Appunti di reti di calcolatori e programmazione di reti

Prime lezioni

Nozioni generali

Possiamo iniziae con una semplice definizione, ovvero cos'è l'**internet**? Bene, per rispondere a questa domanda bisonga prima avere dei concetti pregressi prima di poter rispondere concretamente a questa domanda.
Innanzitutto, partiamo dall'esterno con i dispositivi, ovvere la parte **finale** della nostra rete, loro infatti sono i responsabili dell'interfaciamento con gli utenti e per questo sono agli estremi e vengono chiamati **Internet's edge**. Questi dispositivi si interfacciano con l'esterno grazie a degli **switches** nel caso di connesione cablata oppure tramite degli **Access Point** nel caso della connessione wireless. In generale tutti i dispositivi si interfacciano a uno switch in una rete (domestica ed aziendale). A loro volta, gli switch si interfacciano con i **router** che si interfacciano con la rete centrale detta **ISP** (internet service provider, ma questo lo vedremo dopo). Tutto questo permette di creare dei **network**, ovvero un insieme di tutti questi apparecchi elencati sopra che lavarono per ricevere e spedire ***dati e informazioni***, questo è l'internet.

Altre nozioni

L'internet però è governato da delle regole rigide che permettono lo spostamento dei dati in tutto il mondo grazie alle infrastrutture interconnesse di ISP. Tali regole sono dettate dai **protocolli** i quali sono delle vere e proprie regole che definiscono il formato dei messaggi inviati e ricevuti tra le entità di un network.

Mezzi trasmissivi

Per inviare i dati utilizziamo diversi mezzi trasmissivi come quelli **guidati e non guidati** oppure con i **cavi incrociati** o twisted pair. I più usati rimangono ancora il cavo coassiale e la fibra ottica:

- Il primo lavora con dei conduttori in rame con un rivestimento molto spesso per evitare disturbi;
- Il secondo è una fibra di vetro che trasmette fasci di luce ad altissima velocità. Ha però bisogno di ripetitori per poter riacquisire la sua forza durante il tragitto.

Network Edge

Con **Network Edge** è già stato spiegato che tutti i dispositivi ai agli estremi di un network sono chiamati *host* (sia client che server). Questi si collegano tramite una connessione wireless o cablata a network

esterni che poi si andranno ad interfacciare al **Network core**, ovvero un grafo di routers conenssi tra di loro che possono collegare più ISP tra di loro tramite collegamenti chiamati **IXP** (Internet exchange point) oppure tra router come il collegamento di **peering** (o peer to peer che in italiano vuol dire tra simili).

Accesso alle reti

Gli accessi alla rete sono molteplici e, ocn il passare del tempo, sono cambiati sia nel modo trasmissivo che nei mezzi veri e propri. La **DSL** è stata una delel prime reti fruibili a tutti nelle case, questo perchè sfrutta i doppini telefonici già presenti nelle case. In linea di massima questo è stato possibile con la diviisione del canale tramite uno *splitter* così da poter far passare sulla stessa linea sua la rete che la voce grazie a una divisione in frequenza.

Come avviene l'invio

Quando un'host deve inviare delle richieste il procedimento non risulta così semplice come pensiamo, infatti il nostro messaggio viene suddiviso in **pacchetti**. Ogni pacchetto ha una dimensione fissa e vengono instradati tramite un **link** (mezzo trasmissivo come una rete cablata) fino allo switch. Ogni rete ha una capacità trasmissiva che viene misurata generalmente con bits/sec. Una formula permette di calcolare il ritardo totale dell'instradamento dei pacchetti con la formula **L/R** dove L è la lunghezza in bit dei pacchetti e R è la capacità trasmissiva

---

Forwarding e Routing

Nell'instradamento dei pacchetti troviamo il **Forwarding e Routing** come funzioni necessarie per la ricerca di un giusto percorso dei pacchetti inviati. Con **Routing** definiamo un instradamento generale, ovvero il network sceglie il percorso più veloce ed efficiente tra un router e l'altro. Il **Forwarding** invece è quel sistema che permette la gestione in particolare dell'instradamento, è come se decidesse su quale router è meglio "svoltare" nel suo tragittoche, ricordiamo sempre dura centesimi di secondi.

