificato, invia il proprio certificato e la pre-master key cifrata con la chiave pubblica del server, poi richiede il passaggio alla comunicazione cifrata;
- **Server → Client**: conferma l'avvenuta autenticazione e avvia la comunicazione cifrata;

Mettendo a confronto i due protocolli, IPsec e SSL/TLS:

- **IPsec** è un'**architettura complessa** con più protocolli, mentre **SSL/TLS** è un **protocollo definito tramite RFC**;
- **IPsec** offre più metodi di autenticazione, ma **SSL/TLS** si basa solo sui certificati digitali;
- **SSL/TLS** può autenticare solo il server senza il client, mentre **IPsec** richiede autenticazione reciproca;
- **SSL/TLS opera a livello Session**, proteggendo i dati fino alla consegna. **IPsec opera a livello Network**, proteggendo tutto il traffico IP ma non i dati dopo l'arrivo all'host;
- **SSL/TLS funziona solo con TCP**, mentre IPsec protegge tutti i protocolli sopra IP (TCP, UDP, ICMP);

Classificazione della VPN in Base alla Sicurezza

In base ai protocolli che utilizzano e al grado di sicurezza che garantiscono, possiamo classificare le VPN in 3 categorie:

Trusted VPN = Nelle trusted VPN la riservatezza dei dati trasmessi attraverso Internet è controllata da un ISP. Queste non utilizzano i protocolli che permettono la cifratura e il tunneling dei dati trasmessi, l'ISP assicura una qualità del servizio utilizzando e controllando i percorsi dedicati, garantendo che nessun altro possa usufruire del canale assegnato alla VPN. I protocolli e le tecnologie utilizzate dalle Trusted VPN sono:

- Layer 2: trasporto di rete ATM e trasporto del layer 2 su tecnologia MPLS;
- Layer 3: MPLS con distribuzione limitata dalle informazioni del percorso attraverso il BGP;

Secure VPN = Le secure VPN utilizzano i protocolli che consentono la cifratura e il tunneling. Per essere definita secure VPN, una VPN deve garantire:

- la presenza di un sistema di comunicazione;
- che i dati viaggino criptati;
- che il livello di cifratura dei dati sia elevato e modificabile nel tempo;

I protocolli e le tecnologie utilizzate dalle secure VPN sono le seguenti:

- IPsec;
- SSL/TSL;
- PPTP (point-to-point Tunneling Protocol);
- SOCKS Protocol;
- L2TP (Layer 2 Tunneling Protocol);
- L2TPv3;
- MPLS (Multiprotocol Label Switching);

Hybrid VPN = Le Hybrid VPN rappresentano il tentativo di unire le caratteristiche delle Trusted VPN e delle Secure VPN, infatti le Secure VPN assicurano la cifratura dei dati ma non assicurano i percorsi, mentre le Trusted VPN assicurano le proprietà dei percorsi ma non garantiscono un alto livello di sicurezza. In merito ai protocolli usati nelle Hybrid VPN, si può affermare che ogni tecnologia supportata dalla Secure VPN si muove attraverso ogni tecnologia supportata dalla Trusted VPN.

Reti Wireless

Le reti wireless permettono la comunicazione tra dispositivi senza l'uso di cavi, sfruttando onde radio o segnali infrarossi. Come le reti cablate, possono essere classificate in base all'estensione dell'area coperta.

WPAN

Le **WPAN** (Wireless Personal Area Network) coprono pochi metri e sono adatte per ambienti domestici o piccoli uffici, usando tecnologie come **Bluetooth** o **IrDA**, impiegate anche nella domotica.

Il **Bluetooth** opera a 2,4 GHz, ha una velocità massima di 2 Mbps e segue lo standard **IEEE 802.15**. Una rete Bluetooth, detta **piconet**, è costituita da un dispositivo Master che gestisce fino a sette dispositivi Slave. Più piconet possono formare una **scatternet**. Con **Bluetooth 5.0**, la velocità arriva a 2 Mbps e la portata può raggiungere i 240 metri, migliorando le prestazioni rispetto alle versioni precedenti, soprattutto per dispositivi a basso consumo.

WLAN

Le **WLAN** (Wireless Local Area Network) sono simili alle tradizionali LAN cablate, ma senza fili. Lo standard più usato è **IEEE 802.11**. Le WLAN includono dispositivi mobili (WT) e uno o più **Access Point (AP)**, che fungono da ponte tra la rete wireless e quella cablata. Un **Basic Service Set (BSS)** è formato da un AP e dai dispositivi nella sua area di copertura. Più BSS collegati formano un **Extended Service Set (ESS)**, che si comporta come una sola rete WLAN.

Gli **ESS** possono includere BSS parzialmente sovrapposti, disgiunti o co-locati per garantire continuità, ridondanza o migliori prestazioni. Lo standard 802.11 gestisce la **mobilità** dei dispositivi, distinguendo tra transizioni statiche, tra BSS e tra ESS. In quest'ultimo caso, la connessione viene interrotta poiché si passa da una WLAN a un'altra.

