Argomenti Reti di Calcolatori

Definizioni/Semplici Spiegazioni

LEGGENDA

COMPLETA: paragrafo visto e rivisto.
QUASI COMPLETA: appunti presi a lezioni + slide, da rivedere per sistemare solo qualche dettaglio.
DA INTEGRARE: Appunti presi a lezioni con parte o nulla delle slide.
IN FASE DI ELABORAZIONE: paragrafo nel quale sto integrando le slide

---
Lezione 2 QUASI COMPLETA

Componenti di una rete:
- Hardware (apparati di interconnessione e apparati per il controllo della trasmissione)
- Software (Protocolli e Drivers)

Funzionalità di una rete: Fornisce una comunicazione efficiente e in grado di connettere ambienti applicativi diversi, rileva e corregge automaticamente dati corrotti, persi o duplicati. Si occupa anche di trovare i cammini ottimali da una specifica sorgente a una specifica destinazione.

Rete telematica: Insieme di dispositivi informatici collegati reciprocamente tra loro.

Una rete di telecomunicazione può essere definita come un sistema distribuito che permette la trasmissione di informazioni da un suo capo all'altro consentendo un indirizzamento universale. La rete deve implementare funzionalità per trasportare le informazioni e funzionalità per l'indirizzamento e per l'instradamento delle comunicazioni.

Un modello che soddisfa la definizione di rete di telecomunicazione deve avere:
- Host, dispositivi connessi ad una rete
- Link, collegamenti tra punti tramite nodi di commutazione
- Nodi di commutazione, questi si occupano di riconoscere le richieste per l'apertura di una connessione e fare in modo che i dati giungano a destinazione

DTE (Data Terminal Equipment): Complesso costituito dal sistema (unità di elaborazione), dal terminale (punto di ingresso ed uscita per l'utente) e dalle relative risorse (driver e protocolli) collegati in rete per la trasmissione dei dati. Un DTE può essere qualsiasi cosa connessa ad un rete come utente finale. L'interconnessione dei vari DTE per lo scambio di dati è lo scopo della rete.

DCE: Switch o router in ambito Ethernet

Modalità di trasmissione:

- Punto a punto: Quando un circuito collega due soli DTE. I vantaggi sono semplicità della gestione e tempi di attesa nulli. Gli svantaggi sono elevato il costo numero linee pari linee collegamento.

- Multipunto: Consiste nel mettere più di due DTE sulla stessa linea, in questo caso possono nascere problemi di contesa.

- Broadcast: Queste sono dotate di un unico canale di comunicazione che è condiviso da tutti gli elaboratori. Questa manda messaggi (pacchetti) da un elaboratore che sono ricevuti da tutti gli elaboratori connessi.

Funzionamento Reti: Un elaboratore riceve un pacchetto, esamina l'indirizzo di destinazione se questo

coincide con il proprio, lo elabora, altrimenti lo ignora.

BroadCasting: Reti mandano un pacchetto per tutti gli indirizzi.

MultiCasting: Vogliamo inviare il pacchetto solo ad un sottoinsieme di elaboratori.

Topologie di rete: Una topologia di una rete è la configurazione geometrica dei collegamenti tra i vari componenti della rete. La configurazione più comune è la rete ad albero.

Rete ad albero: In questa rete il traffico di dati va dai nodi dei livelli più bassi verso i nodi intermedi o verso il nodo del livello più alto, il quale è il nodo più potente della struttura.

- Problemi rete ad albero: Visto che il responsabile della gestione della rete è principalmente il nodo principale se questi ha un sovraccarico si ha un rallentamento dei servizi per tutti gli utenti, nel peggiore dei casi la "caduta" del nodo principale rende inutilizzabile l'intera rete. Per questo si possono adottare altri nodi che "sostituiscono" il principale.

Rete a stella: La sua configurazione è simile a quella ad albero con una fondamentale differenza, non c'è una distinzione a livelli e tutte le funzioni degli utenti periferici sono realizzate nel nodo centrale.

Rete a dorsale: Questa configurazione è composta da un unico cavo che collega tutte le stazioni. La trasmissione di una stazione viene ricevuta da tutte le altre. Visto che il cavo è unico c'è bisogno di un meccanismo di arbitraggio che decide chi può trasmettere. Il vantaggio della rete dorsale è che la tecnologia di accesso è molto semplice. Lo svantaggi della rete dorsale c'è un portante che serve tutte le stazioni ed una eventuale sua interruzione mette fuori uso l'intera rete, infine la mancanza di punti di concentrazione rende difficile l'individuazione di punti di malfunzionamento.

Rete ad anello: Resa popolare dalle LAN, in questa la trasmissione è unidirezionale, anche qui abbiamo bisogno di un meccanismo di arbitraggio.

Rete a maglia: Consiste nel collegare le varie stazioni con diversi circuiti. La rete a maglia assicura buone prestazioni visto che il traffico viene ripartito in vari percorsi, inoltre essendoci percorsi multipli è anche più affidabile, di contro però avere dei collegamenti "extra" richiede dei cosi più elevati.

Trasmissione Simplex: In questo caso i dati viaggiano in unica direzione. Alcuni esempi sono le reti di comunicazione delle agenzie stampa, generalmente però non viene utilizzato per la comunicazione dei dati, questo perché quando si trasmettono dei dati è necessario verificare la correttezza dei dati e segnalarla cosa non possibile in un flusso unidirezionale.

Trasmissione Half-duplex: Nella Hal-duplex i dati possono viaggiare in entrambe le direzioni ma non contemporaneamente.

Trasmissione full-duplex: In questo caso i dati possono viaggiare contemporaneamente in entrambe le direzioni, questo è particolarmente indicato per le reti a configurazioni multipunto.

La trasmissione Half-duplex richiede un circuito a due fili con un filo per i dati e l'altro per il ritorno elettrico mentre il full-duplex richiede il doppio doppino telefonico ossia 4 fili i cui due per i dati e due per i rispettivi ritorni elettrici. Comunque la trasmissione full-duplex è possibile anche sul circuito a due fili ma sarebbe più lenta.

Commutazione: Processo che determina il percorso che le informazioni inviate dal mittente devono seguire per raggiungere il destinatario.

Commutazione di Pacchetto: Si basa sulla suddivisione del messaggio in più unità autonome. Ognuna di esse ha le opportune informazioni di controllo come identificativi del mittente e del destinatario e numero

d'ordine del pacchetto all'interno dell'intero messaggio. Ogni pacchetto è instradato indipendentemente e la rete non ne garantisce l'inoltro e la ricezione nel giusto ordine. Questa commutazione può avere due implementazioni.

1) Implementazione Rete di Datagrammi: In questa implementazione ogni pacchetto viene instradato in modo indipendente verso la destinazione e non segue un percorso prestabilito, in ogni dispositivo si decide il successivo.

2) Implementazione Rete di circuiti virtuali: In questo caso viene calcolato un percorso prima che inizi la comunicazione e i pacchetti seguono un percorso stabilito e arrivano nello stesso ordine in cui sono stati trasmessi.

Commutazione di Circuito: Con la commutazione di circuito vi sono una serie di dispositivi di commutazione con i quali si determina una connessine fisica diretta che simula un cavo tra le due stazioni. Questa connessione è assegnata permanentemente alla coppia di stazione ed è mantenuta fino al termine della comunicazione. Questa commutazione ha un tempo di attivazione della connessione, inoltre ha una bassa efficienza nell'uso del mezzo dato visto che la connessione rimane attiva anche quando i due utenti non la stanno utilizzando.(Telefono)

Pacchetto vs Circuito: La commutazione di pacchetto ottimizza la gestione delle risorse ed è estremamente efficiente per pacchetti di piccole dimensioni, risulta per meno efficiente per il trasporto di dati di grande quantità.

DSE (Data Switching Equipment): Anche detto nodo di commutazione è un nodo intermedio della rete la cui funzione principale è commutare il traffico tra DTE non direttamente collegati tra loro. Il DSE sceglie il percorso di rete che i messaggi devono seguire per arrivare alla loro destinazione. Il DSE effettua scelte anche in base al carico delle linee favorendo in questo modo il controllo della congestione.

Protocollo: Serie di norme e convenzioni per lo scambio di dati tra due elementi. Esistono molti livelli di protocolli si va dal più basso che regola il modo di trasmettere segnali sulla linea (protocollo di connessione) ad un livello più alto che indica come interpretare i dati a livello applicativo.

Routing Protocol: Dato un DTE di destinazione e un DTE sorgente la scelte di quale strada usare per connetterli spetta al routing protocollo.

Protocollo di linea: Necessario al passaggio di dati su ciascuna linea da un punto ad un altro. Interviene dopo il routing protocol.

Protocollo di trasporto: Questo invece si concentra sulla comunicazione tra la sorgente e al destinazione.

LAN (Local Area Network): Sono reti private ed hanno un estensione di qualche KM si espandono in edifici.

WAN (Wide Area Network): Queste si estendono invece a livello mondiale e il numero di terminali collegati è molto alto, hanno spesso una struttura a maglia.

MAN: Punto di incontro tra LAN e WAN ed hanno una estensione urbana.

Connection Oriente Mode: I DTE si assicurano della presenza della linea e viene instaurata la connessione che dura il tempo necessario per lo scambio dati. La connessione è gestita dal software dei DTE che si occupano di gestire ritmo di interscambio e il controllo delle regole per quest'ultimo. Inoltre sono capaci di interrompere la controparte e di controllare errori ed eventualmente correggerli.

Connectionless mode. Un DTE può inviare un messaggio ad un'altra DTE anche se questo non è presente in linea, il vantaggio è non sono necessari servizi di controllo. Il suo problema principale è il

controllo degli errore che possono verificarsi. D'altra parte questa mancanza è un bene in alcuni casi poiché su linee affidabili questi controlli sono inutili. Sarebbe quindi buona norma affidare il controllo alle applicazioni

Internetwork: Quando reti diverse (LAN WAN MAN) sono collegate fra loro. In questo caso nascono spesso problemi se vogliamo collegare reti progettualmente diverse, in questo casi si deve ricorrere a router di multi-protocollo dette Gateway che oltre ad instradare i pacchetti da una rete all'altra effettuano le operazioni necessarie per il trasferimento.

Sottorete (subnet): Nelle WAN è l'insieme dei DSE e delle line di trasmissione

Rete (network): L'insieme costituito da una subnet e da tutti gli host collegati.

Lezione 3 QUASI COMPLETA

Progettazione reti di computer: Le reti di computer sono progettate secondo modelli concettuali stratificati, ogni livello di occupa di un particolare aspetto della comunicazione di rete.

Incapsulamento: In una pila di protocolli a più livelli, ognuno riceve un carico utile dal livello superiore e forma un PDU. Che a suo volta viene passato al livello inferiore

PDU (Protocol Data Unit): Composta da un'intestazione con informazioni sul controllo e un carico utile. In pratica è un blocco di dati trasmesso attraverso la rete.

Deincapsulamento: Può succedere che il carico utile sia troppo grande per una singola PDU, in questo caso il passaggio viene suddiviso in una sequenza di pacchetti (frammentazione), il ricevente effettua poi riassemblaggio.

Modello ISO OSI: Modello concettuale che descrive le funzioni di comunicazione di una rete dividendola in livelli distinti. Ognuno di questi svolge un compito specifico nell'elaborazione dei dati durante la comunicazione tra dispositivi su una rete.

Livello fisico: Trasmissione di bit sul canale fisico di trasmissione.

Livello del Data Link: Trasforma la linea fisica in una linea in cui gli errori di trasmissione sono sempre segnalati. Divide le informazioni in pacchetti e li trasmette attraverso il mezzo fisico. Gestisce anche l'eventuale duplicazione dei frame ricevuti e la sincronizzazione dei mittenti. Infine gestisce l'accesso al canale di trasmissione condiviso.

Livello del NetWork: Gestisce l'indirizzamento universale dei nodi in rete e l'instradamento dei pacchetti. In alcuni casi si occupa anche della gestione della congestione e di controllare il flusso. Implementa anche interfacce per la comunicazione tra reti di tipo diverso.

Livello del Trasporto: Assicura un servizio privo di errori end to end (quindi per l'intero percorso) con l'ordine corretto di ricomposizione. Gestisce anche l'invio di messaggi a più applicazioni sullo stesso host e fornisce il servizio di recapito dei messaggi senza garanzia di arrivo.

Livello Application: Implementa specifici servizi applicativi che interfacciano direttamente l'utente.

Livello di Presentazione: In questo livello ci si limita alla traduzione dei dati che viaggiano sulla rete in formati astratti.

Lezione 4 (Livello Fisico) QUASI COMPLETA

Segnale: Un segnale x(t) rappresenta l'andamento nel tempo t di una grandezza fisica x.

Segnale analogico: Se T (dominio) è un sottoinsieme continuo in R e D (codominio) è un sottoinsieme di R o C, ovvero T è costituito da un infinità non numerabile di numeri reali e D è costituito da un infinta non numerabile di numeri reali o complessi. Spesso usati per applicazioni broadcast e sono trasmessi con riferimenti analogici unidirezionali (radio).

Segnale digitale (numerico): Se T (dominio) è un sottoinsieme continuo in R e D (codominio) è costituto da un numero finito di elementi. Utilizzato per le reti dati, video ed altro. Queste vengono digitalizzati ovvero il segnale che trasporta un bit è comunque analogico anche se l'informazione è associata è numerica.

