Corso di RETI

Lezione 21 Novembre 2024

Accesso al mezzo

Con questo termine (Accesso al mezzo di trasmissione) si riferisce al modo in cui i dispositivi di rete gestiscono e coordinano l'uso del canale fisico attraverso cui i dati vengono trasmessi. Questo concetto è strettamente legato al livello di collegamento dati (livello 2 del modello OSI) e più specificatamente, al sottolivello di controllo dell'accesso al mezzo (MAC, Media Access Control)

Il mezzo è la risorsa fisica utilizzata per trasmettere i dati tra i dispositivi, come cavi Ethernet, fibre ottiche o onde radio nel caso di reti wireless.

Esistono vari metodi di gestione dell'accesso al mezzo, ognuno adatto a un tipo specifico di rete o di tecnologia:

- Accesso casuale (contention-based)
  Questo consente ai dispositivi di trasmettere quando il mezzo è libero, ma implementa meccanismi per gestire collisioni
- Accesso determinato
  Qui l'accesso la mezzo è regolato da un ordine prestabilito o da un sistema di prenotazione come un Token Passing dove un token viene passato tra i dispositivi e solo chi lo possiede può trasmettere
- Accesso centralizzato
  In questo caso, un dispositivo centrale, come un access point, decide quale dispositivo può trasmettere in un dato momento. Questo è comune nelle reti cellulari o in alcuni sistemi wireless

Un corretto controllo dell'accesso al mezzo è cruciale per:

- Evitare conflitti o sioni che causano una perdita di pacchetti e necessità di ritrasmissioni
- Garantire l'efficienza nella trasmissione dei dati, soprattutto in reti ad alta densità di dispositivi
- Supportare la qualità del servizio, assegnando priorità a dati più importanti

Reti locali

Le reti locali sono reti di comunicazione che connettono dispositivi all'interno di una piccola area geografica. Sono progettate per condividere risorse in modo rapido ed efficiente tra utenti locali

Trasmissione di informazioni

La trasmissione di informazioni si riferisce al processo con cui i dati vengono inviati da una sorgente a una destinazione attraverso un mezzo di comunicazione. Questo riguarda l'insieme di meccanismi, delle tecniche e dei protocolli utilizzati per trasferire informazioni in modo affidabile ed efficiente

La trasmissione dei dati implica spesso processi di **codifica** e/o **modulazione**

- Codifica: conversione dei dati in una forma adatta alla trasmissione
- Modulazione: applicata nei segnali analogici e consiste nel modificare proprietà come impietta, frequenza o fase per trasportare informazioni

Tipologia di trasmissione

1. In base al flusso di dati
    - Simplex → i dati viaggiano in una sola direzione, dalla sorgente alla destinazione
    - Half-duplex → la trasmissione è bidirezionale ma i dati possono viaggiare in una sola direzione alla volta (es. walkie-talkie)
    - Full-duplex → la trasmissione è bidirezionale e simultanea
2. In base alla modalità di trasmissione
    - Trasmissione seriale → i dati sono inviati un bit alla volta, in sequenza (connessioni a lunga distanza)
    - Trasmissione parallela → più bit vengono inviati contemporaneamente su canali distinti (connessioni a breve distanza, come tra CPU e RAM)
3. In base al mezzo fisico
    - Trasmissione cablata → attraverso cavi come rame (Ethernet) o fibra ottica
    - Trasmissione wireless → utilizza onde radio, microonde, infrarossi o onde luminose

Le reti collegano:

- Computer (desktop, laptop, server): Per lo scambio di file e l'accesso a risorse centralizzate.
- Stampanti e scanner: Permettono a più utenti di utilizzare lo stesso dispositivo.
- Smartphone e tablet: Per accedere a internet e alle risorse aziendali o domestiche.
- Smart TV e dispositivi multimediali: Per lo streaming o il controllo remoto.
- Dispositivi IoT (Internet of Things): Come termostati, videocamere di sicurezza, elettrodomestici e sensori intelligenti.

