RETI

* LEZIONE 28/02

*Parte introduttiva*

La materia non si dovrebbe chiamare reti di calcolatori: c’è un equivoco. Prima (inizio anni ‘60) vi erano grandi mainframe che comunicavano tra loro attraverso linee dedicate (non si parlava ancora di internet) ; con il tempo questi calcolatori si iniziarono a rimpicciolire di dimensioni, però stavano solo nei grandi centri di calcolo dove vi era al massimo un elaboratore per una regione o per uno Stato. Poi uscì il pc e quindi vi era la necessità di farli comunicare tra di loro per cooperare, condivide nel contesto del lavoro. Poi con l’avvento di google, yahoo ecc. abbiamo cominciato a lavorare in un mondo più network in cui i nostri sistemi obbligatoriamente avevano necessità della rete e qui viene fuori la questione dell’equivoco: sulla rete venivano fuori altri apparecchi come lo smartphone e quindi sono oggetti eterogenei. Ora in rete inizia ad entrare frigoriferi, auto, occhiali, orologi quindi fondamentalmente troviamo più oggetti che sono in larga maggioranza rispetto ai calcolatori; quindi si dovrebbe parlate di rete di oggetti, non a caso anche il global internet si sta trasformando in “internet delle cose”.

Ma quanti sono gli oggetti in rete?

Per ora conta 10miliardi di macchine, le previsioni degli analisti prevedono che tra 2 anni avremo circa 50 miliardi di oggetti in reti di cui i dispositivi come smartphone o pc saranno una piccola parte meno del 10%. Si parla di smarthome, di smartcity …

Le reti cambiano il nostro modo di vivere.

C’è un protocollo che è un insieme di regole per far interagire gli oggetti eterogenei in rete.

Di che cosa è fatta una rete (fisicamente)?

La rete è fatta di fili, fibre ottiche, onde radio, onde elettromagnetiche , ma è fatta fondamentalmente di connessioni, collegamenti punto a punto o punto a multipunto tra oggetti.

Ma queste connessioni come sono? Internet che tipo di copertura ha? Ha una copertura world wild.

Si preferisce ancora la fibra ai segnali radio perché la trasmissione è più veloce.

La rete è fatta anche di altri oggetti ovvero proprio quei componenti che fanno funzionare la rete stessa: i router ad esempio.

Internet è fatto anche di dispositivi analogici.

*La rete in generale*

Le componenti di una rete sono sia hardware che software; dove quelle hardware sono apparati di interconnessione e di controllo della trasmissione e poi c’è la parte software che è costituita da protocolli, driver dell’interfaccia che costituiscono il modo di comunicare, il formato dei dati, il modo di gestire e rilevare gli errori, il modo di controllare la congestione (significa gestire il controllo di flusso) e la qualità del servizio (banda e latenza parametri per capire la qualità).

Cosa chiediamo ad una rete?

La rete deve essere:

* Affidabile: quello che noi mandiamo deve arrivare, inoltre deve essere in grado di rilevare e correggere gli errori;
* Efficiente: quello che noi mandiamo deve arrivare in un tempo accettabile;
* Scalabilità: deve crescere insieme al numero di utenti/nodi;
* Eterogeneità delle comunicazioni: apparati diversi devono essere in grado di interagire.

Le informazioni devono arrivare dall’altro lato nell’ordine esatto in cui sono state mandate.

Un’altra cosa fondamentale la rete deve essere in grado di individuare n possibili percossi per congiungere qualsiasi sorgente a qualsiasi destinazione e deve essere fatta anche in maniera ottimizzata cioè deve individuare tra n possibili percorsi il migliore (instradamento).

La definizione più semplice di una rete telematica: è un insieme di dispositivi informatici mutuamente collegati tra loro cioè tutti a tutti.

3 funzionalità fondamentali: trasporto, indirizzamento, commutazione.

Per definire formalmente una rete si usa un grafo con tre componenti le stazioni/macchine/utenti poi i link di commutazione e infine i nodi intermedi quelli che fanno da commutatori.

DTE cos’è? È l’utente finale, elemento host, è l’insieme di componenti hardware e software che caratterizzano l’host connesso alla rete quindi il sistema, il terminale che in qualche modo si deve connette alla rete per la trasmissione di una serie di dati (può essere un pc, un frigorifero ecc.). Ovviamente lo scopo della rete è di mettere i raid DTE (data terminal equipment ) in condizioni di comunicare tra di loro.

Come si interfacciano i DTE con la linea di comunicazione? Hanno bisogno delle interfacce fisiche, queste tipicamente hanno una loro terminologia, tipicamente si definiscono anche come date circuite equipment (interfaccia verso il circuito di comunicazione). Il DTE può parlare con la rete attraverso uno o più DCE.