Segnale sinusoidale definito con:

- Ampiezza: Livello massimo del segnale.
- Frequenza fondamentale: La frequenza più bassa che un sistema oscillatorio è in grado di raggiungere.
- Fase: misura della posizione relativa del segnale ad un dato istante
- Periodo: Intervallo temporale della periodicità del segnale ed è dato dal reciproco della frequenza.
- Lunghezza d'onda: Distanza in metri tra due punti di uguale fase in periodi adiacenti, ovvero la distanza tra due punti più alti dell'onda.
- Velocità di propagazione: La velocità con cui si sposta una cresta d'onda nello spazio, dove per cresta si intende il punto più alto di un'onda

Segnale periodico: Un segnale che ripete i suoi valori

Duty Cycle: Frazione di tempo che un segnale passa in uno stato attivo in proporzione al tempo totale considerato.

Potenza: Come si dissipa in un trasduttore.

Un segnale viene acquisito e trasformato in una grandezza elettrica grazie ai trasduttori.

Sistema: Blocco che trasforma un segnale in ingresso in uno di uscita attraverso una trasformazione chiamata funzione di trasferimento.

- Sistema lineare: Sistema in cui è valido il principio di sovrapposizione

- Sistema permanente: Sistema che non varia dal tempo.

Filtro: Quando un sistema è lineare e permanente.

Impulso: Segnale di durata brevissima e di ampiezza elevatissima che ha un area definita.

Risposta impulsiva: La risposta di un filtro in cui viene mandato in ingresso un impulso.

Serie di Fourier: Strumento matematico utilizzato per rappresentare un segnale periodico come una somma di funzioni trigonometriche (seni e coseni) o esponenziali. Questo approccio permette di decomporre il segnale complesso in componenti più semplici, chiamate armoniche.

Coefficienti di Fourier: Ampiezze delle armoniche, più coefficienti ho più mi avvicino al segnale iniziale. La loro sequenza è detta spettro del segnale periodico.

Rappresentazione spettrale: Grafico delle ampiezze rispetto alle frequenze di cui è composto il segnale.

Canale: Mezzo che permette il trasferimento di segnali tra mittente e destinatario, e la sua capacità di

trasmettere armoniche dipende dalla larghezza di banda disponibile.

Trasformata di Fourier: Serve per sviluppare un segnale non periodico in Fourier, posso vedere quel segnale con un periodo infinito e applicare la serie di Fourier, queste hanno un modulo e una fase.

Antitrasformata di Fourier: Operazione inversa che riporta una funzione dal dominio della frequenza al dominio del tempo, ricostruendo il segnale originale.

Funzione di trasferimento di un filtro: (Provare a descrivere cosa sia). Questa può essere rappresentata con il diagramma di Bode che consiste in due grafici che rappresentano rispettivamente l'ampiezza e la fase della funzione complessa risposta in frequenza.

Lavoriamo nel dominio delle frequenze perché ci è più facile.

Prendo un filo di rame quando passa corrente ha resistenza e condensatore RC [Filo è un sistema], di conseguenza una linea di trasmissione può essere vista come un circuito RC.

Faccio passare il segnale lo prendo e lo passo in Fourier dove ottengo una frequenza ed una base.

Frequenza di taglio: La frequenza per la quale si ha il dimezzamento del livello del segnale.

Segnale limitato nella banda [-W,W]: Un segnale si definisce tale se la sua trasformata di Fourier è identicamente nulla per valori diversi da [-W,W]. Definiamo quindi banda di un segnale l' intervallo nel dominio delle frequenze in cui la serie di Fourier non è nulla. La quantità di W si misura in Hz e costituisce la larghezza di banda del segnale

Segnale di banda base: Gamma di frequenze occupate da un segnale che non è stato modulato a frequenze più alte.

Ogni canale di comunicazione ha una banda specifica che definisce quali frequenze possono essere trasmesse. Il canale agisce come un filtro, attenuando le frequenze fuori dalla sua banda e annullando completamente quelle non supportate, lasciando passare solo le frequenze all'interno della sua banda.

Filtraggio analogico: Manipolazione di un segnale nel dominio delle frequenze per poter selezionare una parte dello spettro del segnale stesso.

Fasi di filtraggio:

1) Si ha un segnale con un spettro.
2) Il segnale viene inviato in un filtro che consente il passaggio di solo alcune armoniche.
3) Il segnale in uscita dal filtro è privato di parte del suo spettro.

Frequenza passa-basso: passano frequenze più basse di una valore.
Frequenze passa-alto passano frequenze più alte di una frequenza.
Frequenze passa-banda: passano inalterate tutte le frequenze tra determinati valori.

Percorrendo distanze le ampiezze si abbassano e per questo utilizzo degli amplificatori, che aumentano l'energia del segnale. L'amplificazione può essere più tollerata per i segnali analogici, nei segnali digitali può portare più errori.

Trasmissione digitale: In questo caso si tiene conto dei dati e consiste nella conversione del segnale analogico in quello digitale. Per percorrere grandi distante il segnale non viene solo amplificato ma anche interpretato, questo per permettere di rigenerarlo con dei ripetitori.

Vantaggi trasmissione digitale: Si altera meno su lunghe distanze, più sicuro e utile a diverse tipologie di

dato.

Amplificatore aumenta la grandezza, ripetitore amplifica rigenera il segnale dando un segnale più pulito.

Cosa significa avere la banda doppia? Significa che una comunicazione occupa il doppio dello spazio perché le armoniche sono più grande e potrei non riuscire a metterlo nel canale, richiede anche maggiori costi.

Le interfacce prendono il segnale lo mandano nel mezzo trasmissivo e sa già che codifica utilizzo perché parlano la stessa "lingua"

Il campionamento è il processo di trasformazione di un segnale continuo (dove i suoi valori sono definiti in ogni istante di tempo) in un segnale discreto (dove i suoi valori sono definiti solo in punti specifici, determinati da un insieme discreto di valori).Il passo successivo è convertire questo segnale discreto in un segnale digitale. In un segnale digitale, i valori non possono assumere qualsiasi valore ma sono limitati a un insieme finito di livelli, quindi quantizzati. Più livelli di quantizzazione utilizziamo, maggiore è la quantità di informazione che può essere trasmessa nello stesso intervallo di tempo. Tuttavia, un numero eccessivo di livelli rende ogni singolo livello sempre più piccolo, fino al punto in cui, in ricezione, potrebbe non essere più distinguibile dal rumore.

Quantizzazione: Si divide la dinamica del segnale (intervalli di valori che un segnale può assumere) in livelli. In seguito ad ognuno si associa il livello di appartenenza. Più livelli abbiamo più il segnale quantizzato sarà simile al segnale originale.

Teorema del campionamento di Nyquist-Shannon: Il teorema del campionamento afferma che, dato un segnale a banda limitata (il segnale non contiene frequenze superiori a una certa frequenza massima), è possibile ricostruire completamente il segnale a partire dai suoi campioni se la frequenza di campionamento (frequenza con cui prendiamo "campioni" del segnale continuo, quanto spesso misuriamo il valore del segnale) è almeno il doppio della larghezza di banda del segnale. Se si utilizza un campionatore, è necessario che il segnale in ingresso abbia una banda limitata a metà della frequenza di campionamento del dispositivo.

In sintesi, il teorema del campionamento di Nyquist-Shannon ci dice quanto velocemente dobbiamo campionare un segnale per poterlo ricostruire senza perdita di informazioni

Effetto Aliasing: Sovrapposizione del segnale campionato che rende impossibile l'esatta ricostruzione del segnale originale. Per questo motivo ogni apparato di conversione analogico-digitale ha un filtro passa-basso che limita lo spettro del segnale di ingresso.

Rumore: Forma di energia indesiderata che si somma al segnale, degradandone il contenuto informativo non permettendo di rilevare tutte le informazioni trasmesse.

Codifiche: Le codifiche devono avere una sincronizzazione temporale e possono fungere anche da rilevazione di errore.

-Unipolare Rz: Prevede la trasmissione di un segnale di lunghezza T per ogni bit. Il segnale è nullo in corrispondenza del bit 0, mentre è un impulso di tensione di durata T/2 per il bit 1.

-Unipolare NRZ: Differisce dalla RZ perché il livello di tensione per il bit 1 rimane alto per tutta la durata del bit. Questa codifica ha il vantaggio di essere semplice da progettare e realizzare e ha inoltre un utilizzo efficiente della larghezza di banda. D'altro canto esiste un componente continua e delle lunghe sequenze di bit di uguale valore producono un segnale continuo senza transizioni.

-NRZ-L: Questa prevede un segnale +V per il bit 1 e -V per il bit 0 riducendo l'impatto della componente continua.

-NRZ1: Il segnale qui cambia in occasione di un bit 1.

Codifiche multilivello: Queste codifiche utilizzano tre livelli dove lo 0 indica il bit 0 mentre il bit 1 è identificato da +V e -V alternati. Questo tipo di codifica risolve il problema della sequenza di bit 1, che presentano sempre un transizione utilizzabile in ricezione. La componente continua è azzerata, utilizza una larghezza di banda inferiore e degli errori isolati possono essere visti come violazione del codice.

- Manchester:La codifica Manchester utilizza due livelli di tensione. Il bit 1 è rappresentato da un cambio di tensione: -V nel primo mezzo periodo e +V nel secondo mezzo periodo. Il bit 0 è rappresentato con una sequenza inversa. Nella codifica Manchester differenziale, il bit 1 rappresenta sempre un cambio di tensione rispetto al bit precedente, mantenendo il livello di partenza.

-B8ZS: Se ho una sequenza di 8 zeri lunga la sostituisco con una codifica precisa, scompaiano le lunghe sequenze di 0.

-HDB3: Ogni sequenza di 4 zeri viene sostituita anche qui

Modulazione: Hardware che prende due segnali e modifica nel tempo le caratteristiche di un segnale ausiliario sinusoidale. Modulazione manda una segnale nel canale aggiustato per rientrare nella caratteristiche proprie del canale. La traslazione è una delle possibili modulazioni. Vantaggi della modulazione sono la trasmissione a ponte radio la riflessione multipla. Un'altro vantaggio è la possibilità di trasmettere più comunicazioni differenti e contemporanee sullo stesso mezzo.

Tecniche di modulazione: Si può modificare l'ampiezza, la frequenza e la fase della portante.

- ASK: Si modula in ampiezza tramite un operazione semplice di moltiplicazione tra la modulante e portante. Meglio perché sono meno armoniche.
- FSK: Si realizza con due armoniche con frequenze diverse e modifica in frequenza il segnale portante in funzione del segnale modulante. Fa corrispondere frequenze ai due valori del bit. Un requisito per questa tecnica è la continuità di fase negli istanti di transizioni di frequenze.
- PSK: Si realizza modula in fase una portante, rappresentiamo solo tra 0 e 1
- QPSK Prendo tutto lo spettro dei radianti posso rappresentare più informazioni, è come se facessi più livelli sul segnale sinusoidale

Tecniche di multiplazione

TDM: Divisione nel tempo "fare i turni", divido il il canale in quanti di tempo e ne assegno ad ognuno uno. Divido il flusso dati in frame e se ha una successioni di informazioni manda un pacchetto per volta e lo slot è il tempo che il pacchetto impiega dall'origine alla destinazione.

SDM: Suddivisone fisica del canale in pezzi, in due linee separate, il problema è che deve dividere fisicamente il canale.

FDM e WDM: Divido in base o alla lunghezza d'onda o alla frequenza.

CDM: Differenziazione dei dati con diversa tipi di codifica.

SDM vs TDM: SDM tanti fili quanti i segnali nella TDM il filo è uno ed ognuno ha un slot assegnato. TDM è difficile perché dobbiamo sincronizzarci e devono sapere esattamente quando inizia lo slot e devono sapere sempre a chi tocca e questo non è sempre facile. Anche nel caso della multiplazione questa non è precisa, per esempio se non si capisce quando inizia lo slot ci sono delle collisioni.

TDM Deterministico: Questo è più semplice da fare ma ogni canale di comunicazione è identificato dalla sua posizione in termini di slot temporali all'interno della trama.

TDM Statistico (più efficiente, esempio pratico ethernet) divido le risorse in base agli utenti, nel TDM statistico le trame dipendono dal massaggio da mandare, non ha una taglia fissa. Il problema è che non so dove possa andare ed ho necessità di aggiungere nella trama per capire dove va. Ho bisogno di bufferizzazione perché non è detto che quando porto il dato questa sia disponibile a riceverlo. In base al protocollo. Ho un efficienza del mezzo.

Mezzi trasmissivi: I mezzi fisici di trasmissione si classificano in mezzi guidati come quelli elettrici o ottici e mezzi non guidati come onde radio. Un mezzo trasmissivo ottimale è caratterizzato da una bassa resistenza bassa capacità e bassa induttanza, ovvero un mezzo poco dispersivo e poco dissipato.

Schermatura generalizzata: Serve a ridurre la sensibilità e l'emissione di disturbi elettromagnetici e possono anche migliorare anche le caratteristiche del cavo.

Rifrazione: Fenomeno per cui un raggio luminoso passando da un mezzo trasparente ad un altro trasparente cambia direzione nel punto in cui attraversa la superficie di separazione dei due mezzi.

Finestra operativa: Range di lunghezza d'onda.