L'instradamento

Nella fase di instradamento troviamo dei ritardi dovuti a diverse caratteristiche della comunicazione stessa, ecco qui un elenco:

- Durante l'instradamento il delay non è dato solo come quello totale citato prima, ma ne esistono di diversi tipi e forme. In genera 3 dei 4 tipi di delay nascono dal router. Il primo detto **store and forward (trasnmission)** dove i pacchetti vengono inviati dall'host al router fino al completamento totale del singolo pacchetto. Questo avviene per tutto il processo di instradamento dei pacchetti.
- Oltre a questo tipo di delay si pone il problema della fila o **queue** dove i pacchetti provenienti dagli host hanno una velocità di trasmissione dal link precedente molto maggiore di quello successivo. Questo forma nello switch un ritardo interno (**bottle neck**) dove una fila di pacchetti si ferma e deveono aspettare che quelli davanti siano sviluppati (questa coda è anche chiamata FIFO, ovvero first come first served).

Se la coda dovesse essere troppo lunga i pacchetti arrivati per ultimi vengono persi e rispoditi successivamente. Inoltre, una legge permette di calcolare l'intensità del traffico moltiplicando la lunghezza del pacchetto per la quantità media di pacchetti in arrivo fratto la capacità trasmissiva della rete. Se il risultato dovvesse essere maggiore di 1 allora si ha il bottleneck, altrimenti il delay può variare da molto piccolo con valore intorno allo zero fino a un delay medio con il vavlore che si approssima ad 1. Tutto questo venne teorizzato e poi sviluppato da **Kleinrock**

- Il tipo di delay principale è quello di **propagazione (propagation)**, ovvero quello che divide il nostro router a quello del destinatario. Questo delay è quello principale perchè nel caso di un trasferimento di dati trans-oceanico avremo molto delay, si parla di almeno 200ms. Ma nel caso la distanza sia molto piccola il delay creato da questa caratteristica è quasi inesistente.
- Un delay che esiste ma in linea di massima non influenza veramente la trasmissione è quello detto **nodal processing**, ovvere quel tempo di trasposto del pacchetto dal nostro host al router.

Throughput

Con questo termine si indica la capacità trasmissiva della rete misurata in bit/sec . Questa definizione viene spesso accompagnata da quella di bottleneck già vista in precedenza dove la quantità di dati in arrivo da un primo link ha un Throughput maggiore del link in uscita. Questo provoca ritardi e, nel peggiore dei casi perdita di pacchetti

Commutazione di circuito

La commutazione di circuito è un'alternativa a quella di pacchetto dove la comunicazione avviene su la rete telefonica tradizionale. Questa rete viene divisa tra gli utenti che la utilizzano così da rendere un singolo canale valido per più utenti contemporaneamente. La divisione può essere **a divisione di frequenza** oppure a **divisione di tempo**. La differenza principale tra le due commutazioni sta nella divisione del canale trasmissivo, questo perchè nonostante quella di circuito abbia una migliore capacità trasmissiva non può essere usata contemporaneamente da molti utenti. Invece, quella di pacchetto permette a molti utenti di inviare informazioni graie a una tecnica dove il canale si mette in **idle (riposo)** quando non trasmette. Inoltre, quella di pacchetto trasmette in un modo **bursty**, ovvere con un forte *colpo* e poi smette, questo avviene ad intervalli regolari per permettere a tutti sulla rete di poter inviare dati.

I Network

Come già citato prima, gli ISP sono coloro che formano la rete vera e propria, ma anche loro hanno bisogno di avere delle regole per poter funzionare a dovere. Prima di tutto devo avere una certa **topologia** (forma) che gli permetta di comunicare con il minor numero possibile di **hop** nella rete. Questi ISP sono suddivisi in reti che parlano tra di loro con degli **IXP (Internet Exchange Point)** che sono messi tra una rete di ISP e un'altra. Gli ISP devono essere concentrati perchè su di loro vengono inviati i dati e i servizi del **Content provider network**, ovvere di tutti quei servizi che offrono dei servizi come Netflix o Youtube. Poi questi servizi arrivano a noi utenti tramite delle regional ISP, che non sono altro che delle reti più piccole che poi arrivano a noi clienti finali.

Security

Introduzione

All'inizio di internet la sicurezza non era neanche stata presa in considerazione dai creatori stessi ,questo perchè internet doveva essere una risorsa resa disponibile ai soli governi, scienziati ecc...
Però con il passare del tempo e con l'avanzamento scientifico internet è arrivato nelle case dei cittadini e, quando una cosa diventa comune se ne pagano le consequenza se non viene gestita da delle regole. Internet è uno di questi casi dove i network erano constantemente attaccati nei suoi primi anni di vita.
Naturalmente ci sono diversi tipi di attacchi che un mal intenzionato può fare per provare a rubare informazioni al un utente, ecco un elenco:

- **Packet sniffing** è il nome utilizzato per il tipo di attacco non grava che permette a un malintenzionato di poter vedere il pacchetto durante il traffico dati e leggere delle informazioni al suo interno come la **header e i protocolli utilizzati**, ma anche l'ip del mittente e destinatario.
- La fase successiva è quella dell' **Ip spoofing** dove viene ruabta l'identità e si mandano pacchetti cammuffati nella sequenza di pacchetti del mittente, così da poter inserire codice malevolo.
- Il peggiore è il **Dos (Denial of service) e il DDos (Distributed denial of service)** dove, proprio come ci dice il nome, andiamo a negare un servizio bloccandolo con un overflow di pacchetti che portano a un malfunzionamento globale del sistema per colpa delle troppe richieste. Il DDos funziona allo stesso modo ma con una rete di botnet alle sue spalle, ovvero un'organizzazione ben gestita di attaccanti che inviano contemporaneamente richieste a un serve che alla fine non riesce a reggere il carico.

A tutti questi problemi le soluzioni elaborate sono disponibili con i concetti dei **pilastri della sicurezza**, ovvero:

- **Authentication** grazie all'utilizzo di credenziali univoche per ogni utente connesso alla rete.
- **Confidentiality** grazie a una serie di algoritmi di crittografia come l'MD5 o l'SHA.
- **Integrity check** che permette di firmare digitalmente un documento così che il criterio della paternità.
- **Access restriction** con l'utilizzo di VPN con protocolli di tunneling e incapsulamento dei dati.
- **Firewall** ovvero difese di tipo hardware e software presenti nei dispositivi che dovrebbero formare ina linea difensiva, come dice il nome muro taglia fuoco.

I Protocolli

Definizioni e concetti generali

Come già detto prima, i **protocolli** sono delle vere e proprie regole che definiscono il formato dei messaggi inviati e ricevuti tra le entità di un network. L'organizzazione dei protocolli è di tipo stratificato,

dove ogni protocollo lavora in un ben definita area della comunicazione.

Tipo	Descirzione
Applicazione	Supporta le applicazione network come il protocollo HTML o SMTP
Trasporto	Per il trasferimento dei dati da processo a processo grazie all'incapsulazione
Rete	Invio dei datagrammi incapsulati da sorgente a destinatario e invio dei dati tra due elementi vicini in una rete
Fisico	Livello base dove si lavora con l'hardware

Questa pila è detta **TCP/IP** ed è stata inventata da inforamtici Americani. Noi Europei invece abbiamo creato una pila simile chiamata **ISO/OSI** che però non ha avuta vita lunga dato che aggiungeva 2 layer alla già esistente pila Americana che in realtà sono stati unificati nella fase di trasporto. Questi due layer sono **Sessione e Presentazione**.

Modulo 2 Appunti

Mezzi trasmissivi

Per segnale definiamo la forma dell'informazione. Può essere di tipo analogico o digitale. Quello analogico varia in un certo range di valori.

Segnali analogici

Un segnale è caratterizzato da 3 parametri:

- **Ampiezza**, ovevro il picco di un segnale;
- **Frequenza**, quanto velocemente il picco torna a valle e vice versa;
- **Fase** movimento della curva sull'asse delle x;

Più sinusoidi unite tra di loro possono avere come risultato un segnale molto diverso dalle 2 originarie. Questo perchè sicuramente i primi 2 segnali (sinusoidi) erano diverse. L'unità di misura della frequnza è l'**Hertz**.
Sequenze significative si chiamano **larghezza di banda (bandwidth)**. Più è complesso un signela più sarà grande la lunghezza di banda. Non tutte le frequenzo sono trasmesse allo stesso modo, questo comporto un cambio del mezzo trasmissivo per diverse frequnze. Con l'arrivo dell'elettronica negli anni 70'/80' si può applicare la teoria del **sampling**, ovvero del campionamento nel tempo dell'onda sonora prendendo l'ampiezza ogni x secondi. È molto importante avere un criterio di campionamento dell'onda analogico.
Il **Teorema di Shannon** dice che il campionamento di un'onda analogica, affinchè non si perda sengale, deve essere fatto 2 volte la frequenza del sengale stesso. Con il quantizzatore possiamo prendere il singolo campione e digitalizzarlo in un segnale digitale trasformando il valore prima in decimale e poi in binario.
Le caratteristiche che comporta il passaggio al digitale sono:

- L'**integrazione** che permette di avere un solo sistema per la comunicazione dei dati, dato che ora le informazioni sono condivise tramite bit e non più pacchetti come prima che, potevano essere più grandi rispetto al canale trasmissivo e quindi venivano troncati.
- La **computazione** è la trasformazione dell'informazione da analogico a digitale tramite i bit che sono processabili con computer.