Ci sono mezzi di trasmissione che posso lavorare solo punto a punto cioè un segnale trasmesso da un lato che arriva dall’altro; poi posso avere mezzi trasmissivi in modalità broadcast: cioè il messaggio arriva a tutti nella rete, questo allora comporta che si potrebbe avere la necessità di indirizzare e quindi identificare i singoli utenti.

Vantaggi di comunicazione punto a punto: tutto è più facile e tempi di attesa nulli; svantaggi sono delicate, costose, spreco di banda.

Ci sono tecniche intermedie tipo le reti multi punto in cui ci sono diversi DTE sulla stessa linea cioè un oggetto che raccoglie le informazioni e diversi DTE condividono la stessa linea trasmissiva, ovviamente deve essere gestita la contesa del mezzo fisico essendo lo stesso per tutti e questo problema c’è anche nelle reti broadcast. Nella rete broadcast possiamo trasmettere in modalità unicast (mandare un’informazione destinata ad una sola entità) o mandare l’informazione a tutti o in multicast( individua gruppi di utenti/DTE usando specifici indirizzi multicast ). Per differenziarle ci sono dei bit che specificano il tipo di indirizzo (unicast. Multicast, broadcast). Ci sono vari tipi di flussi trasmessivi:

simplex; si trasmette in una sola direzione da A a B e finisce così (ad es. tv);

half-duplex : si trasmette uno alla volta (ed es. prima trasmette A poi smette e trasmette B);

full-duplex: simultaneamente entrambe le stazioni posso trasmettere (modalità più efficiente e preferibile ).

LEZIONE 6/03

La funzione di questi nodi di fare relay cioè passare quello che ricevono da una interfaccia mandarla avanti verso un altro nodo ad un’altra interfaccia è una funzione che si chiama commutazione.

Uno switch non fa altro che fare la commutazione in maniera automatica. Stabilisce il ruolo di uno di questi elementi intermedi e stabilisce una comunicazione che (potrebbe durare ) dura il tempo del passaggio del dato tra un interfaccia e l’altra.

La commutazione può essere strutturata in due modi diversi:

* Commutazione di pacchetto;
* Commutazione di circuito.

L’analogia che ci fa capire bene come funziona la com. di pacchetto è quella di come funziona il nostro sistema postale.

Esempio. Mandare un libro di 100 pagine per posta e si può mandare una pagina alla volta. Quindi si imbusteranno tutte le pagine singole e su questa busta apporrò l’indirizzo di destinazione e si mette nella casella postale e così via per tutte. Il postino si porterà tutte le lettere della casella non solo le 100, poi verranno smistate e portate da altri postini. Fondamentalmente si aggregano tante info da mandare in un comune mezzo trasmissivo che è stato utilizzato in maniera molto efficiente (multiplazione statistica: si sfrutta la capacità del mezzo trasmissivo in maniera ottimale, lo utilizzano tutti gli utenti a cui serve e questo processo è stato fatto più volte).Ogni busta è un evento autonomo. Nessuno garantisce che le buste arrivino nell’ordine giusto: perché non è detto che facciano lo stesso percorso; nessuno garantisce che le buste arrivino, in questo caso il destinatario può avvisare il mittente che il pacchetto non è arrivato e quindi sarà rispedito dal mittente. Questo servizio è unreliable (inaffidabile ), non ha controllo, ma nelle reti questo servizio è vincente. È vincente perché questo inoltro in cui ogni evento è indipendente fa gestire molto bene la capacità disponibile dei mezzi trasmessivi e quindi degli investimenti che ha fatto. Il fatto che ogni evento può fare percorsi diversi mi dà anche un’altra garanzia, oltre al bilanciamento migliore del carico e sfruttamento migliore delle risorse, mi dà un enorme garanzia dal punto di vista dell’ affidabilità dell’infrastruttura (la rete si può adattare al cambiamento di situazione, scala benissimo ). C’è una fatica in più solo per instradare ogni singolo evento perché ognuno non ha nessuna relazione con il precedente. Ha un piccolo difetto cioè (best enfort) impegno il mezzo al meglio che lo posso utilizzare, ma non sono in grado di dire che il mio pacchetto abbia una garanzia di qualsiasi tipo.

Per capire la commutazione di circuito si può associare al vecchio sistema telefonico.