Il mezzo di trasmissione per il wireless è l'aria. Trasmettitore a cui è collegata un antenna ricevente che trasforma in elettrico e poi passa al trasmettitore. Antenna sia per trasmettere che per ricevere con un elemento che fa da switch tra le due modalità. Nel mezzo trasmissivo si propagano le onde elettromagnetiche. Abbiamo due campi elettrico e magnetico, nei quali si muove l'onda sinusoidale. Le onde elettromagnetiche possono essere viste su spazio temporale e e spaziale. La frequenza è inversamente proporzionale alla lunghezza d'onda.

Antenne trasforma segnali elettrici in radio-frequenza. Un 'antenna ha un ampiezza (capacità di trasmettere o ricevere in un'area) ed un guadagno (rapporto tra il caso reale e il caso immaginario).

Pathos: Quanta rapporto potenza manda e potenza ricevuta, quanto si è dissipato nel tragitto.

Segnale ridondate serve per sopperire al degrado dell'informazione.

Frequency hopping: Saltare da una frequenza ad un altra, questi cambi di frequenza permettono di migliorare la sicurezza e la resistenza alle interferenze nel trasferimento dei dati.

Radiodiffusione: Trasmissione wireless analogica.

Trasmissione via ponte radio: Metodo affidabile ed efficiente per trasferire dati tra due punti distanti utilizzando onde radio, antenne direzionali e processi di modulazione per la trasmissione e ricezione dei segnali.

Satelliti: Utili in futuro per il 6g e usati in maniera complementare per coprire dove le antenne non arrivano.

Lezione 5 Data Link QUASI COMPLETA

Riceve dal livello di rete pacchetti e forma delle trame che passa al livello fisico. Il modello data link deve dare un trasferimento affidabile a quel canale.

Caratteristiche: Framing impacchettare dati in una struttura detta frame, multiplazione perché ho più utenti che usano quel mezzo fisico, inoltre visto che la trasmissione deve essere affidabile, si occupa di verificare se ci sono degli errori e provare a correggerli ed evitare la collisione. Inoltre deve fare controllo di flusso altrimenti lo porta alla saturazione. Il problema è che non conosce il canale sottostante ma vede il servizio che offre il livello fisico (Ethernet sa che c'è filo no quale). Cercare di implementare un

opportuno modo di comunicazione.

DLL (Data Link Layer): Facilita la comunicazione con il livello superiore. Gestisce la trasmissione dei dati con tre diverse classi di servizio tra cui scegliere in base alle necessità specifiche.

Differenziazione del servizio: La differenziazione del servizio è importante quando non tutte le caratteristiche sono necessarie. Ad esempio, potrebbe non essere richiesto un servizio affidabile se il canale di comunicazione è già affidabile di per sé.

Gestione degli errori: La gestione degli errori utilizza la ridondanza temporale, ritrasmettendo i dati, e la ridondanza spaziale, aggiungendo informazioni extra per tollerare e recuperare gli errori automaticamente.

Organizzazione del flusso di bit e controllo della trama: Il DLL organizza i flussi di bit in frame, includendo meccanismi di controllo per la sincronizzazione. Per gestire gli errori, identifica le trame utilizzando combinazioni specifiche di bit e byte, con l'aggiunta di flag per marcare l'inizio e la fine delle trame. La lunghezza della trama è espressa in byte. Sequenze ASCII come DLE vengono utilizzate prima e dopo la trama per delimitarla, con l'aggiunta di bit se una sequenza simile compare nel pacchetto stesso per evitare conflitti.

Violazioni di codifica: La rappresentazioni di bit non seguono le codifiche e questo è un modo per far capire che sta iniziando la trama.

Rilevazione dell'errore: Replicazione di bit, perdita di bit..., al livello due nell'header si aggiunge un check-sum che calcolo prima che mi arriva, una volta arrivato ricalcolo il cheksum se non è uguale ci sono errori.

Controllo di parità si vedono i bit alti se vedo che i numero di bit alti è pari aggiungo 0 o 1 in base a se voglio che i bit siano pari o dispari. Unico bit di parità serve solo a controllare non a correggere. Parità bidimensionale calcolo il bit di parità sulle righe e sulle colonne di una matrice di "parole".

I campi di Galois rappresentano una fondamentale struttura matematica applicata nelle reti per migliorare l'affidabilità delle comunicazioni e per garantire la sicurezza delle informazioni trasmesse attraverso l'uso di codici correttori di errori e algoritmi crittografici avanzati.

CRC: Somma di elementi sul campo di Galois dove i bit sono i suoi simboli.

Adattatori: Prende il pacchetto dal livello superiore e lo mette nelle trame.

Codice CRC: Rilevamento degli errori migliorie lavorano sul campo di Galois. Data una parola aggiungo un codice di controllo. Una rappresentazione dei valori binari è per mezzo di polinomi. Da una sequenza posso fare un polinomio di grado n (numero di cifre) - 1. Elementi polinomiali sono gli elementi che hanno un bit alto. Lo trasformo in polinomio per poter utilizzare l'algebra polinomiale. Aggiungo qualcosa affinché la risultante sia divisibile per il polinomio. Dalla ricezione arriva un valore con bit di controllo se il polinomio è divisibile per il g(x) [Standard] allora non ci sono errori. Determino il bit di controllo affinché sia divisibile. Aggiungo al polinomio ricevente degli zeri a destra. Voglio che la quantità sia pari a 0. Prendo px e lo shifto di radio dello generatrice e in quei bit metto il resto della divisione tra la portante e la generatrice.

Controllo di flusso: Se io ho un buffer in cui vado a mettere le informazioni se mando troppo è inutile continuare a trasmettere perché quelle informazione poi andranno perse.Buffer non solo risorsa ma anche tempo di svuotamento. Quindi devo fare delle tecniche di rallentamento. Ma posso anche dirgli di aumentare il flusso.

Problema di flusso: Il data link offre servizi al livello superiore ed ha ha un interfaccia. Interfaccia che ha

due funzioni. Quando il livello due ha dei dati il livello 3 non lo sa, quindi abbiamo un meccanismo che il livello due e 3 attendono che qualcosa succeda sotto (wait-for-event). Il livello fisico avverte il livello data-link e cosi via. Quando il livello data link ha detto al livello 3 che ci sono delle informazioni ha già fatto prima delle operazioni. Quando i livelli comunicano tra loro non sono sincroni. Ci sono dei momenti di attesa e lo "passo" solo quando è pronto e spesso ci sono delle bufferizzazioni. Risalita non immediata. ESEMPIO trama 123 avvisa il data link e avvisa il livello 2 e gli passa la trama 1 il livello 2 fa operazioni sulla 1 e quando poi il livello fisico gli dice che è arrivata anche al 2 il data link la lascia nel livello fisico. Quando comincio devo sapere più o meno i tempi di risposta.

Struttura trama: Pacchetto vero e proprio che sono i bit mi arrivano dal livello superiore header parte di prima e trailer parte finale e agli estremi ci sono le start e end flag. Poi devo capire anche che tipo di messaggio è e la sequenza perché la rete spesso mixa. Ack informazioni per cui dico che ho ricevuto la trama con quel numero infine ho la che sum.

Trasferimento affidabile su un canale che non è affidabile: Il trasferimento affidabile si mette nel livello datalink e trasporto. In qualsiasi caso devo dare delle direttive in modo che sembri che ho un canale affidabile. Quando devo realizzare questo servizio devo implementare della logica aggiuntiva per farlo sembrare affidabile. Prima interveniamo meglio è, overhead aggiuntivo. Nel livello trasporto non posso scegliere.

Se il checksum mi dice che il dato è corretto lo butto. E lo devo comunicare e devo fare una NAK un negative ack, che va partire la trasmissione. L'ack ovvero il messaggio positivo per liberare spazio.

Protocollo stop-wait: Arriva un messaggio attendo il positive ack, ogni volta che arriva una trama deve mandare un messaggio di controllo. ACK ACKnowledge, RR per dire sono pronto. Il canale fisico è Half-duplex. Problema delle ritrasmissione è la duplicazione dei pacchetti.

Finestra scorrevole: Dire che ho n bit per la sequenza, con una finestra vedo un numeri di informazioni pari alla dimensione della finestra. In trasmissione devo capire quali sono i frame inviati e non riscontrati. Nella sequenza la finestra mi dice quali son numeri disponibili a cui posso assegnare il dato che mi arriva. Finestra anche in ricezione.

Go-Back-N (GBN):
Il protocollo Go-Back-N funziona in questo modo:

1) Trasmissione dei pacchetti: Il mittente invia una serie di pacchetti numerati al destinatario.
2) Finestra di trasmissione: Il mittente tiene traccia dei pacchetti che ha inviato utilizzando una finestra di trasmissione. La finestra di trasmissione è un insieme di pacchetti che il mittente può inviare senza attendere un riscontro dal destinatario.
3) Acknowledgement (ACK): Il destinatario invia un ACK per confermare i pacchetti ricevuti correttamente. Se il destinatario riceve un pacchetto fuori sequenza o danneggiato, scarta il pacchetto e ignora i pacchetti successivi fino al pacchetto mancante.
4) Go-Back (ritorno indietro): Se il mittente non riceve l'ACK entro un certo timeout o se riceve un ACK negativo, ritrasmette tutti i pacchetti nella finestra di trasmissione, a partire dal pacchetto non confermato.

Piggybacking è un termine utilizzato nelle reti di computer e nelle telecomunicazioni per descrivere una tecnica in cui un pacchetto di dati sfrutta un altro pacchetto già in transito per la stessa destinazione. Questo approccio consente di ottimizzare l'utilizzo della rete riducendo il numero di pacchetti trasmessi e migliorando l'efficienza complessiva della comunicazione.

MAC: per comunicare con il livello inferiore.

Lezione 6 (Data Link) COMPLETA

Quando ricevono una trama ognuno vede se è indirizzato a lui , confrontando il suo MAC Address con quello di destinazione sulla trama. Modalità promiscua ovvero si fanno passare tutte le comunicazioni.

Un collisione avviene quando i nodi ricevono due o più trame contemporaneamente.

Protocolli per evitare le collisioni sono decentralizzati , ognuno deve decidere cosa fare, questi fissano le modalità con cui i nodi regolano le loro trasmissioni sul canale condiviso, le comunicazioni per la coordinazione avvengono nello stesso canale usato per i dati.

I protocolli di accesso multiplo sono:

- Protocolli a suddivisone del canale: Divido il canale in intervalli chiamati slot che possono essere di tempo o frequenza.Se la trama è più grande dello slot devo dividere le informazioni. TDMA divide il canale in intervalli di tempo, quindi ogni dispositivo ha un intervallo di tempo specifico in cui può trasmettere e gli slot non usati rimangono inattivi. FDMA suddivide il canale in bande di frequenza a ciascuna è assegnata una banda di frequenza prefissata e trasmette solo su quella frequenza.

- Protocolli ad accesso casuale: Quando un nodo deve inviare un pacchetto utilizza il canale al massimo. Possono esserci collisioni e se succedono devo capire come rilevare la collisone e capire come ritrasmettere.

In Aloha i pacchetti hanno la stessa dimensione, suddivido il canale in slot simile a TDMA ma a sua differenza non c'è una assegnazione predeterminata degli slot ai dispositivi. La collisione deve essere rilevata prima che lo slot termini e l'unica cosa da fare è trasmetterlo durante gli slot successivi. In Aloha puro i dispositivi possono trasmettere in qualsiasi momento , mentre nella slottata solo all'inizio dello slot. I vantaggi sono la semplicità e la decentralizzazione , di contro ci sono molti slot vuoti e collisioni specialmente nella pura (nella slottata meno collisioni si trasmette solo ad inizio slot)

In CSMA appena ho qualcosa, trasmetto se il canale è libero altrimenti un intervallo di tempo. Per capire se qualcuno sta trasmettendo utilizzo la codifica Manchester. Posso avere comunque collisioni perché se la stazione è lontana potrei non rilevarla. Ascolta il canale e vede se il canale è libero e vede se quello che sente equivale a quello che sta tramettendo, se c'è una collisione cessa subito la trasmissione.

CSMA 1-Persistente, quando un calcolatore ha dati da trasmettere ascolta continuamente il segnale presente sul mezzo trasmissivo, se è libero trasmette altrimenti ascolta fino a quando non è libero. In caso di collisione aspetta un tempo casuale, si chiama 1-persistente perché quando trova il canale occupato resta in ascolto continuamente ed appena si libera trasmette. Importante il ritardo di propagazione, più grade è il ritardo di propagazioni più collisioni avremo. Differentemente da slottata aloha non attende la time slot successiva, questo evita di lasciare inutilizzata la slot temporale.

CSMA non persistente: Nel non persistente no consumo di energia ma soluzione più conservativa, infatti non resta ad ascoltare ma aspetta un tempo casuale e riprova. Nella non persistente visto che il tempo è casuale è molto difficile che trasmettano contemporaneamente.

CSAMA p-persistente: C'è anche una via intermedia tra persistente e una non persistente, qui trasmetto o attendo in base ad una probabilità in caso di collisione attende un periodo casuale. Via di mezzo perché il persistente va bene per carichi non elevati e l'altro per carichi elevati , tardano la probabilità posso decidere su chi "puntare".

CSMA/CD: Ascoltando il canale mi accorgo che c'è stato un problema, in questo le stazioni non vanno avanti nelle trasmissioni, qui appena mi accorgo di una collisone mi fermo per un periodo casuale e avviso gli altri che c'è stata una collisione (Jamming, interferenza trasmissiva). Le stazioni riconoscendo il frammento scartano i bit ricevuti. L'efficienza dipende da N ovvero i frame da trasmettere.