Trasmissione

La **Multiplazione** è un network che permette la condivisione in un canale di più link. Ci sono 2 tipologie di multiplazione, ovvero quella a divisione di **frequenza** e quella a divisione di **tempo**. Le differenze principali, anche se già spiegate in precedenza, sono principalmente il tipo di sengla che viene trasmesso. Ovvero in quella di frequenza dividiamo il segnale, nella seconda dividiamo i bit.
La multiplazione a **divisione di codice** che, con una elaborazione matematica permete di mandare le informazioni tutto il tempo dividendole dalle altre che stanno comunicando.
Quando faccio la multiplazione a divisione di tempo dobbiamo definire delle *fasi*.
Dobbiamo tener presente degli istanti di tempo, o meglio **slot**, dove dividiamo il tempo in unità fondamentali che permettono la trasmissione solo ad intervallo di tempo predefinito. La versione **unslotted**, senza istanti di tempo, permette la trasmissione senza divisione temporale, dove tutto viene condiviso insieme allo stesso tempo. Nel caso della soluzione slotted, possiamo formare dei *gruppi o **frame*** dove le informazioni vengono organizzate con dei divisori.
Il canale telefonico digitale ha uno standard trasmissivo di 64000 bit al secondo.
L'Europa per trasmettere utilizza lo standard **frame E1**, questo perchè la trasmissione slotted framed permette un controllo accurato di tutta la trasmissione. Questo però porta un limite massimo di trasmissione. Il limite di trasmissione viene superato da un TDM unslotted dove ogni blocco di bit viene legato al mittente.
Se la nostra comunicazione ha bisogno di una grandezza ben specifica dobbiamo usare lo slotted framed, mentre se non abbiamo bisogno di una grandezza fissa (come il messaggio di whatsapp o skype) usiamo quello unslotted. In realtà la differenza è che con l'unsloted non siamo interessati
Due leggi importanti sull'evoluzione della tecnologia sono quella di **Moore** e quella di **Edholm**.
La prima dice che ogni 18 mesi il numero di transistor per processore raddoppia, e questa è vera sin dal primo processore; e poi quella di Edholm che dice che ogni 18 mesi la banda a disposizione dell'utente raddoppia a costo costante.

Mezzi trasmissivi

Come primo contetto trasmissivo dobbiamo l'**attenuazione**, ovvero la misura di degrado del segnale (elettromagnetico), misurando la sua perdita di potenza e si misura in dB/km. Questa cresce in base alla distanza e a segnali di alta frequenza.
I mezzi trasmissivi principali sono stati i **doppini telefonici** e cavi di rame. In realtà il doppino è formato da 2 cavi di rame intrecciati. Questo intreccio (chiamato **twisted pair**), se fatto bene, diminuisce l'attenuazione del segnale. Con lo sviluppo i mezzi trasmissivi avevano la necessità di migliorare la loro efficienza e qualità, per quseto vediamo come il tiwsted pair si può dividere in due categorie, ovvero l'**STP (Shielded twisted pair) e UTP (Unshielded twisted pair)**. Con l'STP abbiamo un cavo formato da tante coppie avvolte un un conduttore che fa da schermo. Naturalmente i contro di questo cavo

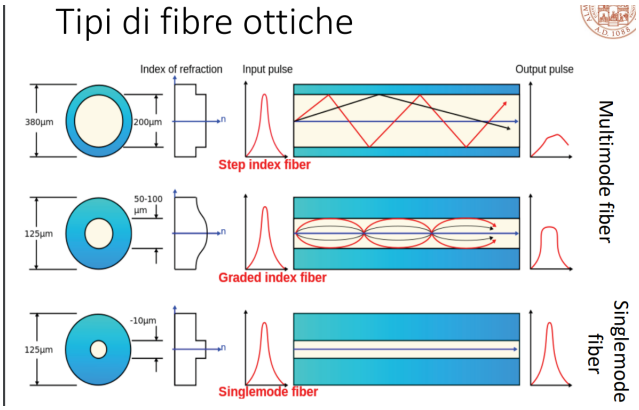
sono il maggior costo, la necessità di essere messo a massa e la grandezza. Con l'UTP invece abbiamo un cavo meno costoso, più semplice da spostare ma non schermato. I cavi vengono divisi in categorie, nello specifico dalla 1 alla 7 e vediamo come ogni categoria ha un bandwidth maggiore e una frequenza maggiore.
Il cavo STP più comune è il **cavo coassiale**. La sua sezione ha forma cilindrica, è formato da due conduttori, uno interno e uno esterno, entrambi con schermatura. Questi cavi possono differire per diamentro e quindi, possono diventare molto costosi e difficili da maneggiare. Il diametro infatti è fattore importante della resistenza all'attenuazione del nostro cavo, più è grande meno attenuazione ci sarà.