Si manda un segnale alla centrale specificando l’indirizzo di destinazione facendo un booking, la centrale individua l’indirizzo, la risorsa disponibile(la capacità della comunicazione richiesta) e richiedeva a una centrale più alta di impegnare un canale per quella destinazione indicata e così ricorsivamente sempre più in alto nella gerarchia delle centrali fino a tornare indietro all’utente finale che rispondeva al telefono stabilendo un cammino statico che durava per tutta la durata della comunicazione. Ogni informazione ha una garanzia assoluta di avere disponibile questa capacità trasmissiva, quindi la risorsa di canale impegnata è garantita nessuno altro se l’ha può prendere; in più l’instradamento avviene solo per la prima e poi non si fa più. Quando si chiude si liberano le risorse e il percorso viene rilasciato. Garanzia che il pacchetto arrivi e anche nell’ordine giusto (percorso affidabile). Questa tecnologia è perdente perché non scala. Una volta impegnate le risorse il canale sarà impegnato anche se non si invia niente. Se si devono mandare grandi quantità di dati in continuità comincia a diventare vantaggiosa la commutazione di circuito. La commutazione di circuito è stata necessaria anche per l’ingegnerizzazione del traffico, per avere una garanzia dai gestori telefonici. (SLA accordo di servizi) Questo comportava un cattivo utilizzo delle risorse e doveva avere due strati uno a commutazione di pacchetto appoggiato su uno a commutazione di circuito.

I DSE (data switching equipment) o **nodo di commutazione** è un nodo intermedio della rete, senza alcunafunzione di supporto diretto agli utenti, la cui principalefunzione è quella di commutare (switch) il traffico tra due o piùDTE non direttamente collegati tra loro. Quindi nella rete abbiamo DSE, DCE e DTE.

Topologia di rete:

è il modo in cui decidiamo di connettere tutti gli elementi che devono comunicare cioè apparati di terminazione, interfacce, commutatori e linee trasmissive in modo tale da costruire un grafo; a secondo del modo in cui si costruirà quest’ultimo condizionerà la qualità della comunicazione. Gli obiettivi sono ridurre i costi e massimizzare l’efficienza.

La più semplice di topologia è la stella, perché è il modo di connettere n nodi con il minimo numero possibile di collegamenti bastano n-1. Non funziona perché se sono pochi i nodi sta bene, per una grande no; ha 0 affidabilità se si rompe il nodo centrale si interrompono tutte le comunicazioni, non è scalabile è solo vincente dal punto di vista dei costi.

L’anello ci garantisce il minimo numero di percorsi, ma differenziandoli. Qualunque nodo si rompe la rete continua a funzionare, quindi funziona dal punto di vista dell’affidabilità, ma non è scalabile(non è sostenibile su larga scala perché avremo percorsi immensi ) e costi ok.

È utilizzato nelle infrastrutture in fibra.

Full-mesh tutti collegati a tutti, c’è una ridondanza di percorsi quindi è affidabile, ma non scala. Le topologie ordinate non scalano.

C’è anche la topologia ad albero che solitamente si utilizza negli edifici pubblici e risente dei point of failure che solitamente vengono duplicati in modo tale se si rompe uno si sostituisce con il duplicato.

Un’altra topologia è la rete a bus condiviso cioè si ha un unico mezzo trasmissivo condiviso da tutti e si dividono la capacità o attraverso la multiplazione statistica: chi ha bisogno di trasmettere si prende il canale e lo usa, in questo caso c’è bisogno di un arbitrato che ci dica chi ha il diritto in un certo momento di utilizzare il mezzo. Oppure multiplazione statica a divisione di tempo dove ognuno ha dedicato uno slot di tempo sia che trasmette sia che non lo fa però in questo caso si spreca il mezzo.

La soluzione migliore è di trovare delle topologie abbastanza organizzate e allo stesso tempo sufficientemente caotiche. Si basano sul principio “attachment preferences” e “il ricco diventa sempre più ricco”.

Quindi si ottiene un’organizzazione in cui si vanno a creare dei cluster intorno a degli hub centrali a dei grandi aggregatori di grandi attività che sono i pilastri della rete.

Quindi internet si regge attraverso una rete dove ci sono pochissimi nodi con tantissime organizzazioni e tantissimi nodi con pochissime connessioni (tipicamente una). Questa organizzazione ha una proprietà magica ovvero cercando di raggiungere un’altra connessione si devono compiere pochissimi salti.

Le 3 grandi famiglie dei protocolli

Un protocollo è una serie di norme, convenzioni e tecniche per lo scambio di dati, comandi e informazioni di controllo tra due elementi.

I protocolli di DCE parlano tra loro per scambiarsi le info di raggiungibilità, cioè questi percorsi che vengono stabiliti dinamicamente.

I protocolli sono stabiliti dagli organismi di standardizzazione promulgando delle “leggi” universalmente conosciute che si chiamano Standard. Abbiamo protocolli a vari livelli.