- Protocolli a rotazione: Ogni nodo ha il suo turno di trasmissione.

Protocolli Collision-free: Token-ring non utilizza un mezzo broadcast ma un insieme di collegamenti punto-punto. Prevede l'utilizzo di una topologia ad anello, sull'anello circola un frame detto token che le stazioni ricevono da una parte e trasmettono dall'altra in continuazione. Una stazione è autorizzata a trasmettere dati solo quando è in possesso del token. Il token è una sequenza particolare di bit. Per capire se il
pacchetto è il token o meno si usa un bit. Protocollo poco efficiente.

Rete Ethernet: Standard per le comunicazioni in rete cablate. Lo standard IEEE 802.1 ci dà l'architettura di riferimenti. Questo standard divide il livello Data Link in LLC (Logica Link Control) e MAC (Media Access Control)

LLC: Interfaccia unificata verso il livello di rete comune a tutte le LAN. Riceve dati dallo strato di rete a cui aggiunge un suo header con le informazioni di numerazione della trama. La sua funzione principale è mascherare lo strato di rete le specifiche dei protocolli. È importante perché semplifica l'interazione con il livello di rete rendendo più facile il supporto a diversi protocolli.

MAC: Gestisce l'accesso al mezzo trasmissivo, la struttura dati e come viene trasmessa (PDU) e impatta sulle collisioni. Riceve dati da LLC e aggiunge il proprio header includendo indirizzi MAC e informazioni di controllo. Gestisce inoltre le collisioni e l'organizzazione dei dati sulla rete. MAC è essenziale per organizzare e gestire efficacemente la comunicazione in una LAN broadcast dove tutti i dispositivi ricevono tutte le trasmissioni e devono distinguere quali trame sono per loro.

L'indirizzamento è fondamentale. Gli indirizzi MAC sono composti da 48 bit e vengono rappresentati in esadecimale, suddivisi in parti separate da due punti (:). In un indirizzo MAC, la prima parte identifica il costruttore mentre la seconda parte specifica la scheda di rete. Gli indirizzi IP, invece, sono indirizzi logici rappresentati in formato decimale, con quattro gruppi di cifre separati da punti (ad esempio, 192.168.1.1). È possibile risalire da un indirizzo IP a un indirizzo MAC utilizzando la tabella ARP (Address Resolution Protocol).

Protocollo ARP: Il dispositivi mittente trasmette una richiesta (ARP Request) in broadcast contenente l'indirizzo IP del destinatario di cui cerca il MAC. Il dispositivo destinatario riconoscendo il proprio IP risponde (ARP Reply) con il MAC. Si memorizza nella cache questa associazione.

Pacchetto Ethernet:

- 6 byte per indirizzo di destinazione
- Campo tipo che permette a Ethernet di supportare vari controlli di rete
- CRC rilevare presenza di errori.

Il frame 802.3 è il formato standard utilizzato nelle reti Ethernet per la trasmissione dei dati all'interno delle LAN (Local Area Network). Lo standard IEEE 802.3 definisce le specifiche fisiche e di accesso al mezzo per le reti Ethernet cablate. Ogni frame 802.3 inizia con un preambolo di 7 byte, utilizzato per la sincronizzazione del clock tra il mittente e il ricevente. Segue il campo Start of Frame (SFD), che segnala l'inizio effettivo del pacchetto dati. All'interno del frame sono presenti due campi di indirizzo: uno per l'indirizzo di destinazione e uno per l'indirizzo di origine delle trame.

Presente un campo di 2 byte per indicare cosa si deve fare di quel frame. (?)

Exponential Backoff, algoritmo usato dal CSMA/CD Ethernet per calcolare il tempo di attesa dopo una collisione.

Funzionamento Exponential Backoff: Quando si rileva una collisione si interrompe la trasmissione. Dopo una collisione si aspetta un periodo casuale calcolato con questo algoritmo. Il periodo di attesa viene incrementato esponenzialmente dopo ogni collisione. Esiste comunque un limite di attesa se il calcolo

prodotto lo supera verra atteso il tempo massimo. Viene eseguito se si trova il mezzo occupato , dopo ogni ritrasmissione e dopo una trasmissione andata a buon fine. Non viene eseguito invece se il mezzo è libero.

Ethernet con CSMA/CD presenta le seguenti caratteristiche:

Basso carico: Tempi di ritardo ridotti e alta efficienza, simile al CSMA 1-persistente con rilevazione delle collisioni.

Alto carico: Aumento delle collisioni, ma l'algoritmo di Backoff esponenziale rende il protocollo simile a un CSMA p-persistente, migliorando la gestione del carico.

Efficienza stabile: L'efficienza tende a stabilizzarsi su un valore non nullo man mano che il carico aumenta.

Influenza della dimensione dei frame: Frame più piccoli aumentano l'overhead del periodo di contesa, riducendo l'efficienza complessiva.

Non fare da 90 fine (escluso controllo di flusso)

Controllo di Flusso: Per gestire la disparità che si crea tra reti di diversa velocità è stato aggiunto un controllo di flusso. Questo meccanismo consente allo switch di comunicare con l'interfaccia della stazione GE dicendogli di sospendere le trasmissioni di frame Ethernet e anche per quanto tempo , questo si fa inviando un frame Ethernet normale con un tipo specifico.

Lezione 7 Data Link San Switching Completa

Al fine di costruire delle reti più ampie diversi cavi possono essere connessi con ripetitori il quale lavora a livello fisico ritrasmettendo un segnale.

I bridge e gli switch consentono di interconnettere più LAN mantenendo la suddivisione a livello data link. Un bridge collega due segmenti di rete e facilita la creazione di una LAN estesa tramite il processo noto come bridging, che include anche la rigenerazione del segnale. Durante questo processo, il bridge crea una tabella hash chiamata MAC address table che associa ciascun indirizzo MAC alla porta del bridge corrispondente. Utilizzando questa tabella, il bridge decide se inoltrare o scartare il frame, determinando la destinazione corretta o la necessità di ritrasmettere il frame su un'altra linea.

Switch ha la stessa modalità di funzionamento del bridge ma ha più porte. Il suo funzionamento è uguale ad un bridge multiporta.

Dominio di collisione: Insieme di nodi che concorrono per accedere allo stesso mezzo trasmissivo e successivamente trasmettere.

Per sapere su quale porta debba essere trasmessa la trama lo switch deve creare e mantenere aggiornata una tabella relativa alla associazione tra indirizzo di destinazione e porta, per fare questo è stato creato un meccanismo di auto-apprendimento. All'inizio la tabella è vuota e lo switch inoltra la trama ricevuta a tutte le porte connesse. I frame contengono l'indirizzo del mittente ogni volta che un frame passa per lo switch questo "impara" che la stazione mittente è raggiungibile attraverso la porta da cui è arrivato il frame. Più tempo passa più la tabella si riempie e più lo switch diventa efficiente. I frame in broadcast e multicast vengono comunque inviati a tutte le porte allo stesso modo dei frame indirizzati ad indirizzi non presenti in tabella.

Tipi di switch:

- Cut-Through switching: Frame reindirizzato subito alla porta corretta.

- Store-and-forward: Il frame è letto completamente dallo switch e prima di inviarlo viene controllato il CRC, in caso di errore scartato.
- Port-based switching: Ad ogni porta corrisponde un solo indirizzo Ethernet.
- Segment-based switching: Ad ogni porta corrispondono più indirizzi.

NO 23-34

Un "broadcast storm" è una situazione indesiderata in una rete informatica in cui ci sono così tanti pacchetti di broadcast che il traffico diventa incontrollabile e congestiona la rete. Questo succede quando un dispositivo invia un pacchetto di broadcast che viene trasmesso a tutti i dispositivi nella rete. Se alcuni dispositivi ricevono e ritrasmettono questo pacchetto a loro volta, senza controlli adeguati, può crearsi un ciclo in cui i pacchetti continuano a circolare e aumentano esponenzialmente, consumando larghezza di banda e risorse di rete.

Topologia di ridondanza due switch in parallelo (replicazione) per evitare la perdita di informazioni.

- Replicazione broadcast mando a tutti.
- Replicazione di trama mando due volte la trama.
- Unicast pacchetto rivolto ad un solo computer.

Spanning tree: Switch o bridge comunicano tra loro creando una topologia virtuale. I passi per attuare questo algoritmo sono selezionare un root bridge (bridge con priorità più passa in caso di parità indirizzo Mac più basso), determinare il percorso meno costoso da ciascun bridge a rete a root bridge (root Port) e infine disabilitare i collegamenti inutilizzati. Tutte queste informazioni per identificare i vari ruoli ci vengono date da BPDU.

Dominio di broadcast: Insieme di computer in una rete che possono scambiare dati a livello datalink in modo broadcast.

Le VLAN (Virtual Local Area Network) sono reti locali che organizzano i dispositivi in base alla struttura aziendale anziché alla disposizione fisica, per motivi come sicurezza e gestione del carico di rete. Ogni VLAN definisce un dominio di broadcast separato, simile a come funziona un bridge fisico.

Nel contesto degli switch, ogni VLAN è come se fosse un switch virtuale, permettendo di isolare il traffico tra gruppi di dispositivi anche se collegati allo stesso switch fisico. Se dispositivi in VLAN diverse devono comunicare, è necessario utilizzare il livello 3 del modello OSI, ovvero il livello di rete, per il routing tra le VLAN.

Per identificare a quale VLAN appartiene un frame in arrivo, è possibile utilizzare diverse metodologie: può essere identificata in base alla porta fisica di ingresso dello switch o in base all'indirizzo MAC del dispositivo che ha trasmesso il frame.

Trunking: Metodo utilizzato per collegare due switch di VLAN, permettendo a una VLAN di essere condivisa tra più switch. Un trunk è un collegamento tra due switch che consente di trasportare il traffico di più VLAN attraverso di esso. Ad esempio, le porte di VLAN su uno switch A possono essere collegate alle porte di VLAN su uno switch B tramite un trunk.

Il Trunking è utile perché permette ad un singolo collegamento tra switch di supportare e trasportare più VLAN, inoltre fornisce un metodo centralizzato per gestire il traffico di VLAN attraverso la rete.

Backbone: Il backbone è la parte principale di una rete che collega vari segmenti e dispositivi.

VLAN Tag: Un'etichetta (tag) aggiunta ai frame Ethernet per identificare a quale VLAN appartengono. Ogni volta che entra in uno switch l'etichetta VLAN viene aggiunta per indicare a quale VLAN appartiene il frame.Il processo di tagging delle VLAN è trasparente per i dispositivi finali (come computer o stampanti),

che non devono fare nulla di speciale per gestire le VLAN. Il tag viene poi eliminato alla porta di destinazione finale , la trama infine viene poi inoltrato ala sua destinazione senza tag come se fosse un trama normale.

Inter-Switch Link (ISL): Una tecnologia usata per trasportare le informazioni delle VLAN tra switch

VTP: Protocollo usato per distribuire e sincronizzare le informazioni sulle VLAN tra gli switch all'interno di una rete. In pratica per evitare di dovere configurare uno ad uno i vari switch per le VLAN.

VTP Domain: Area logica che utilizza VTP per la gestione delle VLAN, tutti gli switch all'interno di un dominio VTP condividono informazioni sulle VLAN. I vari switch delle VLAN da configurare devono appartenere a questo dominio.

Ci sono 3 modalità con cui uno switch può operare con VTP

- Server Mode: Ovvero lo switch può creare, modificare e cancellare VLAN.
- Client Mode: Lo switch non può fare nulla se non ricevere e applicare l informazioni sulle VLAN dai server VTP
- Transparent Mode: inoltra le informazioni VTP ma non applica le modifiche, permettendo una gestione locale delle VLAN senza interferenze da parte del protocollo VTP.

VTP manda informazioni tramite multicast.

Configurazione statica una base alla porta che uso sono su una porta piuttosto che un altra.

Router on stick: Tecnica che permette di usare un'unica interfaccia fisica del router sviluppando interfacce logiche da usare come default Gateway per le varie VLAN da far comunicare.

L3 Switch che opera anche al livello 3 , L4 che opera al livello 4

Core Block: Non possono esserci truck quindi vengono fatti di meccanismi di instradamento che son di livello 3 e 4 (EXTRA non strettamente legato con Core Block) , questi possono aver dei fallimenti quindi li vado a replicare. Il core Block è quindi il cuore dell'infrastruttura di rete di un'azienda e funziona da centro di instradamento per tutto il traffico della rete.

Lezione 8 Quasi Completa

Ogni tipologia di rete si muove in una determinata area geografica.

WLAN (Wireless-LAN) : Rete locale i cui nodi comunicano tra loro attraverso il canale radio. Hanno però delle problematiche perché i segnali wireless non sono performanti come i cablati.

W-LAN non significa necessariamente via radio. Anche gli infrarossi sono W-LAN. In generale no cavo.

Utile per ampliare le zona di competenza, si è imposta perché nel tempo sono cambiati anche i dispositivi in uso. Inoltre è meno costosa perché non c'è bisogno del cablaggio.

Esistono bande di frequenza dedicate all'uso pubblico e si chiamano ISM, sono da 2.4 e 5 GHz.

Stazione: Dispostivi che possono trasmettere e ricevere dati utilizzando la banda di frequenza della tecnologia 802.11 (Wi-Fi). Contiene le funzionalità del protocollo 802.11 e possono essere mobili, portatili o stazionare.