Radio comunicazioni

La radio ccomunicazione permette il broadcast (tramisssione a tutti coloro che hanno la stessa frequenza) e quindi si presenta come un ottimo mezzo diffusivo. Inoltre, non ha vincoli fisici e per questo è adatto per la mobilità. Ma come difetto ha il fatto che presenta un solo spettro radio. Le onde elettromagnetiche prodotto per la diffusione radio viaggiano in linea retta, oppure vengono trasmesse tramite la ionosfera, ovvero rimbalzando su questo strato per poi essere captate da altre antenne. La prima comunicazione radio venne effettuaa nel 1895 da Marconi con il ponte radio. Tutti questi servizi radio funzionano tramite antenne e tralicci. Ogni singola antenna ha una propria area di copertura che permette a un certo numero di utenti di potersi collegare alla rete tramite frequenza. Con la venuta delle metropoli si è ideato il sistema **cellulare** dove venivano piazzate tante **celle** per permettere la copertura totale ai clienti. Ogni cella ha una frequenza diversa e, grazie alla loro forma a scacchiera la sovrapposizione delle celle non è un problema perchè hanno frequenze diverse.

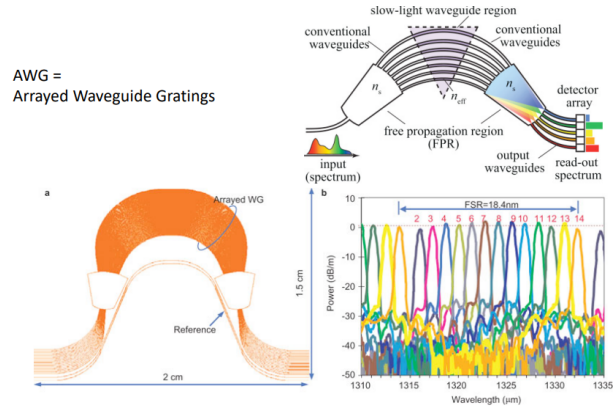
Fibra ottica

La fibra ottica è un filamento di vetro o plastica molto sottile.Facendo passare un fascio di luce in un filamento di vetro con il tempo perderà intensità perchè il vetro assorbe la luce. Per esempio un vetro di una finestr assorbe moltissima luce, questo perchè al suo interno ci sono motle impurità. Questo è dato dal fatto che il vetro è fatto di ossido di silicio, che può contenere impurità. La fibra ottica invece è fatta da vetro molto puro che non permette l'assorbimento della luce. La luce all'interno della fibra viaggia tramite riflessione grazie a un indice di rifrazione del **cladding**(mantello) più grande di quello del core.

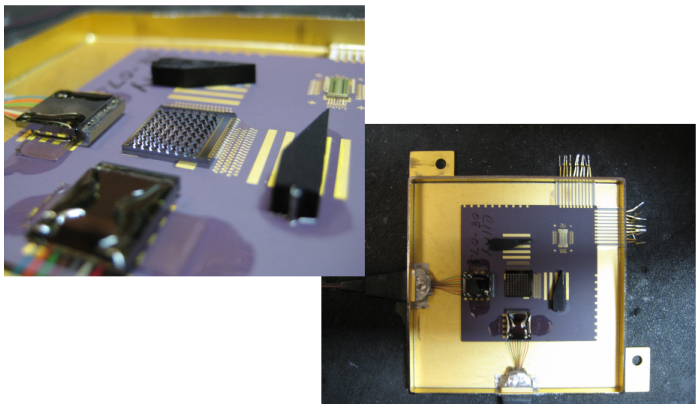


Divisione tra fibre monomodali e multimodali.
La trasmissione in una fibra è iniziata da un diodo led o laser e poi letta in uscita da un foto-rilevatore. A livello storico la fibra ha fatto un paradosso nelle comunicazioni, ovvero che è molto più performante rispetto al rame e meno costosa del rame stesso. L'unica criticità delle fibre è la **giuntatura**

(collegamento) tra due fibre. Per far si che questo avvenga è necessario un macchinario molto costoso che fonde i due cavi e il core. Con un **amplificatore ottico** possiamo far tornare l'intensità del fascio di luce al suo stadio originale tramite il **drogaggio** di una parte di cavo con il *germanio* che funzionerà da ripetitore.
Con l'evoluzione negli anni 90 si è sviluppata la possibilità di poter cambiare il colore dei laser che fino a poco prima erano solo in luce bianca. Con la presenza di laser *colorati* possiamo dividere la fibra ottica con diversi laser che però, per entrane nella fibra, devono passare per un prisma che permette a tutti i laser colorati di diventare luce binaca, ottenendo una capacità molto più elevata in base al numero di colori dei laser trasmissivi. Naturalmente alla fine della fibra ci sarà un altro prisma che da luce bianca restituisce i laser colorati. Questa divisione viene chiamata **WDM (Wavelength Division Multiplexing)** ed è un tipo di divisione di frequenza.