Ci sono tre grandi famiglie di protocolli (due importanti mentre il primo no):

* Proprietari; sono alcuni costruttori che specificano che i loro apparati “parlano questa lingua” la cui è propria e nessun’ altro la può sapere; cioè solo gli apparati che ne fanno parte interagiscono tra di loro (scarsa interazione) e non sono in grado di interagire con apparati di altri costruttori. Quindi questi protocolli/standard tendono a scomparire nella rete.
* Di diritto: definiscono delle regole sulle caratteristiche che devono avere i dispositivi ad esempio un’interfaccia eternet o wifi. Sono rigidi. (riguarda l’hardware). Vi sono grandi enti di standardizzazione come ISO, CCITT.
* Di fatto: sono utilizzati a livello più alto, ad esempio protocolli che definiscono il controllo della congestione su un circuito end to end, sono implementati a livello di driver nel sistema operativo. Sono legati a delle funzionalità essenzialmente implementate in software e quindi posso essere più facilmente gestiti. Vi sono grandi enti di standardizzazione come IETF. Le regole su Internet si trovano sempre in una forma RFC sono standard di fatto che in qualche modo definiscono le regole su Internet.

I Protocolli, per poter cooperare, devono essere formalizzati secondo questi standard, solo in questo modo si avrà l’interoperabilità universale.

Classificazioni delle reti in ragione della copertura geografica

Le reti assumono nomi diversi in ragione della copertura che li caratterizza.

Network on chip: ad esempio come comunica alu e cpu attraverso una rete a bus, distanza di pochi millimetri.

BAN (body area network): ad esempio se si possiede uno smartphone, iwatch e comunicano tra di loro.

PAN (personal area network): ad esempio se su una scrivania vi sono un pc e una stampante che sono a meno di un metro di distanza e comunicano tra di loro.

LAN (local area network): reti che hanno una copertura di un edificio o di un insieme di edifici vicini nell’ordine di qualche km al massimo 5km. Le LAN utilizzano una tecnologia comune a basso costo e con capacità abbastanza elevate (tipicamente del gb di accesso e di 10gb di distribuzione). Nella rete locale passa solo il traffico di quell’unica organizzazione che gestisce la rete locale: USO ESCLUSIVO. Per gestirle facilmente si utilizzano strutture gerarchiche.

MAN (Metropolitan area network) : reti che hanno una copertura di una città nell’ordine di 20/30km. Tipicamente utilizzano tecnologie della velocità delle LAN, ma su una scala in terminologia di costi più bassa (grandi capacità- basso costo), si fanno cose da MAN, ma con costi da LAN. Capacità dai 10 a 100gb massimo.

WAN (Wide Area Network): reti di copertura geografica a grandi distanze, centinaia o migliaia di km. Abbiamo strutture variamente meshate (perché ci interessa la ridondanza di percorsi). Dato che queste reti devono aggregare grandi quantità di dati che sono di più gestori che condividono il costo di esercizio della WAN e si dividono l’infrastruttura, essendo reti tipicamente pubbliche. Quindi parliamo di connettività nell’ordine delle centinaia di giga o di terabit (reti a grandissima capacità) perché devono aggregare tanti utenti insieme.

Global Internet: tutto il pianeta.

A seconda della tecnologia utilizzata cambiano le prestazioni e non solo; ad esempio la network on chip piccolissime distanze grandissime capacità. Oltre alla tecnologia che cambia a seconda della distanza, cambia anche la proprietà e la gestione ad esempio la LAN è gestita da chi la utilizza.

Lezione 07/03

Connectionless e Connection-oriented

Sopra a uno strato di commutazione si devono realizzare dei servizi di connettività, che sono fondamentalmente quello che gli utenti finali della rete si aspettano di usufruire. Tipicamente i servizi di connettività vengono erogati in due modalità: connection oriented e connectionless (NON SI DEVONO CONFONDERE con la com. di pacchetto e di circuito).

Quando si parla di connection oriented, indipendentemente da come funziona la rete sottostante, si offre all’utente uno strato di comunicazione che prevede il setup di un collegamento stabile fra A e B. Questa connessione ci garantisce l’inoltro certo dei pacchetti, l’arrivo dei pacchetti, che arrivino nell’ordine giusto e che siano eliminati i duplicati. Parliamo di un servizio di trasporto che realizza questo canale virtualmente perfetto. Si garantisce un canale sicuro anche se sotto vi è la com. di pacchetto attraverso dei protocolli più sofisticati che per esempio gestiscono meccanismi di ritrasmissione, controllano l’ordine di sequenza. Un servizio del genere serve con reti meno affidabili, che percorrono distanze maggiori.

Operare in modalità Connectionless significa che non c’è la necessità di fare il setup della connessione iniziale e il segnale di conclusione alla fine, non è importante se l’info mandata venga perduta, ma è importante mandarla in maniera efficiente. È un servizio estremamente efficiente, leggero (non fa controlli rispetto al c.o.) e non ci si preoccupa dell’affidabilità. Il problema significativo è che manca qualsiasi controllo degli errori quindi se una cosa la si invia e non arriva non ce ne si può rendere conto.

Questo può essere una fregatura per esempio quando si cerca attraverso un indirizzo simbolico e non si ottiene la risposta ossia non si ottiene l’indirizzo reale; per ovviare questa cosa si ripropone la query (solitamente sono rari questi problemi quindi i vantaggi di c.l. sono superiori agli svantaggi). Non è in grado di governare la velocità del trasmettitore rispetto al ricevitore e viceversa, cioè non ha meccanismi per controllare il controllo di flusso.

