CS0424IT - Lecture Notes

Simone La Porta

May 31, 2024

Contents

1 LIVELLO 2 - VLAN

Switch (livello data, MAC address) permette di segmentare i domini di broadcast mediante la creazione delle virtual LAN, ovvero un insieme logico di host e device di rete: le VLAN si creano aggiungendo un tag o VLAN id alle porte dello switch, o mappando il mac address dell'host con il VLAN ID.

Ipotizzando di voler restringere la comunicazione ed il dominio di broadcast ad A, B, C. Creiamo una VLAN identificata con ID 100 e associamo i MAC di ABC a quella VLAN (ma non quello di D).

Se A invia un pacchetto all'indirizzo di broadcast esso sara ricevuto solamente da B e C. VLAN = segmentano i domini di broadcast e eliminano il problema di latenza su grosse reti.

2 Livello 3 di rete: router-gateway

Cosi come per il livello data ci sono dei dispositivi di rete ad hoc (router-gateway): dispositivi di livello 3 che instradano i dati anche a personal computer che sono connessi su reti diverse.

Switch dispositivo di livello 2 e non sa come dirottare i pacchetti su un'altra rete (instrada solo tramite MAC address e non tramite IP address, il quale appartiene al livello di rete).

Il router riceve il pacchetto dallo switch controlla la sua routing table per capire verso quale delle sue interfacce instradare il pacchetto affinché giunga alla rete di destinazione.

3 LIVELLO 4 - TRASPORTO

Livello di trasporto si occupa di instaurare un collegamento tra le applicazioni che sono su computer diversi.

ATTENZIONE: pacchetti possono andare persi, non sempre un problema (ad es parlare al telefono) ma puó essere un problema (operazioni finanziare ecc).

Quindi per alcuni servizi/applicativi é **INDISPENSABILE** che ci sia un controllo sull'effettiva consegna dei pacchetti.

Livello 4 mette a disposizione due protocolli fondamentali: **TCP** (transmission control protocol), e **UDP** (user datagram protocol).

TCP: garantisce controllo sul traffico dei pacchetti e sull'effettiva consegna al ricevente. Più sicuro, TCP è connection oriented cioè prima di iniziare lo scambio fa sì che si instauri un canale di comunicazione tra sorgente e destinatario. Agisce con un **three-way handshake**:

- client che inizia la connessione invia un pacchetto TCP al server destinatario con il flag SYN abilitato ed un numero di sequenza casuale.
- server risponde inviando al client un pacchetto con i flag SYN e ACK abilitati, ed un altro numero di sequenza casuale, mentre l'ACK sarà uguale al precedente Seq+1.
- client completa la sincronizzazione inviando un pacchetto ACK ed inviando i numeri Seq, ACK, come fatto dal server (ACK sempre Seq ricevuto +1).

UDP invece è protocollo connectionless non ha necessità di instaurare un canale di comunicazione prima di iniziare il flusso. Più snello e veloce per attività che richiedono continuo streaming di dati.

Per capire qual è il processo o servizio destinatario di un determinato pacchetto, il TCP o UDP utilizzano le porte o meglio la coppia IP:PORTA. Mentre con l'IP si identifica la macchina destinataria la porta da info sul servizio. Ogni servizio attivo su un pc utilizza una porta.

Porte si dividono in WELL KNOWN ports utilizzate per i servizi standard tra 0-1023 (prime 1024).
HIGH ports servizi non standard e comunicazione (1024-65535).
Importante ricordare le well known ports associate ai servizi più noti. SMTP:25
HTTP:80
SSH:22
POP3:110
IMAP:143
NETBIOS:137,138,139
SFTP:115
HTTPS:443

TELNET:23 FTP:21
RDP:3389
MSSQL:1433
MySQL:3306

Per visualizzare porte in ascolto e le connessioni in corso possibile utilizzare NETSTAT che darà in output info circa i demoni (daemon) in ascolto su PC localmente e le connessioni verso server remoti:

netstat -ano (WIN) netstat -tunp (LINUX) netstat -p tcp -p udp (MAC)

4 LIVELLO 5 - SESSIONE

Livello di applicazione, si organizzano i dati: si apre una sessione (es ssh) tra utente che intende utilizzare un servizio che è in ascolto su un determinato server, si controlla la durata della sessione e di mantenerla attiva durante il flusso di informazioni (ad esempio cambio ip con vpn).

5 LIVELLO 6 - PRESENTAZIONE

Preparazione dei dati per essere presentati agli utenti: concetto di CIFRATURA dei dati.

Su un canale di comunicazione i dati possono transitare in maniera visibile o cifrati (ALGORITMO DI CIFRATURA), in maniera tale da rendere disponibili i dati cifrati.

6 LIVELLO 7 - APPLICAZIONE

Livello interagisce direttamente con le applicazioni utilizzate. Protocolli più comuni HTTP, HTTPS (cifrato), DNS (traduce la richiesta di un dominio, basato su UDP), FTP (basato su TCP gestisce trasferimento dati tra host).

DNS fondamentale per funzionamento di internet, www(host).store(subdomain).google(domain).com(toplevel domain).

DHCP permette ai dispositivi di una LAN di ricevere una configurazione di rete.

NAT/PAT: network address translation per far fronte all'esaurimento del IPv4. Da questo momento in poi vi è una distinzione tra ip pubblici (es per andare su internet) e privati (interno della rete locale e non raggiungibili su internet), configurati tramite router.

PAT port address translation, forma specifica di NAT in cui oltre alla traduzione degli indirizzi IP vengono anche tradotte le porte dei dispositivi all'interno della rete locale.

Le porte sono numeri a 16bit associati a ogni connessione e PAT permette a più dispositivi di condividere lo stesso IP pubblico distinguendo le loro connessioni in base alle porte.

Mentre NAT traduce indirizzi ip privati in 1 o più indirizzi ip pubblici, il pat va oltre traducendo anche le porte, consentendo a più dispositivi di condividere lo stesso indirizzo ip pubblico.