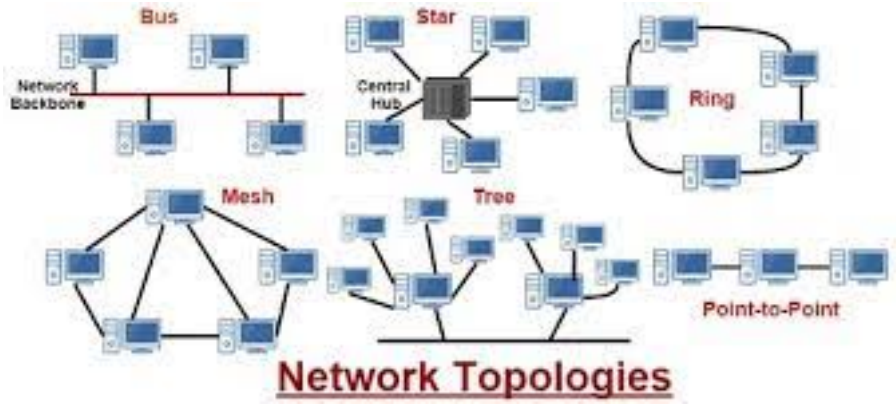
Questa immagine rappresenta una **AWG = Arrayed Waveguided Gratings** e descrive il funzionamento dei prismi in entrata e uscita della fibra ottica. Questa possibilità di spostare i fasci di luce è resa possibile dai **MEM**, ovvero dei piccoli specchi meccanici che, se angolati, permettono di direzionare i fasci di luce. Se invece non si ha più bisongo di uno specifico fascio di luce lo si fa sbattere contro un pezzo di plastica nero, questo perchè il nero assorbe la luce.



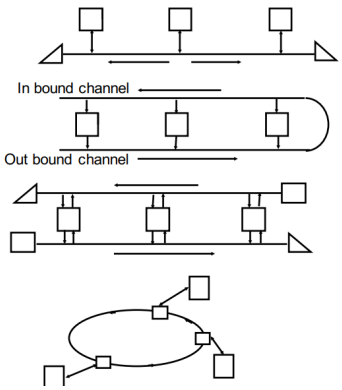
Nome	Descrizione
FTTCab	Fiber to the cabinet, la fibra arriva fno agli armadi e poi arrivano nelle case con i doppini
FTTC	Fiber to the curb, la fibra arriva fino al marciapiede
FTTB	Fiber to the building, dove la fibra arriva fino al
FTTH	Fiber to the home, dove la fibra raggiunge la singola abitazione

Reti LAN

Per **LAN** (Local Area Network) definiamo un tipo di infrastruttura di telecomunicazioni che consente agli host (dispositivi connessi alla rete) di comunicare in un'area *delimitata* attraverso un **canale fisico condiviso** con un tasso di errore basso e con un elevato bit rate (con velocità di trasmissione alta).
Le LAN sono molto utilizzate per piccole reti, dato il loro prezzo basso e conveniente. Inoltre prediligono il rame come mezzo trasmissivo e non la fibra ottica perchè essendo piccole non possono sopportare un prezzo così alto per poter ottenere delle fibre di tipo FTTH. La loro peculiarità però è la topologia (forma), ne possiamo avere di diverso tipo e questo perchè sono adattabili alle esigenze. Le più diffuse sono quelle a stella, a maglia e gerarchica. Quelle peer-to-peer (punto-punto) vengono utilizzate solo se i terminali sono pochi e quindi non serve un nodo di comunicazione.



- Bus bidirezionale
- Bus unidirezionale
- Doppio bus (dual bus)
- Anello



La seconda immagine invece rappresenta delle **topologie** punto-multipunto, queste sono particolari perchè sono in broadcast, ovvero che ogni messaggio inviato da un host viene visto da tutti gli host della rete ma, solo il destinatario effettivo lo può leggere o vedere il suo contenuto, questo grazie a un protocollo. Questi reti sono importanti perchè lavorano con un solo mezzo trasmissivo, il bus e permettono lo scambio di dati a tutti gli host in una LAN. Un problema di queste reti però rimane la collisione, perchè non esiste un mediatore tra host e bus e quindi, seppur piccola, c'è la possibilità che 2 host trasmettano nello stesso istante e quindi i pacchetti alla fine andranno persi.