BSS (Basic Service Set): La più piccola unità di una rete Wi-Fi, comprende un gruppo di dispositivi wireless (stazioni) che comunicano tra loro.

Esistono due tipi principali di BSS:

BSS indipendente (IBSS): Insieme di stazioni che si sono identificate reciprocamente e sono connesse tra loro in modalità peer-to-peer (ogni nodo ha capacità responsabilità equivalenti). Non ci sono funzioni di relay ovvero meccanismi che permettono ad un nodo di agire come intermediario per inoltrare dati tra due o più dispositivi in una rete.

BSS infrastruttura : È una BSS con un componente chiamato Access Point che da le funzioni di relay per a BSS. La sua architettura è fatta da celle fatte dalle BSS ed ogni cella è controllata dall'AP e le comunicazioni tra stazioni avvengono solo grazie a quest'ultimi.Access Point fa anche da bridge perché passa da cablata a wireless. Quando un dispositivo vuole comunicare con un altro dispositivo nella stessa rete, i dati passano attraverso il punto di accesso.

Il Distribution System è fondamentale nelle reti Wi-Fi per consentire la comunicazione tra diverse aree di copertura, migliorare la gestione del traffico dati e supportare la mobilità degli utenti. Esso integra vari BSS in una rete coesa e gestisce efficacemente l'inoltro dei pacchetti, l'associazione e il roaming dei dispositivi. Uso ad esempio se da rete A ho bisogno di stampante in rete B.

Un Extended Service Set (ESS) è una rete wireless composta da più Basic Service Sets (BSS), ognuno dei quali è gestito da un access point (AP). Questi AP sono collegati tra loro tramite il Distribution System (DS), che permette la comunicazione tra i diversi BSS. All'interno di un ESS, gli utenti possono spostarsi da una cella (copertura di un AP) all'altra senza perdere la connessione. Questo processo è noto come roaming. Durante il roaming, il dispositivo mobile passa automaticamente da un AP all'altro, mantenendo la connessione attiva e senza interruzioni percepibili. Dall'esterno i vari AP sono visti tutti come un unica rete logica.

No [20-22]

Lo spreading spectrum è una tecnica di comunicazione utilizzata per trasmettere un segnale su una banda di frequenza molto più ampia del necessario. Questa tecnica offre diversi vantaggi, tra cui una maggiore resistenza alle interferenze e una maggiore sicurezza nella trasmissione dei dati. Esistono due principali tecniche di spreading spectrum: Frequency Hopping Spread Spectrum (FHSS) e Direct Sequence Spread Spectrum (DSSS)

FHSS: Il segnale cambia rapidamente in modo casuale tra diverse frequenze, salto di frequenza controllato. Sicura e resistente alle interferenze, ma limitata in banda ed è impossibile da usare nel WI-FI ad altri bit-rate.
DSSS: Ogni bit di dati viene moltiplicato da una sequenza di bit più lunga. Codifica ridondante che la rende più immune ai rumori, si spreca più banda.

Jamming: Interferenze che possono essere intenzionali o meno.

Dynamic Rate Shifting: Meccanismo che consente di modificare automaticamente la velocità di trasmissione dei dati per compensare le variazioni del canale.

CSMA/CA: La collisone detection è complicata da fare nel wireless perché nella ricezione di errore dovrei controllare se quello che ascolto è uguale a a quello ricevo, nelle reti wireless non è possibile però che una stessa antenna riceve mandi contemporaneamente, non posso mettere due reti vicine senno c'è interferenza. Funziona in linea con i CSMA quindi aspetta che il canale sia libero e trasmette se è occupato aspetta il backoff se non riceve un ACK aumenta il backoff. Il ricevente dopo aver aspettato un tempo SIFS manda l'ACK. Tre problemi principali sono:

1) Nodo nascosto: Due dispositivi potrebbero non essere in grado di rilevare le trasmissioni l'uno dell'altro perché fuori portata. Possono però entrambe comunicare con un nodo comune .

2) Nodo esposto: Un nodo che rileva una trasmissione vicina potrebbe penare di non poter trasmettere anche se la sua connessione non causerebbe collisioni.

3) Fading: I due dispostivi sono posti in modo che la forza del loro segnale non è sufficiente per rilevare le trasmissioni , ma il loro segnale è abbastanza forte da interferire con una stazione e metà strada.

Per risolvere questi problemi vengono mandati dei segnali (RTS per dire di star inviando) (CTS per dire che di essere pronti a ricevere) per farsi cha gli altri dispositivi sappiano che c'è una trasmissione
---
Lezione 9 Completa

ADSL: Standard per fornire un'accesso digitale a banda più elevata. Tecnologia che permette di collegarsi a Internet tramite la linea telefonica tradizionale. Asimmetrica (+ download - upload). C'è un filtro (splitter) che separa le frequenza per evitate che la telefonia faccia interferenza.

DSLAM: Dispositivo a cui arrivano i nostri dati che provvede poi a instradare i dati verso internet e gli ISP.

ATM: Tecnolgia di commutazione a pacchetto utilizzata per trasmettere dati orientato alla connessione. Utilizza celle di dimensione fissa. Inoltre combina il traffico da diverse fonti in un singolo flusso di celle (multiplexing). Le celle sono inviate solo se ci sono dati da trasmettere. Supporta inoltre diverse classi di servizio per gestire in modo appropriato i vari dati. Usa inoltre dei circuiti virtuali che per instradare le celle nella rete e sono di due tipi PVC (predefiniti e permanenti) SVC (dinamici).Il modo di trasferimento dei dati è ATD (divisione asincrona del tempo) I suoi vantaggi sono l'efficienza la scalabilità e il supporto a diverse classi (QoS), d'altro canto è costosa e complesse.

Celle ATM: 5byte di intestazione con gli identificatori utilizzati per instradare la cella attraverso la rete, le informazioni nel payload la priorità della cella in caso di connessione e l' HEC ovvero mi campo di controllo degli errori per l'intestazione.

Lezione 10 Completa

Al livello trasporto la comunicazione deve apparire come una comunicazione punto-punto, lo strato di rete deve quindi fornire allo stato trasporto un servizio per la consegna di dati in modo da mascherare la sottorete.

Nomenclatura:
- Host (End-node): Stazione su cui opera lo strato di trasporto che deve trasmettere o ricevere i dati. Due host sono solitamente separati da un certo numero di nodi e sono connessi da svariate linee. Spesso è possibile che siano disponibili più percorsi tra due nodi.
- Pacchetto: Insieme di dati header, trailer che lo strato di rete costruisce e deve trasmettere a destinazione.
- Router: Stazione che lavora al livello 3 che riceve pacchetti e li inoltra attraverso la sottorete.

Il livello 3 deve quindi determinare il tragitto ,tra quelli disponibili, che i dati dovranno seguire, deve anche reagire a modifiche di topologia ed evitare il sovraccarico delle linee e infine deve risolvere i problemi di transito su reti differenti. Servizio connection-less, ovvero inviare dati senza una connessione dedicata. Questo è utile per la flessibilità e l'efficienza nella consegna dei pacchetti in reti inaffidabili , l'integrità invece è controllata a livello più alto.

Ogni pacchetto è instradato in maniera indipendente. Un router ha una tabella che definisce su quale linea di uscita deve essere trasmesso un pacchetto in base alla destinazione finale. Quello che fa il router infatti è:

1) Ricevere il pacchetto

2) Memorizzarlo per analizzarlo
3) Trasmetterlo in base alla tabella

Questi passi precludono che ogni pacchetto sappia l'indirizzo di destinazione e visto che le tabelle variano nel tempo non è detto che tutti i pacchetti seguano la stessa strada.

Nel connection-oriented si associa ad una connessione in circuito virtuale e si definisce a priori la sequenza di router che i pacchetti dovranno attraversare (tutti i pacchetti seguono la stessa strada).

Le operazioni principali svolte al livello 3 dai router sono quindi:

- Inoltro, dove in base all'indirizzo di destinazione o al circuito virtuale si sceglie la linea di uscita, in base alle informazioni preesistenti.
- Instradamento, ovvero il processo di creazione e di aggiornamento della tabella che associa una linea di uscita modificando periodicamente la tabella, se ci sono state delle modifiche o problemi (malfunzionamenti fisici).

Protocollo livello 3 IP prende pacchetti e deve farli arrivare a destinazione, fa del suo meglio per evitare errori se ci riesce bene. Se è possibile il datagramma viaggia intero altrimenti viene spezzettato. Se le due stazioni non sono molto vicine IP manda il pacchetto nodo a nodo fin quando non arriva a destinazione. Indirizzamento a 32 bit.

La necessità del livello 3 è supportare le tabelle di routing, si hanno meno bit rispetto al livello 2 perché si manda alla rete e non al nodo come al livello 2.

Pacchetto IP diviso in parole può essere frammentato perché passa su rete diverse ed è il router a fare la frammentazione, è costituito da un header di lunghezza fissa di 20 byte più una parte opzionale, è presente anche una campo per versione (Ipv4 o Ipv6).

Per la frammentazione ci sono dei campi dedicati:

- Indetification: Serve a capire a quale datagramma originale appartengono i frammenti.
- Fragment-offset: Indica la posizione del primo byte rispetto al datagramma originale.
- MF (More-Fragment): Bit che se è 0 indica che è l'ultimo frammento o che non c'è stata la frammentazione, se invece e 1 significa che ci sono altri frammenti dopo di lui.
- DF: Vale 1 se il datagramma non deve essere frammentato con 0 permette invece la frammentazione.

Altri campi sono:

- Time-to-live: Contatore che viene decremento via via che il pacchetto viaggia in rete, quando arriva a 0 il pacchetto viene buttato.
- Protocol: Indica il protocollo di livello superiore a cui sono destinati i dati del pacchetto
- Cheksum: Contenente un codice CRC relativo solo all'header.

Per poter identificare il destinatario ogni host e router devono avere un indirizzo ip univoco che distingue la rete di appartenenza e l'host.

L'indirizzamento IP è gerarchico a due livelli:

- Indirizzo di rete
- Indirizzo di host

Ogni interfaccia di rete deve avere un indirizzo IP. Tutti i nodi IP hanno un ulteriore indirizzo IP detto loopback che rappresenta un indirizzo fittizio indicante se stesso.

L'indirizzo IP è costituito da 32 bit rappresentati in numeri decimali, questo indirizzo contiene una parte che specifica la rete ed una parte che specifica l'host. Il prefisso indica la rete mentre il suffisso identifica un host.

Gli indirizzi IP sono classificati in diverse categorie dette classi

Classe A: tutti quelli tra 0 e 127, questi hanno il primo byte dedicato alla rete e il resto all'host.
Classe B: da 128 a 191 , questi hanno i primi due byte all'indirizzo di rete e il resto all'host.
Classe C: da 192 a 223, 3byte per la rete e resto all host.
Classe D: da 224 a 239 dedicati per l'indirizzato multicast.
Classe E: da 240 a 255 utilizzati per usi sperimentali e non devono mai esser utilizzati come indirizzi.

L'indirizzo contenente tutti 0 nel campo host viene utilizzato per indicare la rete. Mentre l'indirizzo IP con tutti 0 nella parte di rete ha il significato di questa rete. L'indirizzo 255.255.255.255 in pratica con tutti 1 rappresenta l'indirizzo broadcast della rete locale direttamente connessa, ed è l'indirizzo utilizzato per inviare un pacchetto IP broadcast sulla propria rete. L'indirizzo con tutti 1 nel campo host rappresenta l'indirizzo broadcast della rete specificate nel campo di rete

Per risolvere il problema della mancanza di indirizzi sono state applicate due soluzioni:

1) CIDR: In questo caso la parte di un indirizzo IP relative alla rete può avere lunghezza a piacere invece di essere costretta ad numero finito di bit. CIDR utilizza un formato che include un prefisso di rete dopo uno "/". Il numero dopo lo slash indica quanti bit sono riservati per la parte di rete dell'indirizzo.

2) Subnetting: Un organizzazione può usare i bit rimasti per indirizzare gli host per creare altre reti interne alla rete principale. Per fare questo c'è bisogno di identificare quali bit definiscono la rete e quali bit l'host e per fare questo si utilizza una maschera fatta da 32 bit. Di questi 32 bit se un bit vale 1 allora il corrispondete bit fa pare della rete altrimenti fa parte dell'indirizzo di host.

Il subnetting può essere a:

Lunghezza fissa: Costringe a creare sotto reti di dimensioni uguali anche se non corrispondono a quello di cui abbiamo bisogno.

Lunghezza variabile: Permette di creare sottorete di dimensioni diverse a seconda delle necessità.

Ipv6 evoluzione di Ipv4 perché sia stanno esaurendo gli spazi, Ipv6 ha infatti come obiettivo un indirizzamento illimitato (molto grande) inoltre cerca di migliorare il protocollo, migliorando

- Latenza (Ipv4 fa troppe cose)
- Sicurezza (Sopratutto lato wireless che ha problemi di sicurezza al livello 4) al livello 3 c'è un livello di sicurezza ma non è ottimale e non copre tutte le reali necessità di sicurezza quindi si è deciso di metterò al livello 2 e al 4. Con ipv6 però si pensa che ci debba essere una sicurezza anche al livello 3.
- Affidabilità, Ip poi è pensato per pacchetti piccoli e questo è da migliorare.
- Prevedere evoluzioni future.