Internet diverso da internetwork: Internet è un internetwork a copertura globale e si indica con la I maiuscola, mentre internetwork è una connessione di reti locali attraverso reti geografiche o metropolitane (combinazioni di reti per mettere in comunicazione infrastrutture complesse). Visto che è una combinazione di reti i dispositivi che fanno la commutazione devo fare anche da mediatore tra protocolli differenti, quando mediano si dice che assumono la funzione di gateway.

Una sottorete(subnet) è quando una rete è un sottoinsieme di una rete più grande.

Partizioni di un progetto di rete

Un progetto di rete si può vedere partizionato a più livelli, partendo dal livello più basso dove troviamo i mezzi trasmissivi fino ad arrivare ai livelli più alti e vicino all’utente dove troviamo l’applicazione. Questo modello è strutturato a pila, è universalmente riconosciuto ed è stato fatto da un organismo di standardizzazione di diritto; questo modello si chiama “modello di interconnessione di sistemi aperti” (open systems interconection). In questa pila ogni livello vede le cose a un certo grado di astrazione, dando per scontato funzioni che vengono offerte dai livelli inferiori; ogni livello implementa una serie di funzioni.

Ogni host(dispositivo che opera in rete) avrà la pila completa. Tra due macchine l’unico colloquio avviene al livello più basso, ma in realtà ogni livello parla con il suo livello omologo.

Ci sono due modelli uno più didattico e uno che corrisponde alla realtà. Quello didattico è il modello ISO-OSI che ha 7 livelli raggruppati in due sottoinsieme di livelli: quelli più bassi che si chiamano Data flow e quelli più alti che si chiamano processo. I livelli più bassi offrono funzionalità proprie della rete, infrastrutturali mentre quelli più alti offrono funzionalità all’utente che deve usare la rete.

* Livello fisico: si spostano i bit sul dispositivo analogico che li fa trasmettere (un cavo elettrico, una fibra ottica); si specifica come mandare l’informazione, voltaggi, intensità di corrente, come sono fatte le interfacce. (half/full- duplex, simplex)
* Livello datalink: si organizzano i bit in strutture (treni o frame ) in maniera tale da gestire ad esempio tutta una serie di problematiche che servono a governare l’accesso al mezzo. In questo livello si inizia ad avere un canale che è in grado di mandare avanti insiemi di bit strutturati in modo particolare. MAC- address visibilià solo per quel data-link. Un data-link ha una struttura piatta cioè non ci sono nodi di commutazioni intermedi se metto in comunicazione tanti data link differenti, tanti canali e mezzi trasmissivi differenti con caratteristiche differenti allora vado a livello di rete. Trasformazione della linea grezza in una linea strutturata.
* Livello di rete: lavorano a com. di pacchetto, di circuito , indirizzamento universale e instradamento. Rende i livelli superiori indipendenti dai meccanismi e dalle tecnologie di trasmissione usate per la connessione e prendersi carico della consegna a destinazione dei pacchetti. È responsabile di:

-routing: scelta ottimale del percorso di rete da utilizzare per garantire la consegna delle informazioni dal mittente al destinatario, scelta svolta dal [router](https://it.wikipedia.org/wiki/Router) attraverso dei particolari [algoritmi di Routing](https://it.wikipedia.org/wiki/Protocolli_di_routing)

-conversione dei dati nel passaggio fra una rete ed un'altra con diverse caratteristiche, come il protocollo di rete utilizzato.

* Livello di trasporto: come deve essere garantito il trasporto delle informazioni; potrei avere un servizio connection oriented che individua specifici protocolli oppure un servizio connection less. È il primo livello realmente end-to-end, cioè da host sorgente a destinatario. Si occupa di stabilire, mantenere e terminare una connessione garantendo il corretto e ottimale funzionamento della sottorete di comunicazione. Controlla la congestione.
* Livello di sessione: deve far dialogare la componente utente con i servizi di rete offerti dal sistema operativo. Interfaccia i livelli superiori con i livelli più propriamente della rete.
* Livello di presentazione: trasforma i dati forniti dalle applicazioni in un formato standardizzato e offrire servizi di comunicazione comuni, come la [crittografia](https://it.wikipedia.org/wiki/Crittografia), la [compressione](https://it.wikipedia.org/wiki/Compressione_dati) del testo e la riformattazione.
* Livello di applicazione : si trovano servizi di tipo applicativo ad esempio il DNS, la posta elettronica, la navigazione sul web. Si definiscono i protocolli con cui l’utente si interfaccia con la rete attraverso questi strumenti il browser, la specifica app che fa una specifica cosa.

