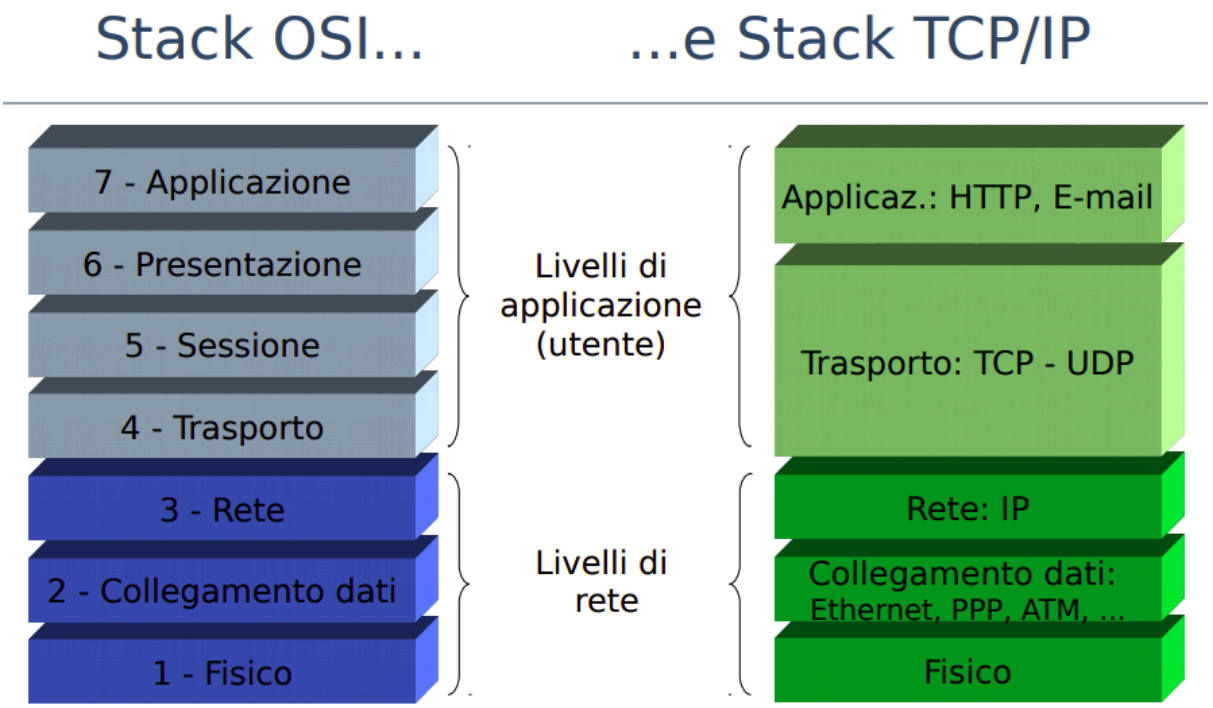
Introduzione ---> Ripasso delle Reti



Livelli TCP/IP:

- **Fisico**: trasmissione fisica tramite cavi e bit interpretati da segnali elettrici;
- **Data Link**: scendendo un gradino nella pila protocollare, troviamo il livello data link, il responsabile della comunicazione efficiente e ordinata all'interno della stessa rete fisica. Immaginate questo livello come il sistema che gestisce le conversazioni e gli scambi tra dispositivi che si trovano nella stessa "stanza" o segmento di rete, che sia una LAN tradizionale via cavo (Ethernet) o una rete senza fili (Wi-Fi, Bluetooth). In questo contesto, il modo in cui i dati vengono trasmessi e gestiti è cruciale. Ethernet, ad esempio, un tempo si affidava a meccanismi come il CSMA/CD (Carrier Sense Multiple Access with Collision Detection) per evitare "scontri" di dati sul cavo condiviso. Oggi, con l'avvento degli switch, le collisioni sono quasi un ricordo, poiché ogni dispositivo ha una connessione dedicata al suo interno, rendendo la comunicazione più diretta ed efficiente. Il Wi-Fi, invece, operando via etere, non può "sentire" le collisioni mentre trasmette e continua a usare un approccio come il CSMA/CA (Collision Avoidance), dove i dispositivi "ascoltano" e aspettano il loro turno per parlare, cercando di prevenire le collisioni anziché rilevarle. A questo livello, i dati viaggiano raggruppati in unità chiamate PDU (Protocol Data Unit), che sono fondamentalmente "pacchetti" o "raggruppamenti di bit/byte". Per assicurarsi che ogni pacchetto arrivi al destinatario giusto all'interno di questa stessa rete locale, si lavora