E permettono l'accesso condiviso a risorse di rete come:

- File e documenti: Archiviati in server, NAS (Network Attached Storage) o cloud.
- Applicazioni e software: Ad esempio, sistemi gestionali aziendali o app di collaborazione.
- Connessione Internet: I dispositivi possono accedere a internet tramite un router o un access point.

Collegano sistemi e servizi:

- Database e server: Per memorizzare ed elaborare dati.
- Server di posta elettronica: Per la comunicazione via email.
- Server web: Per fornire contenuti o applicazioni web.
- Telefonia VoIP: Per effettuare chiamate vocali tramite internet.

Topologia

La topologia di rete è il modo in cui i dispositivi (nodi) di una rete sono organizzati fisicamente o logicamente. La topologia influisce sulle prestazioni, sull'efficienza e sulla manutenzione della rete. Esistono varie topologie di reti:

1. Topologia a **bus**
   Tutti i dispositivi sono collegati a un unico cavo (chiamato bus) che funge da canale di comunicazione condiviso.
    - Vantaggi → economica e semplice da installare
    - Svantaggi → se il cavo principale si guasta, l'intera rete si interrompe
2. Topologia ad **anello**

I dispositivi sono connesso in modo circolare, formando un anello dove i dati viaggiano in una sola direzione passando attraverso ogni dispositivo
    - Vantaggi → nessuna collisione dei dati e adatta a piccoli ambienti
    - Svantaggi → se un nodo o il collegamento si guasta l'intera rete può bloccarsi
3. Topologia a **stella**
   Ogni dispositivo è connesso a un dispositivo centrale (hub o switch)
    - Vantaggi → se un dispositivo di guasta la rete continua a funzionare, facile da configurare e gestire
    - Svantaggi → se l'hub o lo switch si guastano, l'intera rete si interrompe

   È la più popolare per reti domestiche e aziendali di piccole/medie dimensioni, grazie alla semplicità e affidabilità
4. Topologia a maglia (**mesh**)
   Ogni dispositivo è connesso direttamente a uno o più dispositivi creando percorsi multipli tra i nodi
    - Vantaggi → altissima affidabilità in quanto se un collegamento si interrompe ci sono percorsi alternativi
    - Svantaggi → costosa e complessa da implementare

   È la migliore per reti mission-critical dove la resilienza è più importante del costo
5. Topologia ad **albero** (gerarchica)
   È una combinazione di più tecnologie a stella collegate in un'unica struttura gerarchica, con un nodo centrale come radice
    - Vantaggi → facile da espandere aggiungendo nodi alla struttura e adatta a reti aziendali
    - Svantaggi → se il nodo centrale della gerarchia di guasta, molte parti della rete possono diventare inutilizzabili

   Perfetta per reti LAN aziendali di grandi dimensioni o istituzioni
6. Topologia **ibrida**
   Combina più tipi di topologie (es. stella + bus, stella + anello)
    - Vantaggi → flessibilità nella progettazione e combina i punti di forza delle topologie base
    - Svantaggi → complessa da implementare e mantenere

   Ottima per grandi reti aziendali o reti che devono crescere ed evolversi nel tempo

Le **tipologie** possono essere fisiche o logiche. In quelle **fisiche** la disposizione dei cavi, dei dispositivi e delle connessioni è presente ed è effettiva. Nelle topologie **logiche** i dati viaggiano attraverso la rete, indipendentemente dalla disposizione fisica

Protocolli

I protocolli di rete sono insieme di regole e convenzioni che definiscono come i dispositivi di una rete comunicano tra loro. Fungono da linguaggio comune che garantisce la trasmissione corretta, sicura e comprensibile dei dati. Ogni protocollo si occupa di aspetti specifici della comunicazione, come l'indirizzamento, la trasmissione o la sicurezza
Sono regole standardizzate e convenzioni che definiscono come i dati devono essere formattati, inviati, ricevuti e interpretati tra dispositivi connessi a una rete
Ogni protocollo opera in uno dei livelli del modello OSI o TCP/IP