A ciascuno di questi livelli si ha bisogno di implementare specifici protocolli che permettano riscendendo e poi risalendo di stabilire una comunicazione end to end e ciascun livello ha la necessità di inserire, in una testata, delle informazioni di controllo che sono proprie del livello stesso. Quindi dai livelli superiori fino al livello fisico ogni livello inserisce delle info nella testata (incapsulamento) ; nel caso del datalink si inserisce sia una testa che una coda FCS (frame cecking sequens ) che è uno spazio dove vi sono dei codici di controllo che verificano se quello ricevuto è effettivamente coerente con quello trasmesso, se l’info non è integra deve essere scartata. Una volta arrivati al livello fisico si passa dall’altro lato al corrispondete livello fisico e qui si estraggono e utilizzano, a ritroso, le informazioni relative al controllo per ogni livello (deincapsulamento).

Nella realtà si fa riferimento a un modello diverso, più semplificato, ARPANET reference model(modello TCP); nei livelli di data flow non cambia nulla : c’è il livello fisico, link/network interface, rete/Internet e trasporto; gli ultimi tre livelli vengono compattati e fatti convergere in un livello solo che si chiama processo/applicazione. Questo modello elimina tutto ciò che è inutile, ad esempio la divisione tra sessione, presentazione e applicazione.

Livello fisico

In questo livello troviamo dei dispositivi fisici analogici che devo far passare informazioni numeriche in formato digitale facendo variare una grandezza analogica in ragione di qualche meccanismo, cioè si deve gestire un segnale che viene trasmesso e far variare quest’ultimo in maniera tale da poter andare ad interpretarlo come sequenza di bit. Un segnale è la variazione di una grandezza nel tempo. Si va a leggere come la grandezza varia nel tempo a specifici intervalli facendo delle misure; si fa il campionamento: si va ad osservare quella grandezza analogica e prenderne un campione a specifici istanti di tempo, attraverso queste letture si tira fuori l’informazione che poi attraverso traduzioni diventerà l’info digitale.

Serie di fourier

Sono trasformazione matematiche che permettono di scomporre il segnale in cosiddette armoniche, ossia onde di diverse frequenze e di studiarle nel dominio della frequenza (spettro). Ciò è importante perché i mezzi trasmessivi lasciano attraversare solo alcune frequenze e quindi quali e quanti armoniche attraversano il canale, in modo da poter campionare al meglio il segnale ed avere una migliore trasmissione (campionare il segnale= leggere il segnale ad intervalli di tempo). Sfrutto il mezzo trasmissivo alla massima velocità che mi consente.

Segnale, mezzo trasmissivo, Nyquist

Un segnale, che è considerabile come una funzione periodica, lo si può scomporre in un’infinita somma di seni e coseni con delle ampiezze specifiche e le frequenze di queste componenti sono tutte multiple intere di una frequenza fondamentale. Il mezzo trasmissivo va a perturbare il segnale cioè certe componenti in frequenza di questo segnale passeranno altre potrebbero non passare. Per capire come si comporterà realmente un segnale si deve andare a studiare la sua forma spettrale (la sua proiezione nel dominio della frequenza). Il segnale parte con delle sue caratteristiche in frequenza e in ragione della velocità di trasmissione ha un comportamento diverso nel dominio della frequenza quindi la sua visione spettrale si comporta diversamente. Quando questo segnale si andrà a iniettare nel mezzo trasmissivo, quest’ultimo attenua ma non uniformemente cioè l’energia man mano che il segnale viaggia diminuisce. Il problema è che il mezzo trasmissivo non li attenua nello stesso modo quindi mi distorce il segnale, ovvero il segnale che arriva non è quello atteso.

Il mezzo trasmissivo si comporta come un filtro passa banda, cioè guardando le caratteristiche spettrali si scopre che c’è un blocco di frequenze che passano lisce al di fuori di questo blocco c’è un’attenuazione prima progressiva e poi drastica. Quindi ogni mezzo trasmissivo è caratterizzato da un range di frequenze particolari che si chiama “banda passante”. Se si trasmette a frequenze comprese nel range del mezzo trasmissivo quello trasmesso sarà quello che si riceverà; se si aumenta la frequenza si riduce il periodo che mi dura la trasmissione di un bit (si va più veloce).

Quindi si dovranno adeguare la velocità di trasmissione alle capacità del mezzo e adeguare il tempo di campionamento alla velocità di trasmissione e quindi alle caratteristiche del mezzo trasmissivo.

Criterio di Nyquist: se la larghezza di banda del segnale è B allora è certo che sia in grado di ricostruire il segnale se si campiona al doppio della larghezza di banda. Si può campionare per un valore leggermente maggiore a 2B (bande di guardia) per garantire che un comportamento anomalo del mezzo trasmissivo non faccia perdere qualche componente.

Il rumore

Il rumore è una forma di energia indesiderata che si somma al segnale e si degrada il contenuto informativo impedendo di rilevare le info trasmesse.