La configurazione di un Access Point in ambito aziendale richiede la definizione di parametri come **SSID**, **potenza**, **canale**, **crittografia**, **incapsulamento**, **NAT** e **DHCP**.

WMAN

Le **WMAN** (Wireless Metropolitan Area Network) permettono la distribuzione dei dati in aree urbane tramite antenne potenti, offrendo una valida alternativa al cablaggio tradizionale. Il collegamento può essere **point-to-point**, tra due bridge wireless, o **point-to-multipoint**, con un'antenna centrale e più terminali puntati verso di essa. Lo standard usato è **IEEE 802.16**, da cui nasce il progetto **WiMAX**, simile alla Wi-Fi Alliance per le WLAN.

La trasmissione WiMAX può avvenire in modalità **non-line-of-sight**, con frequenze tra 2 e 11 GHz per ambienti urbani, o in modalità **line-of-sight**, su frequenze attorno ai 60 GHz, per coprire grandi distanze.

Le **WWAN** (Wireless Wide Area Network) coprono aree molto estese, fino a livello nazionale o continentale. I **WISP** (Wireless Internet Service Providers) offrono questi servizi con infrastrutture dedicate, e tramite accordi di roaming garantiscono connettività globale.

La Sicurezza nelle Reti Wireless

Dal punto di vista della **sicurezza**, le reti wireless presentano rischi specifici. Lo **sniffing** consente di intercettare passivamente i dati, per cui è essenziale usare meccanismi di crittografia. L'**accesso non autorizzato** avviene spesso tramite **Access Point Rouge** (non autorizzati), contrastabile con l'**autenticazione reciproca** tra WT e AP.

Un'altra minaccia è lo **spoofing**, dove un terminale falso si sostituisce a un dispositivo legittimo. Il **protocollo SARP** può prevenire questo rischio creando tunnel protetti. Gli **attacchi DoS** (Denial of Service) possono bloccare la rete sovrapponendo segnali radio. Barriere fisiche come vernici schermanti possono ridurre l'impatto.

La Crittografia

Tra i principali sistemi di crittografia utilizzati troviamo:

- **WEP (Wired Equivalent Privacy)**: è stato uno dei primi metodi usati per proteggere le reti Wi-Fi. Cifra solo il payload del frame utilizzando l'algoritmo **RC4**, un cifrario a flusso con chiave simmetrica. Tuttavia, è oggi considerato **insicuro** a causa delle sue vulnerabilità;
- **TKIP (Temporal Key Integrity Protocol)**: è una **evoluzione del WEP**, ancora basata su RC4, ma con miglioramenti. Utilizza una **chiave temporanea a 128 bit** condivisa tra il terminale wireless (WT) e l'Access Point (AP), che viene rigenerata ad ogni pacchetto o burst. Aggiunge anche un **IV (Initialization Vector)** di 128 bit per aumentare la complessità della chiave di cifratura. Nonostante ciò, anche TKIP è ormai superato;
- **AES (Advanced Encryption Standard)**: rappresenta lo standard di sicurezza attuale. Utilizza l'algoritmo a blocchi **Rijndael**, considerato estremamente sicuro e praticamente indecifrabile con le tecnologie attuali. Viene usato nei protocolli più recenti come **WPA** e **WPA2**, che

includono anche meccanismi di distribuzione dinamica delle chiavi e **autenticazione reciproca**;

L'Autenticazione

Sul fronte dell'**autenticazione**, esistono diversi metodi per impedire l'accesso non autorizzato alla rete wireless:

- **SSID (Service Set Identifier)**: è il nome della rete. L'Access Point consente l'accesso solo ai dispositivi che cercano di connettersi utilizzando il SSID corretto. Tuttavia, poiché il SSID può essere facilmente intercettato, questo metodo da solo non è sufficiente;
- **Filtraggio degli indirizzi MAC**: l'amministratore di rete può creare una lista di indirizzi MAC autorizzati. Gli Access Point accettano solo i dispositivi presenti nella lista. Anche se utile, questo metodo può essere aggirato da un attaccante che clona un indirizzo MAC valido;
- **EAP (Extensible Authentication Protocol)**: è un protocollo avanzato per l'autenticazione, usato su entrambe le sezioni della rete, cablata e wireless. Si basa su un **server di autenticazione centrale**, che consente un controllo accurato degli accessi e può essere integrato con sistemi di identità aziendali (come RADIUS). EAP permette di implementare forme di autenticazione sicure, come l'autenticazione tramite certificati o credenziali univoche;

Infine, un'infrastruttura wireless aziendale completa può includere un **router Wi-Fi** collegato a un **server AAA** (Authentication, Authorization, Accounting), che gestisce centralmente l'accesso, le autorizzazioni e tiene traccia delle attività degli utenti in rete.