Protocollo del livello di applicazione

Questi protocolli gestiscono le interazioni tra applicazioni e utenti

- HTTP/HTTPS (HyperText Transfer Protocol / Secure)

Questo viene usato per trasferire pagine web e HTTPS (su porta 443) include la crittografia per maggiore sicurezza
- FTP (File Transfer Protocol) → usato per trasferire file tra dispositivi
- IMAP/POP3 (Internet Message Access Protocol / Post Office Protocol)
  Usato per ricevere email
- DNS (Domain Name System) → Traduce i nomi di dominio in indirizzi IP

Protocollo del livello di trasporto

Questi gestiscono la trasmissione dei dati, viaggiano su porte a 16 bit

- TCP (Transmission Control Protocol)
  Garantisce una trasmissione affidabile dei dati, con controllo degli errori e ordine dei pacchetti. Effettua il recupero dei pacchetti ovvero se questi vengono persi li cerca, li recupera e crea l'illusione che non siano stati persi. Più lento perché occupa più banda
- UDP (User Datagram Protocol)
  Più veloce ma meno affidabile del TCP, usato per streaming e giochi online .Se perde pacchetti non gli interessa perché non rilevante come nello streaming

Protocolli del livello di rete (NetWork)

Si occupano dell'instradamento e dell'indirizzamento dei dati tra reti. Sono presenti gli indirizzi di interfaccia

- IP (Internet Protocol), principale e più usato
  Gestisce l'indirizzamento e il routing dei dati. Le versioni principali sono IPv4 e IPv6.
- { ICMP (Internet Control Message Protocol)
  Viene usato per diagnosticare problemi di rete (es. comando ping).
- ARP (Address Resolution Protocol)
  Traduce gli indirizzi IP in indirizzi MAC }

Protocolli del livello di collegamento (DataLink)

Questi operano al livello hardware per gestire la trasmissione fisica dei dati. Gestisce ciò che ho intorno

- Ethernet, è lo standard per reti cablate.
- Bluetooth 2 4 Gh
- Wi-Fi (IEEE 802.11), è lo standard per reti wireless.
- PPP (Point-to-Point Protocol), viene usato per connessioni punto-punto come modem o VPN.

Protocolli di sicurezza

Garantiscono la protezione dei dati durante la trasmissione.

- SSL/TLS (Secure Sockets Layer / Transport Layer Security)
  Sono protocolli che permettono di crittografare le comunicazioni per proteggere i dati (es. HTTPS).
- IPSec (Internet Protocol Security)
  Crea una crittografia e autenticazione per i dati a livello IP.
- SSH (Secure Shell)
  Usato per accedere in modo sicuro ai dispositivi remoti.

Protocolli di gestione della rete

Permettono di monitorare e gestire i dispositivi di rete.

- SNMP (Simple Network Management Protocol)
  Viene usato per monitorare e gestire i dispositivi di rete.
- NTP (Network Time Protocol)
  Usato per sincronizzare gli orologi dei dispositivi di rete.

Architetture di rete: “TCP/IP”

L'**architettura di rete TCP/IP** è un modello di riferimento progettato per descrivere il funzionamento di internet e di altre reti. Si basa su un insieme di protocolli standardizzati che consentono la comunicazione tra dispositivi connessi. Il modello TCP/IP (Transmission Control Protocol/Internet Protocol) è più semplice rispetto al modello OSI a 7 livelli e include 4 livelli principali.