Ogni scheda di rete è segnata da un indirizzo **MAC**, che sono dei codici univoci per ogni device così da poter essere riconoscibile all'intenro di una rete. Questi indirizzi hanno 48 bit (6 byte) e indicano il produttore della scheda e le schede presenti nel nostro device. La rappresetnazione del mac è in esadecimale e un esempio è: 00-60-b0-78-e8-fd

ARRIVATI FINO A PAGINA 10 LAN

Cablaggio

Si basa sugli standard **EIA/TIA 568** (standard di mercato) e **ISO 11801**. In generale in un edificio vengono inseriti diversi cavetti con coppie diverse che forniscono la classica presa a muro con il connettore RJ45.
Vengono utilizzati degli **armadi di rete** per permettere la connessione in un palazzo dall'esterno verso l'interno. Con i **patch panel** abbiamo delle prese che permettono alla rete esterna di poter arrivare in un palazzo tramite dei collegamenti laterali all'armadio stesso. Tramite l'**hub** possiamo connettere il patch panel all'hub stesso tramite i **patch cord** (cavi RJ45 UTP) così che la rete possa essere fruibile in uscita.

Wireless LAN

Per la comunicazione Wireless ci basiamo su l'etere come canale tramisisivo e, soprattutto, su alcune frequenze radio specifiche chiamate **ISM** a 2.4 Ghz. Molti sono gli standard per la trasmissione wireless e appartengono tutti alla stessa famiglia, ovvero 802.11 e tutte le sue evoluzioni.
Con **BSS** definiamo l'infrastruttura che si viene a formare quando colleghiamo degli host a un **Access Point** . Quando si vanno a guardare gli indirizzi in una trasmissione di pacchetto vederemo che gli ultimi 2 indirizza sono il destinatario e il mittente per una ragione di controllo e poi, in cima a questi due, avremo tanti indirizzi quanti sono stati gli **Hop** del pacchetto, quindi tra quanti dispositivi intermiedi è passato il pacchetto per arrivare al destinatario. I pacchetti spediti con cavo hanno solo 2 indirizzi.

Appunti di laboratorio

La virtualizzazione

Esistono due tipi di virtualizzazione, di tipo 1 e 2. Semplicemnte quella di tipo 1 permette di far girare sistemi operatvi da *"console"* in bootstrap, mentre quelle di tipo 2 permette di avviare applicazione per la virtualizzazione già da un sistema operativo.

Tabella con comandi che sarà aggiornata con il tempo. Per aprire il cmd in linux **ctrl + alt + t**, per apreire una nuova finestra **ctrl + shift + t**, per bloccare l'esecuzione di un programma **ctrl + c** e per pulire tutta la cli basta fare **ctrl + l** oppure scrivere **clear**. Molto spesso verranno citate le tabelle **arp** che in soldoni sono delle tabelle dove possiamo vedere l'indirizzo ip e il MAC del dispositivo.

Comandi di base

Nome	Descrizione
cd	change directory, quindi cambia la cartella inserendo il path (assoluto o relativo)
cp nomefile	copia il file selezionato e, dopo il nome, scrivere il path
rm nomefile	rimuove il file o cartella
man	concatenato ad un altro comando permette di leggere il manuale del comando

---

Nome	Descrizione
history	permette di vedere tutti i comandi fatti in precedenza
pwd	vedere il percorso in cui ti trovi
ls	permette di vedere la lista dei file e cartelle nella cartella attuale
ping indirizzo IP	manda dei pacchetti all'indirizzo IP segnalato e aspetta una risposta
traceroute indirizzo IP	è un ping con molte più informazioni
alias comando='comando'	permette di mascherare il comando di destra con quello di sinitra. Per una migliore comprensione degli esercizi consiglio di fare alias ip='ip -c'. Per togliere questo alias basta scrivere unalias ip
sudo nome_applicazione &	avvio applicazione in background
sudo chmod +x nomefile	permette di dare l'accesso di eseguire il file. come negli sh

Nota bene l'appendice (o meglio flag) *-c* permette di colorare ed evidenziare le scritte in uscita, quindi è applicabili alla gran parte dei comandi che restituiscono un output.
Per lavorare da shell abbiamo bisogno dei **Namespace**, ovvero degli *oggetti* (anche se il termine è improprio) di tipo astratto creando uno stack di rete che si appoggia sul kernel di sistema isolato da tutto. Questi namespace, anche se possono essere utilizzati in molti modi, nel nostro caso saranno i dispositivi di rete, ovvero host, router e switches tramite il comando **ip netns**.