Esistono vari tipi di rumore:

* Rumore bianco: il cui spettro comprende energia a tutte le frequenze ed equamente distribuito.
* Rumore di intermodulazione: prodotti dalla non linearità dei dispositivi;
* Rumore di modo comune: che influisce in maniera disuniforme sulle varie componenti di frequenza e aree un effetto assolutamente indesiderato.
* Rumore di quantizzazione: perdita di info che ha luogo durante la trasformazione di un segnale da analogico a digitale.
* Rumore termico: dovuto all’agitazione termica degli elettroni presenti in una resistenza.

Legge di Shannon

Estensione del lavoro di Nyquist sui canali soggetti a rumore casuale(termico).

Sia S la potenza del segnale e N la potenza del rumore, la massima info trasmessa è:

C[bit/s] = log in base 2 (1+ S/N).

In questa formula C è detta capacità del canale (bit/sec) ed indica la massima velocità teorica di trasmissione dei bit entro la quale non vengono confusi con il rumore.

Trasmissione dei segnali

La trasmissione dei segnali è detta analogica se il segnale viene trasmesso senza curarsi del suo significato. La trasmissione si limita a recapitare il segnale, amplificando quando necessario. La trasmissione si dice digitale quando tiene conto del contenuto dei dati trasmessi: il segnale non viene semplicemente amplificato, ma viene interpretato e rigenerato tramite apparati detti ripetitori. Ciò può avvenire a prescindere del tipo di segnale o dato.

Trasmissione in banda base e modulata

Una volta generato il segnale da trasmettere, questo può essere immesso direttamente sul canale; in questo caso si parla di trasmissione in banda base: il segnale che trasposta le info ed il segnale sulla linea sono identici vi sono, però, circostanze che rendono opportuno trasmettere il segnale in modo che occupi una banda differente di frequenza; ciò avviene tramite un processo di modulazione.

Codifica dei dati numerici

La rappresentazione di dati numerici con segnali numerici è normalmente fatta tramite sequenza di impulsi discreti. Il dato binario è codificato in modo da far corrispondere al valore di un bit un determinato livello del segnale. Il ricevitore deve sapere quando inizia e finisce il bit, leggere il valore del segnale al momento giusto, determinare il valore del bit in base alla codifica utilizzata. La migliore valutazione si ottiene campionando il segnale al tempo corrispondente a metà bit.

Caratteristiche delle codifiche

* Spettro del segnale: componenti ad alta frequenza richiedono banda maggiore; l’assenza di componenti contigue è preferibile; spettro concentrato nel centro della banda.
* Sincronizzazione temporale: ricevitore e trasmettitore devono essere sincronizzati.
* Rilevazione di errore: solidarietà del segnale rispetto ad interferenza (energia causata da un fattore esterno) o rumore.

Costo e complessità di realizzo.

Codifica unipolare RZ e NRZ

RZ (return to zero): 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. NRZ(not return to zero): differisce dalla RZ poiché il livello di tensione per il bit 1 rimane alto per tutta la durata del bit. Pregi della codifica NRZ: facile da realizzare; utilizzo efficiente della larghezza di banda. Difetti della codifica NRZ: esiste una componente continua; il ricevitore può perdere la sincronia, poiché sequenza di bit uguali producono un segnale continuo senza transizioni.

Codifica NRZ-L e NRZI

NRZ-L (not return to zero level) -> prevede un segnale a +V il bit 1 ed a –V per il bit 0. Ciò riduce l’impatto della componente contigua, ma non l’annulla (ho sincronizzazione).

NRZI(NRZ invert on ones) -> codifica differenziale in cui il segnale cambia in occasione di un bit 1.

Codifica multilivello binario

Le codifiche multilivello binario utilizzano tre livelli: lo zero indica il bit 0 mentre il bit 1 è identificato con segnali a +V e –V alternati. (si basa sulla AMI bipolare: Alternate Mark Inversion). La codifica pseudoternaria è la stessa con 1 e 0 invertiti. Risolve il problema della sequenza di bit 1, che presentano sempre una transizione utilizzabile in ricezione per sincronizzare (ma resta il problema per sequenze di 0); la componente continua è di fatto azzerata; utilizza a parità di transmission rate una larghezza di banda inferiore.

Codifica manchester

Utilizza due livelli di tensione; il bit 1 è rappresentato da un segnale -V per mezzo periodo, +V per il seguente mezzo periodo; il bit 0 è rappresentato in modo opposto (+V per il primo mezzo periodo, -V per il restante mezzo periodo). Quindi essendoci sempre una variazione nel centro, non ho più continuità di 0 o 1.

Vantaggi :

* Sincronizzazione, per via della transizione di mezzo che può essere usata per la sincronizzazione del ricevitore;
* Totale assenza di componente continua;
* Rilevazione di errore (in assenza della transizione prevista).