1. **Livello Applicazione**
   Questo primo livello fornisce i servizi necessari per le applicazioni di rete (es. navigazione web, email).
   I protocolli principali a questo livello sono:
   - HTTP/HTTPS: Per la navigazione web, protocollo per veicolare pagine web. L’HTTPS, protocollo sicuro per la S che da riservatezza e autenticazione
   - FTP: Per il trasferimento di file.
   - SMTP/IMAP/POP3/POP3S: Per l'invio e la ricezione di email.
     POP3 e POP3S(protocollo sicuro) per la lettura delle mail
     SMTP e IMAP(lascia le mail sul server rendendole accessibili da più dispositivi, non le scarica in locale come POP3) per inviare mail
   - DNS: Per la risoluzione dei nomi di dominio (risolvere nomi in indirizzi IP), l’IP è associato a un dominio. Il DNS è un registro
   - Telnet/SSH: Per l'accesso remoto.
2. **Livello Trasporto**
   Il secondo livello garantisce la consegna affidabile e ordinata dei dati tra dispositivi.
   I protocolli principali usati in questo livello sono:
   - TCP (Transmission Control Protocol): è un protocollo di trasferimento affidabile (con controllo degli errori e gestione dei pacchetti) e adatto a applicazioni sensibili all'integrità dei dati (es. pagine web, email, file transfer). Tutti i protocolli con la S finale, quindi per l’autenticazione vanno sul TCP
   - UDP (User Datagram Protocol): è più veloce ma non garantisce l'affidabilità. Viene usato per applicazioni in tempo reale come (Protocollo RTP, real time transportation) streaming o gaming online. (DNS). In questo caso la perdita di pacchetti è irrilevante
3. **Livello Internet**
   Si occupa dell'indirizzamento e dell'instradamento dei pacchetti tra reti diverse.
   I protocolli principali sono:
   - IP (Internet Protocol): Gestisce l'indirizzamento e il routing e le versioni principali sono IPv4 (indirizzi a 32 bit) e IPv6 (indirizzi a 128 bit).
   - ICMP (Internet Control Message Protocol): diagnostica problemi di rete (es. comandi come ping).
   - ARP (Address Resolution Protocol): traduce indirizzi IP in indirizzi MAC.
   - RARP (Reverse ARP): traduce un indirizzo MAC in un indirizzo IP.
4. **Livello Accesso alla Rete** (o Livello Data Link)
   Gestisce la trasmissione dei dati sul mezzo fisico (cavi, segnali radio, fibra ottica).
   I protocolli principali sono:
   - Ethernet: Standard per le connessioni cablate.
   - Wi-Fi: Per le connessioni wireless.
   - Bluetooth:
   - PPP (Point-to-Point Protocol): Per connessioni punto a punto.

- MAC (Media Access Control): Per la gestione degli indirizzi hardware.

5. Livello fisico → **non fa formalmente parte del modello TCP/IP poiché è gestito da standard esterni**
   Questo livello è fondamentale per consentire la trasmissione dei dati tra i dispositivi
   Nel contesto delle reti, il livello fisico, riguarda la trasmissione effettiva dei dati come segnali elettrici, ottici o radio
   Il modello TCP/IP non definisce direttamente il livello fisico ma lo considera implicito come base per il funzionamento del Livello di Accesso alla Rete

Aspetto	TCP/IP	OSI
Numero di livelli	4	7
Scopo	Pratico, basato su protocolli reali.	Teorico, usato per standardizzare concetti.
Implementazione	È usato per internet e reti reali.	Serve come modello concettuale.
Flessibilità	Più semplice e meno dettagliato.	Più dettagliato e rigoroso.

Applicazioni di rete
Le **applicazioni di rete** sono programmi o piattaforme che utilizzano una rete, come internet o una LAN, per fornire servizi agli utenti. Possono coinvolgere la comunicazione, la condivisione di risorse, l'intrattenimento, il lavoro collaborativo e molto altro. Ogni tipo di applicazione sfrutta protocolli specifici per funzionare correttamente.