Ip è scritto in hardware e quindi devo gestire l'evoluzione del protocollo; Ipv6 è più software. Inoltre deve supportare i protocolli di livello superiore. Gli indirizzi IPV6 sono 128 (vs 32) ci da la possibilità di venire incontro alle esigenze attuali. La rappresentazione è in cifre esadecimali diversamente da ipv4 che sono decimale inoltre non si usa il punto ma due punti. Per scriverlo in maniera più comodo si mettono i due punti se ci sono solo 0.

Le informazioni di rete e host si distinguono con lo / inoltre non vi sono più le classi. Nel pacchetto l'header cresce però si snellisce perché si perde la parte opzionale, il meccanismo di estensione del protocollo lo si realizza con gli header innestati (nel body metto un header con un puntatore all'header).

Cambiamenti header IPv6:

- Versione: La versione del protocollo IPv6 rimane costante e ha il valore 6.
- Traffic Class: Questo campo identifica i pacchetti che richiedono specifiche classi di servizio per un instradamento particolare.
- Flow Label: Introdotta per identificare i pacchetti appartenenti allo stesso flusso di trasmissione, è cruciale per applicazioni come la trasmissione di voce e video che richiedono una connessione definita.
- Payload Length: Indica la lunghezza del pacchetto in byte.
- Next Header: Specifica il protocollo del livello di trasporto a cui sono destinati i dati e indica il tipo di intestazione estesa successiva utilizzata.
- Hop Limit: Simile al Time-to-Live (TTL), ma con l'unico scopo di contare il numero di hop che un pacchetto può attraversare prima di essere scartato.

L'intestazione dei datagrammi in IPv6 è semplificata e non include il campo per la frammentazione, poiché quest'ultima poteva causare ritardi nella trasmissione. Invece di permettere la frammentazione, IPv6 prevede che le stazioni si accordino su dimensioni di pacchetto compatibili. Questo approccio è più efficiente, permettendo alle stazioni di imparare le dimensioni accettabili dei pacchetti per quella rete specifica senza necessità di ridurre le prestazioni per gestire la frammentazione. Inoltre, IPv6 ha eliminato il checksum a livello di rete (header checksum), poiché i controlli di errore sono già gestiti a livello 2 (datalink) e livello 4 (transport). Questa ottimizzazione contribuisce a migliorare l'efficienza complessiva della rete, anche se riconoscere eventuali errori avviene principalmente a destinazione e i casi in cui ciò è necessario sono rari.
Ecco una versione migliorata del paragrafo:

Gli extension header (intestazioni aggiuntive) in IPv6 sono utilizzati per estendere le funzionalità di base dell'intestazione. Ogni extension header inizia con un campo nextHeader che indica il tipo di header successivo, che può appartenere sia al livello 3 che al livello 4 del modello OSI. Ogni header di estensione inizia con due byte, seguiti da un campo lunghezza che varia perché non sono a dimensione fissa. Le informazioni contenute negli extension header possono variare notevolmente a seconda del tipo di estensione utilizzata.

Tipi di estensione: hop-by-hop tutti i router devono esaminare , destinazione , routing per introdurre col concetto di source routing è la sorgente che decide il percorso , frammentazione quando è la sorgente che frammenta non dal router , autenticazione e crittazione.

Quando abbiamo inventato un nuovo protocollo per cambiare ip bisogna cambiare tutta la tecnologia, man man si aggiornano gli apparati. Frammentazione di rete che parlano o uno o altro con pezzi che fanno da ponte.

Indirizzi compatibili modo per prendere un ipv4 e metterlo in ipv6 , si mettono :: e la rappresentazione ipv4 in esadecimale.

Opzione permette a ipv6 di capire e a ipv4 che sa dove prendere l'indirizzo. Il problema della compatibilità non è solo per indirizzi ma anche come datagramma perché vedo un ipv6 come un ipv4, un nodo che parla ipv4 e riceve ipv6 non capisce.

Prima soluzione ponte dual Stack, i nodi IPv6 dispongono di una implementazione IPv4. Questi hanno entrambi gli indirizzi e devono essere in grado di determinare se il nodo con cui devono parlare è un nodo IPv6 compatibile o solo IPv4.

Tunneling: consente di trasportare pacchetti IPv6 attraverso una rete IPv4 incapsulando un datagramma IPv6 completo come payload di un datagramma IPv4. L'header IPv4 contiene l'indirizzo IPv4 del punto finale del tunnel (di solito un router compatibile con IPv6). Il router di origine incapsula il pacchetto IPv6 all'interno del pacchetto IPv4, permettendo al pacchetto IPv6 di viaggiare attraverso la rete IPv4. I router

intermedi trattano il pacchetto come un normale pacchetto IPv4. Quando il pacchetto arriva al router di destinazione del tunnel, questo router riconosce che il payload è un pacchetto IPv6, rimuove l'header IPv4 e continua a instradare il pacchetto IPv6 verso la destinazione finale.

DNS (Domain Name System) può creare un mapping tra IPv6 e IPv4, ma in generale è un sistema che traduce i nomi di dominio in indirizzi IP.

Protocollo di livello ICMP se succedeva qualcosa di livello 3 anomalo serviva a mandare messaggi meccanismo di controllo come il ping e utilizza ip come meccanismo di comunicazione protocollo di livello 3 sotto un protocollo di livello 3. In pratica la sua funzione è monitorare il funzionamento del livello della rete. Principali messaggi ICMP sono ,irraggiungibile , time exceed (scaduto time-to-live), parametri inconsistenti nei datagrammi oppure la sorgente sta pubblicando troppo e quindi il router gli dice di andare più piano, ma ha problema di sicurezza perché si poteva intasare , quindi è stato spostato al livello 4, infine redirect (Instradamento errato).

NAT: Tecnica utilizzata nelle reti per modificare gli indirizzi IP nei pacchetti di dati mentre transitano attraverso un dispositivo. Il suo utilizzo maggiore è quello di permettere a più dispositivi di una LAN di condividere un singolo indirizzo IP pubblico per accedere a Internet. Il NAT divide gli indirizzi in privati e pubblici , quelli privati sono usati in una rete locale e non possono essere instradati su internet , poi abbiamo un unico indirizzo pubblico che è quello che effettivamente si interfaccia con la rete esterna ed è assegnato dal ISP. Il NAT si occupa quindi della traduzione degli indirizzi per la comunicazione e per passare da quello pubblico a quelli privati. Quindi quando un dispositivo nella rete locale vuole comunicare con Internet invia il pacchetto al router che provvede a sostituire l'indirizzo IP privato con il proprio indirizzo pubblico. In fase di ricezione invece il router fa l'operazione inversa.

ARP: Protocollo utilizzato per mappare un indirizzo IP a un indirizzo MAC e opera al livello 2 e 3. Quando un dispositivo in una rete locale vuole comunicare con un altro dispositivo conosce il suo indirizzo IP e non il suo MAC, per ottenerlo tramite l'indirizzo IP usa l'ARP request. L'ARP request viene mandata come un messaggio di broadcast a tutta la rete, in questa request è presente l'indirizzo IP del quale si sta cercando il MAC. Il dispositivo che corrisponde risponde con un ARP reply che contiene l'indirizzo MAC. Una volta ottenuto si memorizza nella tabella ARP in modo da evita ulteriori richieste future.

ReversARP: Conoscere il proprio indirizzo IP grazie al MAC.

DHCP (Dynamic Host Configuration Protocol) è responsabile dell'assegnazione dinamica degli indirizzi IP agli host sulla rete. Gli indirizzi IP assegnati tramite DHCP non sono fissi e hanno un "time to live" (TTL) dopo il quale devono essere rinnovati. I messaggi DHCP sono inviati tramite broadcast per trovare un server DHCP disponibile. Il server DHCP risponde con un indirizzo IP per l'host richiedente, insieme al suo indirizzo MAC. DHCP è un'applicazione client-server; sulla rete c'è sempre un nodo che funge da server DHCP. Nella configurazione di rete, l'indirizzo del server DHCP viene specificato in modo che gli host possano inviare un broadcast e ottenere direttamente un indirizzo IP.

Il DHCP supporta tre diversi meccanismi per l'allocazione degli indirizzi IP

Manuale: Un particolare indirizzo IP è pre-allocato ad un host ad un amministratore ed è solitamente identificato dall'indirizzo MAC
Automatica: Il DHCP assegna automaticamente un indirizzo IP permanente selezionandolo da un insieme di indirizzi IP.
Dinamica: Il DHCP assegna un indirizzo IP ad un host per un breve periodo di tempo.

Fasi del DHCP

1) DHCP Discover manda in broadcast cercando qualcuno che gli dia un IP
2) DHCP Offer gli offre un indirizzo ip
3) DHCP Request accetta l'indirizzo ip

4) DHCP ACK lo registra.

DHCP è un protocollo senza autorizzazione infatti non richiede autorizzazione per ricevere un lease (periodo di tempo in cui un indirizzo è associato ad un client) questo potrebbe portare a DOS perché di richiedono indirizzi IP per indirizzi MAC falsi. Protocollo soft state perché se non viene rinfrescato si cancella lo stato.

Lezione 11 Quasi Completa

Router: Architettura special purpose cioè sa fare una sola cosa, va configurato ed ha un suo sistema operativo per la memoria e per gestione delle risorse.
I router sotto un unico dominio amministrativo sono Autonomus System (AS).

Un Autonomous System è un insieme di reti IP sotto il controllo di un'unica entità amministrativa che segue una politica di routing comune e gestisce le sue tabelle di routing interne in modo autonomo rispetto agli altri AS. La loro principale funzione è quella di consentire il routing delle informazioni tra diverse reti all'interno di Internet, facilitando la comunicazione tra reti geograficamente distribuite e gestite da diverse organizzazioni

I router vengono classificati come ruolo in:

- I router che instradano messaggi all'interno dello stesso AS e non hanno diretta connessione con altre reti sono chiamati Interior Router e scambiano informazioni di instradamento con un IGP (mappa interna che aiuta i router a trovare la strada migliore per comunicare all'interno della stessa grande rete).

- I router che invece instradano i messaggi tra AS diversi sono detti Exterior Router e scambiano informazioni con l'EGP (mappa che aiuta i router a trovare il percorso migliore per comunicare con altre reti).

- I router che fanno da ponte di collegamento tra AS diversi e vengono detti Border Router.

Quando arriva un pacchetto si deve capire dove deve andare e la prima informazione è la destinazione e deve estrarre l'indirizzo ip. Per fare questo ho bisogno di conoscere i router adiacenti. Se la destinazione è all'interno della rete rimango al livello 2. Devo capire quali sono i percorsi e devo scegliere il migliore. Tutte queste cose vengono fatte grazie alla tabella di routing che raccoglie le informazioni e capisce quale è il percosso migliore.

Le informazioni che raccoglie sono:

- Destinazione: Rappresenta il campo più importante nella tabella di routing , infatti quando un router riceve un pacchetto controlla nella propria tabella se esiste una entry per quella destinazione e in caso affermativo inoltra il flusso in quella direzione.

- Metrica algoritmo di instradamento

- Indirizzo router next hop: Indirizzo router successivo per raggiungere la rete di destinazione.

- Interfaccia: Interfaccia attraverso cui deve essere instradato il pacchetto verso il next hop.

- Timer: Scandisce ogni quanto inviare aggiornamenti ai router vicini.

Ogni router ha la sua tabella di routing , non abbiamo l'indirizzo ip della destinazione ma della rete di destinazione, quindi l'algoritmo è per la rete e non per la specifica destinazione.

Router di default se non ho informazioni di routing (switch manda a tutti ma non ha senso qui perché inondo la rete) la soluzione è mettere un router di default che sa cosa fare , se non conosce la rete mandala di li ed è in genere l'ultima riga, è rappresentato da tutti 0.

Quando arriva un indirizzo di destinazione, analizzo la classe di appartenenza e l'indirizzo di rete per capire a cosa corrispondono. Tuttavia, nel caso in cui non ci siano classi predefinite, potrebbe accadere che ci siano più voci (entry) che corrispondono all'indirizzo. In questa situazione, scelgo l'entry con il maggior numero di bit corrispondenti.

Per estrarre l'indirizzo destinazione devo confrontarlo con il mio indirizzo ip e devo capire se siamo sulla stessa rete, se arrivato il messaggio devo decrementare il time-to-live (numeri di passi che deve fare il messaggio) , cerco di capire quali sono le corrispondenze e se siamo sulla stesse rete cerco di capire l'indirizzo, se non siamo sulla stessa rete mi faccio aiutare dalla tabelle di routing costruendo il data gramma per farlo arrivare a destinazione.

Abbiamo due tipi di routing:

- Routing statico: Prevede il calcolo dei percorsi offline quando la rete non è ancora attiva e prevede la configurazione manuale. Nel router statico ho A e B e gestisco io il traffico. Nelle configurazioni statiche vado a mettere anche il default routing. Usati quando si ha un'unica connessione oppure se per tutte le connessioni c'è una destinazione ben precisa.

- Routing dinamico: I percorsi cambiano dinamicamente in base al traffico o congestione vede quindi quello che succede nella rete. Nel router dinamico ho un protocollo che mi mantiene aggiornate le tabelle di routing. Per costruire ogni tabella devo comunicare con i vari router per capire le informazioni che hanno. Non c'è un unico elemento di struttura che guarda la rete perché ognuno ha una conoscenza locale e quindi le scelte sono locali. Usa delle metriche per decretare l'ottimalità, parametri del tipo (percorso più breve meno congestionato , più lungo , il meno costoso) metriche dinamiche (probabilità di guasto o traffico puntale sulla linea). Rip(hop) , IGRP e EIGRP (banda affidabilità e carico ottimale per una ma non per altre).