principalmente con gli indirizzi MAC. Ogni dispositivo di rete ha il suo indirizzo MAC, un identificatore unico di 48 bit, solitamente rappresentato come 6 coppie di caratteri esadecimali separati da due punti (es. 00:1A:2B:3C:4D:5E). Possiamo pensare al router come alla "porta" che connette la nostra "stanza" (la rete locale) al mondo esterno. All'interno di questa porta, ci sono delle "maniglie", le interfacce gateway (in particolare quella di default), che sono i punti di ingresso e uscita dalla stanza stessa. Quando un pacchetto viene inviato all'interno della rete locale, il suo primo campo nell'intestazione è proprio l'indirizzo MAC del destinatario. Questo è un meccanismo estremamente efficiente: le schede di rete di tutte le macchine presenti sulla stessa LAN "leggono" solo questo primo campo. Se l'indirizzo MAC non corrisponde al proprio, possono ignorare il pacchetto immediatamente e senza alcuno sforzo ulteriore di lettura o elaborazione da parte del sistema operativo (SO). Questo evita inutili sprechi di tempo e risorse computazionali, garantendo che solo la macchina destinata debba "aprire" e processare quel pacchetto specifico;

- **Rete**: connessione tra diverse reti locali, tramite instradamento e indirizzi IP (protocollo v4 32 bit, v6 128 bit);
- **Trasporto**: esegue un enumerazione per il trasporto di PDU che devono essere divisi in sotto porzioni gestendo, tramite protocolli come TCP (non dire che è sicuro, bensì affidabile) e UDP, la perdita di PDU e il loro recupero;
- **Applicazione**: questo livello ne ingloba 3 dell'OSI perché troppi livelli introducono complessità ed inefficienza inutile (più header, più costi e più tempi). Attraverso il sistema di porte introdotte dal livello di trasporto, siamo in grado di far comunicare i precisi processi (il DNS è un protocollo di questo livello e non del livello di rete, ed è un esempio di tecnologia che utilizza UDP).

N.B: un protocollo è una convenzione; più un pacchetto scende tra i livelli più si gonfia per via degli header.

STRUMENTI DI ANALISI DELLA RETE

Esistono diversi strumenti SW che consentono di analizzare ed eseguire diagnostica di PDU che arrivano sulla propria interfaccia di rete:

- TCPDUMP, storico tool da linea di comando (per OS Linux);
- WinDump, storico tool da linea di comando (per OS Windows);
- Wireshark, moderno tool con GUI disponibile per Linux, Windows e Mac.

Noi chiaramente useremo il terzo. Le principali funzionalità di questa libreria sono la possibilità di cercare e trovare interfacce di rete, la gestione avanzata di filtri di cattura e la gestione degli errori e statistiche di cattura.

Catturano fisicamente i PDU e li interpretano. Le due funzionalità (cattura e interpretazione) sono distinte, ossia si può catturare il traffico e analizzare in un secondo momento, allo stesso modo analizzare del traffico precedentemente catturato.

Mentre l'interpretazione avviene ad un livello più astratto e che permette all'utente una visualizzazione e una personalizzazione migliore, la parte di cattura coinvolge elementi di basso livello come le interfacce di rete (ricordarsi che sono molteplici wifi-bluetooth, eth., NFC, USB-C 3.0, …). In particolare la 'lo' (loopback) è una rete fittizia sempre presente che rende possibile la comunicazione tra processi della stessa macchina come fossero su diverse reti.

In particolare la parte che esegue la cattura (o sniffing) dei PDU è svolta da una libreria a parte scritta in C chiamata libpcap, che scavalca il SO prendendosi una copia di tutte le PDU in arrivo su una determinata interfaccia di rete prima che il SO ignori ed elimini i PDU che normalmente non sarebbero destinati alla macchina in uso. Pertanto necessita i privilegi di root (sudo), dato che deve lavorare a stretto contatto con l'hw (attivazione flag di mod. promiscua -- vedi primo punto). Esistono due macro-casi per questa operazione:

- sniffing all'interno di reti non-switched: in questa tipologia di reti il mezzo trasmissivo è condiviso e, quindi, tutte le schede di rete dei PC ricevono tutti i PDU, anche quelli destinati ad altri. I propri, invece, sono selezionati a seconda del MAC. Lo sniffing, in questo caso, consiste nell'impostare sull'interfaccia di rete la cosiddetta **modalità promiscua** che disattiva il "filtro hardware" basato sul MAC. Così facendo, si permette al sistema l'ascolto di tutto il traffico passante sul cavo. Un esempio di rete non-switched è la rete WiFi;
- sniffing all'interno di reti Ethernet switched: in questo caso, invece, l'apparato centrale della rete (definito switch), si preoccupa di inoltrare su ciascuna porta solo il traffico

destinato ai dispositivi collegati a quella porta. Quindi, ciascuna interfaccia di rete, riceve solo i PDU destinati al proprio indirizzo, i PDU multicast e quelli broadcast. L'impostazione della modalità promiscua è, pertanto, insufficiente per poter intercettare il traffico in una rete gestita da switch.