- Web
  Ono applicazioni basate sul WWW che permettono agli utenti di accedere a contenuti online. Le tecnologie coinvolte sono HTTP/HTTPS per la comunicazione tra browser e server e HTML, CSS, JavaScript per la creazione di contenuti visivi e interattivi
  Es → siti web come Google e applicazioni web come Gmail
- Videogiochi di rete
  Sono giochi che richiedono una connessione di rete per interagire con altri giocatori o server. Le tecnologie usate sono UDP, TCP, server dedicati o peer-to-peer per gestire le interazioni tra giocatori
  Es → multiplayer online e giochi basati su browser o app
- Social Network
  Sono piattaforme per connettersi e condividere contenuti con altri utenti
  Tecnologie coinvolte: HTTP/HTTPS, WebSocket per notifiche e aggiornamenti in tempo rali e database distribuiti per gestire miliardi di utenti e contenuti
- Streaming multimediale
  Questo fornisce contenuti o audio in tempo reale o su richiesta tramite una rete
  Tecnologie coinvolte: HTTP Live Streaming (HLS) per trasmetter video adattivi, MPEG-DASH ovvero lo standard per lo streaming dinamico e CDN (Content Delivery Network) per distribuire in modo rapido e scalabile
- Audio e conferenza
  Sono applicazioni per la comunicazione vocale o video in tempo reale
  Utilizzano tecnologie come VoIP (Voice over IP) per chiamate audio via internet, RTP per trasmettere audio/video in tempo reale e WebRTC per la comunicazione diretta tra browser senza plugin

Infrastruttura = topologia + applicazioni (es. cloud computing che è un'applicazione di Internet)

Infrastruttura di rete
L'**infrastruttura di rete** è l'insieme di risorse fisiche, logiche e software necessarie per creare, gestire e utilizzare una rete di comunicazione. È il "sistema nervoso" che collega dispositivi e applicazioni, consentendo lo scambio di dati e informazioni.
L'infrastruttura di rete include tutti i componenti necessari per il funzionamento di una rete: dispositivi fisici, protocolli, connessioni e applicazioni ed è composto da:

- Topologia
- Hardware come switch, cavi, server, access point, data center e dispositivi di rete wireless
- Software come sistemi operativi di rete, protocolli, strumenti di gestione e sicurezza
- Servizi come applicazioni di cloud computing (permettono di archiviare ed elaborare dati in remoto tramite internet utilizzando server), database distribuiti, piattaforme di streaming o strumenti di collaborazione

DNS (Domain Name System)
Il DNS è un sistema fondamentale dell'infrastruttura di internet che traduce i nomi di dominio leggibili all'uomo in indirizzi IP utilizzati dai computer per comunicare tra loro → associa i nomi dei domini ai numeri degli indirizzi IP.
Senza il DNS l'utente dovrebbe digitare manualmente l'indirizzo IP per raggiungere un sito web

Struttura del DNS
Il DNS è organizzato in una struttura gerarchica e distribuita, rappresentata come un albero di domini. Questa struttura incluse:

1. Root Domain (Dominio Radice)
   Questo è il livello più alto nella gerarchia DNS, rappresentato da un punto (.), il quale contiene i server radice che forniscono informazioni sui domini di primo livello
   Es. Se si cerca www.google.com, il server radice ti indirizzerà verso i server responsabili del dominio .com
2. TLD (Top-Level Domain o Dominio di Primo Livello)
   Sono i domini subito sotto la radice, come .com, .org, .net, .it, ecc e so dividono in Domini generici usati globalmente (.com, .org, .net) e Domini geografici i quali associano un dominio a un paese o territorio (.it, .fr)
3. Second-Level Domain (dominio di Secondo Livello)
   È il nome registrato sotto un TLD
   Es. google.com, il dominio di secondi livello è google
4. Subdomain (Sottodominio)
   È un dominio creato sotto un dominio di secondo livello.
   Es. mail.google.com, mail è un sottodominio di google.com

Tipologie di reti - Confronto

Caratteristica	PAN	LAN	MAN	WAN
Estensione geografica	Pochi metri	Fino a qualche chilometro	Fino a una città	Regioni, Paesi, continenti
Velocità	Variabile (fino a 3 Mbps - Bluetooth)	Elevata (fino a 10 Gbps o più con Ethernet)	Media (10 Mbps - 1 Gbps)	Relativamente bassa (10 Mbps - 1 Gbps)
Tecnologie utilizzate	Bluetooth, USB, ZigBee	Ethernet, Wi-Fi	Fibra ottica, Wi-Fi, tecnologie cablate	Internet, fibra ottica, satellite
Proprietà	Personale	Privata	Privata o pubblica	Pubblica o mista
Costo	Molto basso	Basso	Medio	Alto
Affidabilità	Alta	Molto alta	Alta	Variabile (dipende dalla tecnologia)
Utilizzo	Collegare dispositivi personali	Collegare dispositivi in una rete locale	Collegare LAN in un'area metropolitana	Collegare LAN e MAN a grandi distanze
Esempi	Smartphone e smartwatch connessi	Rete Wi-Fi domestica	Collegamento tra uffici aziendali in città	Internet, rete aziendale multinazionale