Le informazioni di instradamento arrivano da una sorgente e poi propagate , più è distante la sorgente meno ci si "fida", il valore dato è detto distanza amministrativa.

Gli algoritmi di routing si dividono in:

- Non adattivi: Usano criteri fissi di instradamento e sono statici. Fixed Directory Routing (Ogni nodo ha una tabella con nodo->linea, messe dal gestore e quindi statiche, è lui che deve operare in caso di guasto), Flooding like (Broadcast su tutti tranne il mittente)

- Adattivi: Qui risolvono problema di ottimizzazione si ha un elemento che conosce la topologia e il costo e risolve la tabella di routing. Routing centralizzato (si basa sulle piccole reti, perchè deve conoscere tutta la topologia), Routing isolato (il router vede il "suo mondo" ed ognuno risolve il problema con le proprie informazioni), Routing distribuito (unione precedenti perché ogni nodo riceve le informazioni e prende la decisione e le propaga alle altre).

La rappresentazione della rete è un grafo della rete con nodi (router) e i collegamenti che rappresentano i collegamenti del router e può essere bidirezionale. Ogni arco ha un peso quindi il peso del percorso non è solo il numero di archi. Il percorso più breve di determina in base alla metrica considerata e solo quelle che metto negli archi. La distanza di un percorso è la distanza delle etichette.

Distance Vector: Il router deve conoscere i router adiacenti ed il costo delle linee che li connettono direttamente. Per fare questo scambia con i vicini dei pacchetto per essere aggiornato sulla loro presenza. Quando viene ricevuta la tabella di routing dai vicini si valuta la distanza e si sceglie quella inferiore. Ogni router mantiene oltre alla tabella una struttura detta Distance Vector.

Split Horizon: Non si inviano le informazioni di costo verso la destinazione X sul link al quale vengono inviati i pacchetti per la destinazione X. In pratica, il router non annuncia a un'altra router una rotta che ha imparato da quel router.

Poison Reverse: Questa tecnica è una variante del Split Horizon. Invece di non annunciare la rotta indietro, il router la annuncia con una metrica (di solito infinita o molto alta) per indicare che la rotta non è più disponibile o è stata rimossa. Questo aiuta a informare rapidamente gli altri router della rete della perdita di una rotta.

Gli aggiornamenti partono se ci sono cambiamenti topologici , ovvero quando ci sono delle modifiche oppure se c'è della cogestione perché vanno a cambiare i pesi.

In link state le informazioni di aggiornamento sono mandate con il flooding (sorta di broadcast), è un componente cruciale dei protocolli link-state, assicurando che tutti i router abbiano informazioni aggiornate e complete sulla topologia della rete.Situazione a regime tutti conoscono tutti.

Algoritmo flooding: Ogni pacchetto in arrivo viene inoltrato su ogni linea in uscita eccetto quella da cui è arrivato. Intasa la linea perché manda tutti i pacchetti ovunque ma al tempo stesso visto che segue tutte le vie segue sempre anche quella più veloce, questo lo rende residente ai cambiamenti topologici.

Fluttuazioni: Quando la rete va su e giù, in questo caso uso dei timer per capire il comportamenti di queste reti.

Algoritmi routing link state: Deve costruire informazione topologica complessiva , in memoria devo avere la mappa di tutta la rete e si cerca di mantenere le informazioni topologiche il più aggiornate possibile e data la mappa costruisco la tabella mentre il distance vector avevo solo la tabella. Nel primo momento ho la scoperta dei vicini (a cui associo un numero) e scambio informazioni di adiacenza e poi costruisco la mappa topologica.
Informazioni di adiacenza qui sono i costi e quali sono i nodi adiacenti , anche in questo caso non è una struttura dati complessa perché il router deve essere semplice , ovviamente a partire da questa tabella devo fare la tabella di routing e i passi di un protocollo link state sono
1) individuare i vicini
2) capire le metriche che mi rappresentano il valore di costo
3) costruire i pacchetti che devo mandare
4) costruire i percorsi migliori.

In genere quando un nodo va in rete manda un messaggio a tutte le line e chi lo riceve deve rispondere con il proprio identificativo ed è un meccanismo per identificarsi. In generale il percorso di andata non è uguale a quello di ritorno. Il pacchetto link state inizia con l'identificativo di chi lo manda e manda sequenza di 32 bit (per identificare il pezzetto del pacchetto) e dall'età (capire la versione della tabella perché magari ho due ed una la scarto) , manda periodicamente la risposta per capire che è ancora attivo ed è anche operativo il collegamento per quel nodo.

Routing Gerarchico: Suddivide la rete in aree. Per comunicare tra due nodi appartenenti ad aree diverse e necessario conoscere l'instradamento tra il nodo mittente e la periferia dell'area in cui il nodo mittente appartiene, instradamento tra l'area mittente e l'area destinazione e l'instradamento all'interno dell'area di destinazione.

Protocollo IGP RIP: Basato su distance vector. Usa numero degli hop come metrica e tutte le linee hanno costo 1 e il costo massimo è 15. Le tabelle di routing vengono scambiate tra router adiacenti questo messaggio contiene voci per massimo 25 reti.

OSPF: Progettato per supportare diverse metriche ed è capace di reagire velocemente a modifiche di topologia. Supporta il tunnelling. Ogni router invia agli altri nell'area lo stato dei suoi collegamenti. Ogni

router ha una visione completa della rete. Attraverso Dijkstra ogni nodo calcola il percorso minimo. Le modifiche sono segnalate con flooding. Questo protocollo permette di dividere un AS in più aree. Definisce inoltre router interni, border router , backbone router e boundary router. Ogni router di ogni area conosce la topologia dell'area e può fare routing interno.

Peering: Meccanismo di collaborazione tra Autonomous Systems (AS) che permette il transito del traffico tra di essi, facilitando il raggiungimento delle destinazioni finali.

L'aggiornamento delle tabelle di instradamento può essere fatto in 3 modi:

1) Eseguire un unico algoritmo di instradamento tra organizzazioni adiacenti. Svantaggioso per il ritardo di propagazione e perché tutte le organizzazioni sono costrette ad usare uno stesso algoritmo.
2) Aggiornare le tabelle di instradamento manualmente con percorsi statici predefiniti. Vantaggioso perché nasconde la parte interna dell'AS e per ogni obiettivo esterno si identifica un router. Svantaggioso perché è difficile da manutenere e i malfunzionamenti non sono gestiti
3) Combinare un protocollo di instradamento tra vari domini.

L'Exterior Gateway Protocol (EGP) è un protocollo utilizzato dai router per scambiare informazioni di routing tra sistemi autonomi (Autonomous System - AS) diversi all'interno di un sistema di rete più grande, come Internet. Il suo scopo principale è quello di consentire a router appartenenti a sistemi autonomi differenti di comunicare tra loro e di scambiare informazioni di routing per raggiungere destinazioni al di fuori del proprio sistema autonomo. EGP consente ai router di inviarsi informazioni di routing sulle reti raggiungibili. Inoltre funge da protocollo di Gateway tra differenti AS consentendo a router diversi di cooperare per instradare pacchetti tramite Internet.

BGP: Protocollo di routing utilizzato per scambiare informazioni sulle rotte di rete tra router. Permette la comunicazione tra AS e utilizza informazioni sulle rotte per scegliere il percorso più efficiente per il traffico. I vari router BGP stabiliscono connessioni di peering (ossia creano un collegamento diretto tra due reti per scambiarsi informazioni sul routing). Ogni router annuncia le rotte che conosce e alla fine BGP sceglie il percorso migliore in base alle sue politiche. Inviano la maschera insieme all'indirizzo. Inoltre richiede che ogni AS sia numerato.
Le funzionalità BGP sono:

1) Apertura connessione tra peers
2) Annuncio informazioni sulla raggiungibilità
3) Verifica il corretto funzionamento.

BFG permette ad un AS di offrire connettività ad un altro AS ovvero gli promette il recapito ad una specifica destinazione.

I messaggi che usa sono 4 e sono

1) OPEN usati per aprire una connessione peer ed ha un campo hold che specifica il numero massimo di secondi tra due messaggi. Il destinatario di un OPEN risponde con un KEEPALIVE e OPEN.
2) UPDATE che annuncia nuove reti raggiungibili e il loro raggiungimento.
3) KEEPALIVE verifica periodicamente la connessione.
4) NOTIFICATION controllo o segnalazione errori.

Path Attributes: BGP specifica il percorso verso la destinazione tramite più salti successivi. Gli attributi possono indicare i sistemi autonomi attraverso i quali passa il percorso verso la destinazione o la provenienza delle informazioni di routing. Gli attributi sono comuni a tutte le destinazioni annunciate; destinazioni con attributi diversi devono essere annunciate mediante messaggi separati. Gli attributi possono essere utilizzati in ingresso per il filtraggio delle rotte o per la manipolazione degli attributi delle rotte al fine di influenzare la selezione dei percorsi da parte degli altri sistemi autonomi. In uscita, vengono utilizzati anche per il filtraggio delle rotte e la manipolazione per influenzare i percorsi verso l'esterno.

Limiti di BGP: BGP non è in grado di discriminare tra due percorsi in base a una metrica di costo e seleziona uno dei percorsi disponibili senza tener conto del carico di rete in modo dinamico. È necessario configurare manualmente quali reti vengono annunciate ai router esterni.

Lezione 12 Quasi Completa

Un protocollo dello stato di trasporto deve fornire una comunicazione logica fra i processi applicativi che girano su host differenti. Deve garantire un servizio di trasferimento end to end (da un punto iniziale ad uno finale). Fa tutto mascherando le operazioni intermedie.

Livello di rete: Il livello di rete si occupa di fornire comunicazione logica tra host in una rete. Questo livello gestisce l'instradamento dei pacchetti di dati da un nodo sorgente a un nodo destinazione, indipendentemente dal percorso che i pacchetti devono seguire. Esso utilizza indirizzi IP per identificare gli host e può includere funzionalità come la frammentazione dei pacchetti e il controllo del traffico.

Livello di trasporto: Il livello di trasporto fornisce comunicazione logica tra processi di applicazioni che girano su host differenti. Questo livello è responsabile del trasferimento affidabile dei dati, della gestione delle connessioni, e della multiplexing, ovvero della distinzione tra più flussi di dati utilizzando numeri di porta. I numeri di porta identificano specifiche applicazioni o servizi sui dispositivi, permettendo così la corretta consegna dei dati al processo appropriato.

Non esiste un servizio di consegna veloce o che garantisca l'ampiezza di banda.

I pacchetti del livello trasporto sono chiamati o segmenti (TCP) o datagrammi (UDP).

Gli obiettivi dei protocolli di trasporto sono:

1) Indirizzamento a livello di trasporto: Su uno stesso host possono essere disponibili più connessioni.
2) Multiplare e demultiplare i pacchetti provenienti dal livello di rete sulle diverse connessioni.
3) Gestire il controllo degli errori, i numeri di sequenza e il controllo di flusso. Lettere raccolte per spedire (multiplexing), per consegnare (demultiplexing)
4) Controllo della congestione.

Per stabilire una connessione tra due dispostivi è necessario individuare l'host locale e remoto e il processo locale e remoto. L'host sarebbe l'indirizzo IP mentre il processo sarebbe il numero di porta. L 'insieme di indirizzo IP e porta crea il socket Address.
Un socket address è un'identificazione univoca di un endpoint di rete. Un socket address combina l'indirizzo IP e il numero di porta, permettendo così a un'applicazione di specificare non solo quale host vuole raggiungere, ma anche quale servizio (o processo) su quell'host.

TCP (Trasmission Control Protocol): Protocollo affidabile consegna nell'ordine di invio instaurando una connessione (connection-oriented). Cerca prima di scambiare messaggi per capire se la destinazione è raggiungibile , cerca di costruire un canale affidabile e se ha degli errori cerca di recuperare.

Le applicazioni che utilizzano il protocollo TCP/IP si registrano a un "indirizzo di porta" sul livello di trasporto. La porta è un meccanismo che ha a disposizione un'applicazione per identificare l'applicazione remota a cui inviare i dati. Le porte hanno 16bit.

Demultiplexing: Capacita di un protocollo di trasporto di indirizzare in modo corretto i dati ottenuti al processo appropriato sull'host destinatario, grazie ad informazioni come l'indirizzo IP e il numero di porta. Si usa la socket, una astrazione dei software per i meccanismi di comunicazione che vengono usati al livello sottostante. É una porta attraverso quale i dati passano dalla rete al processo e viceversa.

Demultiplexing UDP: Più semplice rispetto a TCP, quando un host riceve un pacchetto UDP il demultiplexing si basa sul numero di porta di destinazione. Ogni pacchetto contiene informazioni sulla porta di destinazione che indica l'applicazione a cui deve essere consegnato il pacchetto. Ogni pacchetto è autonomo e indipendente. La sua socket ha indirizzo IP e numero porta destinazione.

Demultiplexing TCP: Prima di demultiplare i dati ricevuti TCP identifica la connessione associata con l'indirizzo IP e il numero di porta e durante il demultiplexing deve gestire lo stato della connessione. TCP garantisce che i dati vengano consegnati in ordine e tutti, utilizzando i numeri di sequenza. La sua socket ha indirizzo IP di origine e destinazione e numero di porta di origine e destinazione.