Comandi per la rete

Nome	Descrizione
ip	Questo è il comando universale che permette di vedere le tabellle di routing, manipolare dispositivi e interfacce. Funziona da ipconfig
nano nomescript.sh	per aprire uno script e scrivere da cmd
touch	per creare dei file
ip –c neigh	interroghiamo la tabella di routing, neigh vuol dire neighbourhood quindi vicinato
ip -c link	interroga la routing table del nostro dispositivo per vedere le interfacce, questo è più completo rispetto al comando sovrastante. In realtà questo comando è la versione troncata di ip link, questo perchè ubuntu accetta questa sintassi
ip -c a	permette di vedere gli indirizzi ip delle interfacce e l'indirizzo mac del dispositivo
ip -c r	permette di vedere le routing table del dispositivo su cui lo avviamo. Per routing table definiamo le vie percorribili dai pacchetti
ip addr	mostra tutte le interfacce e il relativo indirizzo IP

Nome	Descrizione
ip addr add indirizzo/subnet mask dev nome_interfaccia	permette di aggiungere e indirizzi alle interfacce
ip addr del indirizzo/subnet mask dev nome_interfaccia	permette di rimuovere e indirizzi alle interfacce
sudo	**super user do** serve per fare comandi da amministratore (in questi esempi useremo sempre questo comando perchè non abbiamo il ruolo di amministratore profilo ubuntu)
sudo !!	permette di utilizzare il comando precedente aggiungendo sudo senza doverlo ricopiare
ip netns	comando per la gestione dei namespace (dispositivi)
sudo ip netns add nome_host	permette di creare un nuovo host (namespace)
sudo ip netns del nome_host	permette di rimuovere un host già esistente
sudo ip netns exec nome_host comando	esempio pratico che permette di eseguire dei comandi sull'host selezionato tramite il comando exec
sudo ip netns list	Permette di vedere in una lista tutti i dispositivi (namespace) esistenti
sudo ip -all netns delete	rimuoviamo tutti i namespace creati
ip link	è un comando per la configrazione dei dispositivi, è sempre concatenato con altre *particelle o **flag*** (è la stessa cosa di ip l)
sudo ip link add **nome** type **tipo**	permette di creare le interfacce (porte) inserendo un nome simbolico e un tipo, il nostro tipo predefinito per ora sarà veth ovvero virtual ethernet
sudo ip link add nome1 type veth peer name nome2	esempio reale della creazione di un cavo ethernet con due interfacce (nome1 e nome2 sono le estremità)
sudo ip link set nome_interfaccia	permette di modificare l'interfaccia selezionata grazie all'aggiunta di altre flag
sudo ip link del nome_interfaccia	permette di eliminare un'interfaccia
sudo ip link set nome_interfaccia netns nome_dispositivo	esempio reale che permette di collegare una delle estremità del cavo a un dispositvo
sudo ip link set nome_interfaccia netns bridge	esempio reale che permette di collegare la seconda estremità del cavo allo switch (bridge è un nome simbolico che indica la porta dello switch)
bridge	comando per gestire lindirizzamento degli switch

Nome	Descrizione
bridge link	imposta le proprietà delle interfacce ai collegamenti
bridge fbd	gestisce il database dei pacchetti inoltrati dal bridge (switch)
sudo ip link set nome_interfaccia master nome_switch	esempio pratico per collegare la seconda estremità del cavo allo switch
sudo ip link set nome_interfaccia nomaster	esempio pratico per scollegare la seconda estremità del cavo allo switch
sudo ip net exec nome_host ip l add default via indirizzo_ip_gateway	serve per inserire il gateway neglio host ai fini di poter paralre tra più reti
sudo ip net exec nome_gateway sysctl -w net.ipv4.ip_forward=1	permette di attivare il protocollo per l'invio dei pacchetti da un'interfaccia a un'altra

La prima cosa a cui devi pensare per svolgere un esercizio è: **Di cosa ho bisogno?** Naturalmente di host, switch e cavi.

Comandi specifi per l'esercizio

sudo ip addr add 10.0.2.16/24 dev eth0	sifica il loro indirizzo ip ask
sudo ip link add eth0 type dummy	creazione di una nuova rete di tipo dummy
sudo ip l add eth_1 type veth peer name veth1_1	creo una interfaccia ethernet
sudo ip link add LAN type bridge	creazione di una rete
sudo ip link set eth1 master LAN	connetto il mio host(eth1) alla rete LAN
bridge fbd	vedo le connessioni
sudo ip link set eth1 no master LAN	sconnetto l'host dalla rete
sudo ip n	
sudo ip netns exec H1_1 ip addr add 192.168.1.1/24 dev veth1_1	inserisco un indirizzo ip nel mio host