Indirizzo IP

Un indirizzo IP è un numero univoco assegnato a ogni dispositivo connesso a una rete che utilizza il protocollo internet. Serve a identificare e localizzare un dispositivo nella rete, permettendo così la comunicazione tra dispositivi

Gli indirizzi IP possono essere di due tipi

1. IPv4 → composto da 32 bit (4 numeri separati da punti) dove ogni numero può variare tra 0 e 255. Offre circa 4,3 miliardi di combinazioni ma con l'aumento dei dispositivi connessi gli indirizzi IPv4 si stanno esaurendo
2. IPv6 → composto da 128 bit (8 gruppi di numeri esadecimali separati da due punti) Offre un numero virtualmente illimitato di combinazioni, risolvendo il problema dell'esaurimento degli IPv4

Ogni dispositivo deve avere un indirizzo IP unico nella rete in cui opera per evitare conflitti. In una rete globale come internet, gli indirizzi IP sono assegnati in modo che siano univoci a livello mondiale. Gli indirizzi IP hanno una struttura gerarchica (in 192.168.1.10) dove 192.168.1 identifica la rete e .10 il dispositivo

L'indirizzo IP può essere **statico** quando non cambia nel tempo ed è quindi ideale per server o dispositivi che devono essere sempre raggiungibili oppure **dinamico** quando è assegnato temporaneamente dal DHCP (Dynamic Host Configuration Protocol) ed è usato per i dispositivi che non richiedono una configurazione permanente.

Oltre a ciò l'indirizzo IP può essere **pubblico** (ID Pubblico) ovvero è un indirizzo univoco utilizzato per identificare un dispositivo su internet o **privato** (ID Privato) quando è un indirizzo univoco all'interno di una rete locale. Questi ultimi non sono raggiungibili direttamente da internet

Formato dei pacchetti
Un pacchetto è l'unità base di dati trasmessa attraverso una rete. È suddiviso in diverse sezioni che permettono ai dispositivi di inviare e ricevere i dati correttamente. Il formato di un pacchetto dipende dal protocollo utilizzato (IPv6, IPv6, TCP, UDP).
Un pacchetto è composto da:

- Header (intestazione) → contiene informazioni di controllo necessarie per la consegna del pacchetto (indirizzi sorgente e destinazione, tipo di protocollo, checksum)
- Payload (dati) → contiene i dati effettivi da trasmettere
- Trailer (coda) → non è sempre presente e può includere informazioni di controllo come una checksum o dati per rilevare errori

Modalità di interazione tra processi dell'applicazione di rete
Le modalità di interazione tra i processi di rete si riferiscono ai diversi modi in cui i dispositivi o i software in rete possono comunicare o scambiare dati tra di solo

1. Peer-to-peer (P2P)
   In un sistema Peer-to-Peer ogni dispositivo (peer) ha sia il ruolo di client che di server. Questo significa che ogni peer può sia inviare che ricevere dati da altri peer senza la necessità di un server centrale. Questa modalità è affidabile perché poiché la rete è distribuita, la perdita di uno o più peer non influisce sul funzionamento globale
2. Client-Server (C/S)
   In questo modello ci sono due tipi di entità: client e server. Il client è il dispositivo o software che invia richieste mentre il server è il dispositivo che risponde alle richieste, gestendo le risorse e i dati. È una modalità meno affidabile del P2P perché se il server è fuori servizio i client non possono ricevere risposte
3. Master-Slave (M/S)
   In questo modello c'è una comunicazione unidirezionale in cui il master controlla e gestisce il comportamento dei slave. Gli slave eseguono compiti specifici dati dai master, sono quindi passivi e si sincronizzano con il master che coordina tutte le operazioni. Gli slave non comunicano tra loro
4. Publish-Subscribe (Pub/Sub)
   In questo modello i partecipanti sono suddivisi tra publisher e subscriber. I publisher inviano dati (messaggi) che vengono "pubblicati", mentre i subscriber si "iscrivono" per ricevere tali messaggi. Questa comunicazione è generalmente asincrona ovvero oil publisher invia messaggi senza sapere chi li riceverà e i subscriber li ricevono quando si iscrivono
5. Broadcast
   Il broadcast è una modalità di comunicazione in cui un messaggio viene inviato da una singola fonte a tutti i dispositivi sulla rete, senza destinazione specifica, ma solo quelli che sono in grado di riceverlo lo processano