Le varie porte definiscono i servizi TCP disponibili. Le porte da [0-1023] sono Well-Known-Ports da [1024-49151] Registered-Ports, [49152-65535] Dynamic or Private Porta.

Al di sopra del livello trasporto c'è il livello applicativo il cui più noto è l Http.

3 Way Handshake, instaurare connessione TCP:

1) Il client invia un segmento SYN al server dove specifica il numero di sequenza iniziale. In pratica gli chiede di iniziare una connessione.
2) Il server riceve SYN risponde con un segmento SYNACK. Il server alloca i buffer e specifica il numero di sequenza iniziale del server. In pratica accetta la connessine.
3) Il client riceve SYNACK e risponde con un segmento ACK che può contenere dati.

Il numero di sequenza iniziale è cruciale per la gestione e il controllo del flusso di dati in una connessione TCP. Garantisce che i dati siano trasmessi in modo ordinato, rilevando e gestendo duplicati e garantendo la corretta sincronizzazione tra i dispositivi comunicanti.

Per la chiusura della connessione TCP:

1) Il client invia un segmento di controllo FIN al server
2) Il server rivede il segmento e risponde con un ACK e invia un FIN.
3) Il client riceve fin e risponde con un ACK
4) IL server riceve un ACK e la connessione viene chiusa.

In genere l'ACK non viene inviato istantaneamente ma ritarda l'invio sperando di avere dati da spedire.

Quindi TCP ha un mittente e un destinatario, inoltre con il controllo di flusso e di congestione definiscono la dimensione della finestra. La connessione è full-duplex ed è orienta alla connessione infatti inizializza lo stato dei mittente e destinatario. Flusso controllato.

Le due funzionalità sono di ritrasmissione e di ricezione e riceve un flusso di dati e li spedisce affidandoli all'indirizzo ip.

Controllo di flusso: Il mittente non vuole sovraccaricare il buffer del destinatario tramettendo troppi dati troppo velocemente. Usa un meccanismo a finestra scorrevole come al livello 2. Vado a numerare il numero di sequenza e vado ad indicare in byte la dimensione della finestra. Il ricevente indica la dimensione della finestra che può gestire in un dato momento. Se si indica una finestra 0 il mittente non può trasmettere i dati. Il mittente può forzare mandando un messaggio da un byte per indicare la prossima finestra. Si usa il timeout di attesa dell'ACK dopo di che si provvede a mandare i dati in caso di problemi.

Controllo congestione:
- Punto-Punto: Nessun supporto alla rete e la congestione è dedotta osservando le perdite e ritardi (Adottato da TCP)

- Assistito dalla rete: I router danno dei feedback ai sistemi terminali un bit per la congestione e comunica in modo esplicito dal mittente la frequenza.

Controllo di congestione capacita adeguata a quella di invio. Per risolvere la congestione vedo le consegne degli ACK e vedo se sta succedendo qualcosa di strano e la risolvo rallentando molto l'invio. Per il controllo della congestione parte piano a poi aumenta esponenzialmente e in casi di problemi (hack duplicati) diminuisce

UDP (User Data Protocol): Non affidabile consegna quando può nell'ordine in cui può , protocollo molto snello. Invia solo il messaggio se arriva bene altrimenti non fa nulla. Ha un header di 8byte. Una volta che mando un datagramma con UDP non posso fare nulla se non sperare che arrivi, si occupa di un datagramma per volta senza frammentare cosa che farà forse ip. UDP è quello di più vicino ad IP non fa nulla di più tranne la multiplazione. Non ha un concetto di flusso o direzione. Quando si passano dati con UDP qui prendo un pacchetto e lo do e questo ciò che fa la sua interfaccia. Mette solo l'header. Tutta la logica quindi di frammentazione deve essere messa al livello superiore. Utilizzo checksum facoltativo. Può essere usato con multicast e broadcast cosa che TCP non può fare. Velocità ed efficienza faccio pochissime operazioni o non faccio nulla e minimizzo il dispendio energetico.

Lezione 13 Quasi completa

Livello sessione gestisce un connessone di comunicazione, ovvero uno scambio di informazioni temporaneo e interattivo tra due o più dispositivi.

Quindi il livello sessione deve stabilire la connessione , gestire le sessioni , aggiungere punti di sincronizzazione e gestire flusso dati.

Una Connessione è tutto quello che viene fatto da due end point per scambiare dati tra loro.

Sessione invece è da quando inizio a scambiare dati (ordine del tempo).Sessione collegato al concetto di stato una delle due parti infatti deve conservare informazioni sullo stato corrente. Non dipende dal livello applicazione , troviamo le sessioni anche a trasporto.

Livello presentazione: Trasforma dati al livello superiore, qualcosa che non è flusso di byte in flusso di byte. Non è solo presentare i dati ma anche la crittografia, dove mette la compressione dei dati, il trasporto non fa compressione che invece il livello presentazione deve dare.

Livello applicazione: Deve definire i tipi di messaggi scambiati e la loro sintassi, la semantica dei campi e le regole per come si deve rispondere ai messaggi. Al livello trasporto abbiamo parlato di scambio dati ma non gli abbiamo dato un significato. Perché se mando un messaggio devo rispondere in maniera opportuna.

Applicazione su rete: Applicazioni che girano su nodi diversi, non sono monolitiche e si può interagire con più nodi da disciplinare, hanno obiettivi requisiti.

Protocolli di rete:

1) Client-server: Architettura che ha due tipologie di nodo:

- Server passivo se non arrivano le richieste, ha un ip fisso ed è ospitato per avere il nodo sempre disponibile. Tutti server devono essere noti ai client.
- Il client è un elemento che si attiva e disattiva in base alle necessità, e fa richieste; non si conosce l'ip ma deve conoscere sempre l'ip del server e non conosce gli altri, quindi non può contattare gli altri client.

2) Peer-to-peer (P2P): Non c'è un unico nodo come ruolo ma tutti nodi hanno stesse responsabilità comunicano tra loro , spalmo le responsabilità tra tutti i nodi e tutti devono essere noti. I peer non devono

essere tutti attivi e cambiano indirizzo IP.

3) Ibride: Il problema client-server è che è sbilanciato sul server nel P2P può essere che nessuna abbia risorse adeguate per rispondere a tutte le richieste , in più nel P2P potrebbe capitare di non sapere chi contattare per ottenere le risorse. Quindi l'ibrida combina P2P e client-server. Scambio P2P logica centralizzata.

Processi comunicanti: Un processa invia e riceve messaggi grazie alla sua socket. Affinché un processo su un host invii un messaggio ad un processo su un altro host il mittente deve identificare il processo destinatario, non è sufficiente per farlo conoscere l'ip perché sullo stesso host potrebbero esserci più processi, per questi si utilizza la porta.

Requisiti: Se devo trasferire dati mi chiedo se devo tollerare la perdita di messaggi e scegli se TCP o UDP. Non tutto è coperto dal livello trasporto per esempio TCP non mi da la sicurezza quindi i livello applicativo non va solo a disciplinare i messaggi ma va anche ad aggiungere le cose che mi mancano.

DNS [Domain Name Server]: Astrazione che serve per la navigazione su rete. Non devo imparare i numeri ma posso sapere solo quale qual'è l'indirizzo mnemonico. Il nostro computer deve chiedere a un nodo che gli dia una tabella dove c'è la corrispondenza none mnemonico e indirizzo ip. Questo ovviamente non può essere solo su un solo nodo ed è ciò che fa il DNS. Si trova ad un livello più alto perché distribuito su più nodi mentre il livello 4 parla con un solo nodo. DNS svolge ruolo server (ha la "tabella") client che fa richiesta. Per il client il DNS è una scatola chiusa in cui mando informazioni. La richiesta va mandata a qualcuno ovvero il server DNS. I nodi DNS sono distribuiti ad albero.

Tipologia di server DNS:

- Server dei nomi locale, server vicino ed è li che arriva la prima richiesta. Quel nodo se non ha la corrispondenza va alla radice.
- Server dei nomi radice, se il server dei nomi locali non può soddisfare immediatamente la richiesta di un host invia qui la richiesta. Lui a sua volta indica un server dei nomi autoritativo che può soddisfare la richiesta.
- Server dei nomi assoluto: Un server è assoluto per un host se ha sempre un record DNS che traduce l'hostname in IP per quell'host.

Risoluzione iterativa: Il client DNS (di solito un server DNS locale) chiede una risposta ai server DNS superiori, uno alla volta, e riceve risposte che gli indicano quali server DNS contattare successivamente fino a trovare la risposta definitiva.

Risoluzione ricorsiva se non ha risorsa va alla radice e gestisce la richiesta negoziano con altri name server della gerarchia. Più leggero ricorsivo, ma nel ricorsivo se cade la conversazione si deve ritornare al nodo radice l'iterativo da un maggiore controllo perché sa che punto della conversazione siamo. Il DNS ha una cache e memorizza le corrispondenze. I DNS radice sono 13 nel mondo.

Server TLD: Si occupano dei domini com, org... e di tuitti i domini di alto livello

Quando un applicazione deve convertire un nome di un host in indirizzo IP chiama la procedura resolver che contratta l DNS del suo dominio.

Posta elettronica ha tre componenti principali:

- Agente Utente: Mail reader sono programmi per leggere e gestire le mail, possono utilizzare protocolli come IMAP e POP3
- Server di posta: Contiene messaggi in arrivo per l'utente nella casella di posta ed ha la coda di messaggi da trasmettere. Usa SMTP per inviare messaggi client come server di posta trasmittente e server che è il server di posta ricevente.

- SMTP (protocolli posta): Asincrono che si basa TCP. Agente di posta costruisce a richiesta di posta e la manda al server di posta. La loro comunicazione è il protocollo SMTP. Protocollo client server.

Funzionamento Posta:

1) Si usa l'agente utente per comporre un messaggio da inviare ad un indirizzo mail
2) L'agente utente del mittente invia al server di posta del mittente e mette il messaggio nella coda
3) Il lato client di SMTP apre una connessione TCP con il server di posta del ricevente
4) Il cliente SMTP invia il messaggio sulla connessione TCP
5) Il server di posta di posta del ricevente mette il messaggio nella casella di posta del ricevente
6) Il ricevente usa il suo agente utente per leggere il messaggio.

Gli indirizzi mail sono risolti dal DNS che individua il server a cui inviare la posta.

MIME: Server per mandare contenuti diversi da testo.

POP3:principalmente utilizzato per scaricare e eliminare i messaggi dal server.
IMAP: Offre più funzioni e consente la gestione e la sincronizzazione dei messaggi direttamente sul server.
HTTP: Utilizzato per accedere ai servizi di posta elettronica basati sul web come Hotmail e Yahoo! Mail.

URL: Identificativo nel web di una determinata risorsa ed è permanente e non può cambiare. La part di rendering è fatta dal browser che fa la rappresentazione grafica della risorsa. I browser ci aiutano nella navigazione.

URL è formato da:

1) Protocollo: Protocollo di comunicazione per accedere ai server
2) Username e password (opzionale): Credenziali per accedere ad una risorsa
3) NomeHost: L'indirizzo fisico del server su cui risiede la risorsa
4) Porta (opzionale): Serve quando il processo server è in ascolto su una porta non conforme allo standard.
5) Percorso (opzionale): Percorso nel file system del server che identifica la risorsa.
6) Query string server per passare al server parametri.

HTTP: Protocollo a livello applicazione del WEB che ha modello client-server. Ogni sito WEB ha un processo server in ascolto su una porta TCP, la standard è l'80. È utilizzato per trasferire ogni tipo di risorsa su WWW. Web server instaura una connessione TCP. I messaggi HTTP sono dei messaggi con un header e un corpo. Http da codici di risposta.

Proxy HTTP: é un server che si interfaccia con il server di destinazione e serve a perché alcune volte deve partire da una determinata rete. Fa da intermediari e vede che la richiesta non parte dalla mia rete ma dalla proxy.

Differenza tra VPN e Proxy : VPN crea un canale sicuro tra due reti mentre proxy che un intermediario.

Connessioni persistente mantengo aperto TCP

Http 1.2: Compressione delle intestazioni , mando solo la differenza tra le richieste. Novità è anche il pipelining. Manda più richieste anche se non ha risposta. Server push: Se so che alcune richieste sono fatte da una successione di richieste non mi aspetto la serie di richieste ma inizio ad anticipare.

Http 2.0: Multiplexing e viene introdotto il server push e viene migliorata la sicurezza. Aggiunto framing binario per ridurre il sovraccarico. Migliorata sicurezza. Si usa l'id stream per creare più richieste sotto un unica connessione TCP. Http2 offre la priorità ponderata che consente agli sviluppatori di decidere quali risorse caricare per prime. Migliora il server push mandando del contenuto anticipato. Come HTTPP 1.2 comprime i messaggi ma ora usa HPACK che è meglio.
Compressione di messaggi e utilizza una codifica binaria per comprimere l'intestazione con la codifica di Huffman.

HTTP 3.0: Non usa TCP ma usa UDP e simula a livello più alto le cose di TCP. In realtà non usa esattamente TCP ma QUIC. Per favorire la scambio delle chiavi di configurazione.

CDN: Infrastruttura creata per distribuire efficacemente agli utenti i contenuti dei siti web più popolari. Vuole alleviare il server dal carico degli utenti e proteggerlo dai picchi improvvisi, vuole offrire contenuti ai singoli utenti tramite server collocati in loro prossimità. Vuole anche rendere il sistema di distribuzione più affidabile e robusto ai guasti.