In WSH ci sono due tipi di filtri:

- filtro di cattura: si utilizza associando un espressione booleana sulla base dei campi dei PDU; avviene prima della cattura effettiva, in quanto lavora ancora una volta insieme alla modalità promiscua volta ad alleggerire il costo della cattura. In questo modo, i PDU che non rispettano l'espressione richiesta vengono completamente ignorati. Per iniziare una cattura basta andare sul menù a tendina 'cattura' e selezionare 'opzioni'; da qui selezionare l'interfaccia desiderata e sulla parte bassa un filtro di cattura per scremare eventuali pacchetti indesiderati;
- filtro di visualizzazione: a differenza del precedente, i PDU ormai sono stati catturati (post cattura), ma serve solo nella mera visualizzazione/ricerca di determinati PDU (non eliminando quindi i PDU che non rispecchiano l'espressione di questo filtro); legato a questo, è possibile anche colorare i PDU per una migliore visualizzazione sulla base di determinate caratteristiche del PDU stesso;

Comandi di utilizzo generale da terminale:

- **ping**: è un semplice strumento per verificare la raggiungibilità di un computer connesso alla rete e il relativo Round Trip Time (RTT), ossia il tempo che intercorre dalla partenza del pacchetto inviato al ritorno della risposta. Per questa operazione viene utilizzato il protocollo ICMP (Internet Control Message Protocol è un protocollo di servizio per trasmettere informazioni riguardanti malfunzionamenti, informazioni di controllo o messaggi tra i vari componenti di una rete di calcolatori);
- **traceroute**: il comando traceroute è, invece, un semplice strumento per tracciare il percorso che un pacchetto segue dalla sorgente alla destinazione. Il comando mostra un elenco di tutte le interfacce dei router che il pacchetto attraversa finché non raggiunge la destinazione. Si noti la presenza di alcuni asterischi in corrispondenza di determinate tappe. Questi sono dovuti al fatto che, certe interfacce di specifici router, non forniscono alcuna informazione. Questa scelta viene presa dagli amministratori di rete per evitare di svelare la topologia di rete a possibili malware. In tal caso traceroute non può mostrare tali passi del percorso (il protocollo è sempre ICMP). Come per le telefonate spam che cercano di capire se il nostro numero di telefono è ancora attivo per venderlo e fare pubblicità, il protocollo ICMP è spesso bloccato dai

network administrator per motivi di sicurezza (in particolare riguardo l'intasamento della rete);

- **nslookup**: il comando nslookup consente di effettuare una interrogazione ai server DNS per poter ottenere da un hostname il relativo indirizzo IP, o viceversa. Si può utilizzare in due modalità interattivo e non interattivo. DNS (Domain Name System) è un sistema di server organizzato gerarchicamente, per la gestione del namespace (Domain Name Space). Il compito principale di questo servizio è quello di rispondere alle richieste della risoluzione del nome di dominio, ovvero la conversione dei nomi di dominio in indirizzi IP. Nello specifico la modalità interattiva permette di effettuare più interrogazioni e visualizza i singoli risultati; viene abilitata in maniera automatica quando il comando non è seguito da alcun argomento. La modalità non interattiva invece permette di effettuare una sola interrogazione visualizzandone il risultato, e si abilita ogni qualvolta si specifichi l'host-to-find;
- **ifconfig**: il comando ifconfig è un utilizzato per configurare e controllare un'interfaccia di rete TCP/IP da riga di comando. L'esecuzione del comando con l'opzione -a mostra a video le informazioni di tutte le interfacce di rete;
- **route**: il comando route è utilizzato per visualizzare e modificare le tabelle di routing;
- **whois**: il comando whois consente, mediante l'interrogazione di appositi database server da parte di un client, di stabilire il nome del privato, azienda o ente al quale è intestato un determinato indirizzo IP o uno specifico dominio DNS. Nel Whois vengono solitamente mostrate anche informazioni riguardanti l'intestatario, data di registrazione e la data di scadenza. Whois si può consultare tradizionalmente da riga di comando, anche se ora esistono numerosi siti web che permettono di consultare gli archivi dove sono contenute tali informazioni (non incappare nella somiglianza con nslookup, qui si inserisce solo il sito senza www, mentre nell'altro si).