Modalità	Descrizione	Esempi pratici	Caratteristiche principali
P2P (Peer-to-Peer)	Ogni dispositivo è sia client che server.	BitTorrent, Skype, Blockchain	Decentralizzazione, alta scalabilità, peer equivalenti
C/S (Client-Server)	Client invia richieste, server le risponde.	Web, email, database	Centralizzazione, comunicazione richiesta-risposta
M/S (Master-Slave)	Un dispositivo (master) controlla più dispositivi (slave).	Sistemi di controllo industriale	Controllo centralizzato, sincronizzazione passiva
Pub/Sub (Publish-Subscribe)	Publisher invia messaggi, i subscriber li ricevono.	MQTT, notifiche push, live streaming	Asincrono, scalabilità, indipendenza tra publisher e subscriber
Broadcast	Un messaggio è inviato a tutti i dispositivi sulla rete.	ARP, DHCP, trasmissione video in rete locale	Comunicazione universale, inefficienza in reti grandi

Prestazione di una rete o qualità del servizio
La prestazione di una rete e la qualità del servizio(QoS) sono concetti cruciali per garantire che una rete funzioni in modo efficace e soddisfi le esigenze degli utenti e delle applicazioni.

- La prestazione di una rete si riferisce alla capacità di una rete di trasmettere dati in modo efficiente, garantendo tempi di risposta adeguati e affidabilità nel trasferimento delle informazioni. La prestazione è determinata dalla latenza, dalla banda, dalla perdita di pacchetti, dell'affidabilità e dalla disponibilità
- La qualità del servizio si riferisce a un insieme di tecniche che permettono di garantire che determinate applicazioni e tipi di traffico ottengano la priorità sulla rete in base alle loro esigenze

Sicurezza delle reti
Gli obiettivi principali della sicurezza nelle reti sono riassunti nel CIA Triad (Confidentiality, Integrity, Availability)

- Confidenzialità (Confidentiality)
  Garantire che le informazioni siano accessibili solo alle persone autorizzate. La riservatezza dei dati è fondamentale per proteggere le informazioni sensibili da accessi non autorizzati. Le tecniche utilizzate sono: crittografia, autenticazione forte e controllo degli accessi
- Integrità (Integrity)
  Assicurarsi che i dati non siano alterati, distrutti o manipolati senza autorizzazione. Ogni modifica ai dati deve essere tracciabile e verificabile. Le tecniche utilizzate sono hashing, firme digitali e firme elettroniche
- Disponibilità (Availability)
  Garantire che i dati e le risorse di rete siano disponibili e accessibili quando richiesti. Gli attacchi che mirano a ridurre la disponibilità, come i DoS devono essere prevenuti. Tecniche utilizzate sono: ridondanza, backup, protezione contro gli attacchi Dos/DDoS

Le reti sono vulnerabili a vari tipi di minacce e attacchi quali:

- Attacchi DoS e DDoS (Denial of Service e Distributed Denial of Service)
  I DoS sono attacchi che mirano a sovraccaricare un server o una rete per renderla non disponibile agli utenti legittimi, mentre i DDoS sono una variante in cui l'attacco viene effettuato da più dispositivi distribuiti, aumentando l'intensità e la difficoltà di difesa
- Accesso non autorizzato
  Gli hacker o gli utenti non autorizzati possono tentare di accedere ai sistemi e risorse di rete senza il permesso adeguato
- Man-in-the-Middle (mInM)
  In questo tipo di attacco, un malintenzionato intercetta e potenzialmente altera le comunicazioni tra due dispositivi. Questo può compromettere la confidenzialità e l'integrità dei dati trasmessi
- Malware
  I virus, worm, trojan e ransomware sono forme di malware che possono infettare una rete, compromettere i sistemi e causare danni

Lezione 28 Novembre 2024

ASCII 8 bit
UNICODE 16 bit
BASE 64 bit

come si codifica un messaggio di posta,pagina web
Pila ISO/OSI
NAT (del provider)

REGISTRAZIONE

Nelle reti di per sé c'è qualcuno che manda cose ad un altro e quest'ultimo risponde. 50 anni fa si sono inventati il fatto di organizzare il software a pila dove la parte più alta è il software di livello applicativo, cioè se questi si stanno scambiando la mail, la parte più alta è proprio il livello applicazione. Il software di livello applicazione è importante

Nelle reti è importante la standardizzazione perché serve per comunicare ma se non standardizzi la comunicazione come fai a effettuarla → la base della comunicazione è creare degli standard

Nel caso della posta elettronica, questa ha un approccio client-server dove, se il mio dispositivo è il client è lui che va a richiedere all'applicazione se sono presenti nuovi messaggi di posta e non viceversa. Può essere percepito come un inganno in quanto sembra che quando mi mandino una mail io la ricevi istantaneamente ma in realtà è il mio dispositivo, client, che continua a chiedere al server se "c'è posta per me" dando l'illusione che mi arrivi direttamente una volta spedita dal mittente. Questo è un following di richiesta
I due livelli applicativi non sono in collegamento diretto tra loro
La prima posta elettronica era solo testuale, ora invece c'è tutta una codifica degli allegati e degli altri destinatari in caratteri ASCII
Gli ASCII sono un byte per carattere (1 byte sono 8 bit). Quanti possibili caratteri posso codificare?

Calcolare da bit a byte a kb a … con potenze e operazioni

Questa è la standardizzazione delle reti

La nuova codifica che seguiamo oggi è l'unicode che è a 16 bit

Codifica base64 che trasforma un qualsiasi file binario in una sequenza di caratteri per poi trasformarlo dall'altra parte. Questa codifica non è una compressione ma un'espansione

MANCA PARTE DUE REGISTRAZIONE

Lezione 19 Dicembre 2024

(prima e seconda interfaccia di rete) Connessioni bluetooth e wifi (livello fisico e data link), usano stessa frequenza 2,4 ghZ
Usano la stessa antenna
(3)NFC (near field communication)
(4)USB, telefono per tethering (modalità) → utilizza interfaccia di rete del telefono per rete pc
Viene visto come un ethernet

Ethernet collegato a switch

Onde effetto doppler

Lettura IPv6
Due punti ripetuti ::
Indirizzo MAC e le sue parti (6 byte totali)

- i primi tre byte sono assegnati al produttore da IEEE
- gli altri 3 vengono assegnati in maniera incrementale da parte del produttore

MAC spoofing

IF config -a comando per linux
IP config /all → windows

Lettura numeri binari negli indirizzi IP e netmask

400ms limite massimo di ritardo accettabile dal cervello umano

comando nslookup

Lezione 23 Gennaio 2025
Metodi misurazioni ascii, bit, byte,

WireShark
LibPCap? - WinPCap?
Indirizzo destinazione per primo in modo tale che se messaggio non indirizzato a me la scheda di rete non lo considera
Libreria → non di vede, fa la cattura …
Parte grafica → mostra info su cattura con colori diversi per specificare il tipo

- in nero errori

Campo type per capire i byte del payload del pacchetto
Indirizzo destinazione e sorgente sono indirizzi MAC

10100110 → 8 bit = 1 byte = 256 possibilità
Codifica Unicode con 2 byte a livello mondiale