Svantaggi: ridividere un segnale a frequenza doppia rispetto al bit poiché il segnale cambia continuamente ad intervalli di tempo.

La codifica Manchester differenziale utilizza lo stesso tipo di rappresentazione, ma il bit 1 è inteso come variazione rispetto alla codifica del bit precedente.

Codifica B8ZS

Una modifica della AMI per risolvere il problema della sequenza di zeri è la B8ZS( Bipolar with 8 zero substitution):

* Ogni sequenza di 8 zeri viene codificata come: 000+-0-+ se l’ultimo impulso è stato positivo; 000-+0+- se l’ultimo impulso è stato negativo .

In questo modo scompaiono lunghe sequenze di zeri e la sequenza è identificata da due violazioni del codice AMI.

Codifica HDB3

Stessa logica per la HDB3 (High Density Bipolar 3 zeros):

* Ogni sequenza di 4 zeri vince codificata come:

se la polarità dell’impulso è stata negativa:

000 - Se c’è stato un numero dispari di 1 dall’ultima sostituzione;

+ 00+ se c’è stato un numero pari di 1 dall’ultima sostituzione.

Se la polarità dall’ultimo impulso è stata positiva:

0 0 0 + per un numero dispari di 1 dall’ultima sostituzione;

-00- per un numero pari di 1 dall’ultima sostituzione.

Anche in questo caso scompaiono lunghe sequenze di zeri e la sequenza è identificata da violazioni opportuna del codice AMI.

Modulazione

È un processo con il quale il segnale da trasmettere (segnale modulante) viene utilizzato per modificare nel tempo le caratteristiche di un segnale ausiliario sinusoidale (portante). Questa operazione ha la caratteristica di generare un segnale che ha una occupazione di banda dell’ordine di grandezza di quella del segnale modulante, centrata però intorno alla frequenza del segnale portante

Vantaggi: multiplazione -> sullo stesso mezzo più segnali insieme.

Tecniche di modulazione

Possiamo far variare il segnale modulato secondo quello modulante:

-Ampiezza: il modulante modifica l’ampiezza del modulato (facendolo salire o scendere).

-Frequenza: il modulante modifica la frequenza del modulo (far variare un segnale periodico, far variare l’intensità di un fischio).

-Fase: il modulante cambia la fase del modulato.

ASK (Amplitude Shitf Keying) -> dato un segnale modulante, se varia l’ampiezza di esso (da 0 a 1), varia anche l’ampiezza del segnale modulato.

FSK (frequency shift keying )-> serve a modulare in frequenza un segnale modulato in funzione del segnale modulate, facendo corrispondere due frequenze ai due valori del bit.

PSK (Phase shift keying)-> il segnale numerico può modulare in fase il segnale modulato associandolo un certo valore di fase ad un certo valore di bit.

BPSK-> è la modulazione PSK bifase si ha un solo segnale modulato e quindi i due valori numerici 0 e 1 sono fatti corrispondere a due fasi diverse della stessa frequenza : 0° e 180° .

QPSK (Quadratore PSK) -> si utilizzano 4 angoli di fase per trasmettere due bit per simbolo.

QAM (Quadratore Amplitude Modulation)-> rappresenta una combinazione in fase e in ampiezza contemporaneamente .

Tecniche di multiplazione

* A divisione di tempo (TDM)-> ognuno ha a disposizione una parte del mezzo per un certo tempo. Modalità deterministica (banda dedicata e ritardo fisso) e statistica (devo chiedere a chi tocca).
* A divisione di spazio (SDM)-> dati inviati su mezzi trasmissivi fisicamente separati.
* A divisione di frequenza (FDM e WDM)-> usa differenti frequenze o lunghezze d’onda per differenziare i dati trasmessi. Ogni segnale si prende una sezione specifica dello spettro senza dar fastidio agli altri.
* Per codifica(CDM)-> si parla tutti insieme, confusionale, ma ognuno si sintonizza con chi comunica con la propria codifica.

SDM -> una connessione fisica per la trasmissione

TDM-> stessa connessione utilizzata per 4 trasmissioni distinte. Richiede tramatura dei flussi e uso di multiplexer e demultiplexer ed è meno efficiente, ma ottimizza i mezzi trasmissivi.

(Time division multiplexing) è utilizzato per trasmettere contemporaneamente un insieme di comunicazioni. Ogni segnale rispetta il suo turno, ovvero interviene quando gli tocca (periodi temporali). Pian piano si fondono i segnali dagli utenti che vogliono trasmettere simultaneamente.

SLOT e FRAME

Ogni intervallo di tempo si chiama slot e può ottenere uno o più bit relativi ad un flusso indipendente. Il flusso dei dati è organizzato in trame (frame). Una trama è l’insieme di slot temporali che contiene almeno un bit per ciascuna trasmissione. Il flusso relativo ad una singola trasmissione è detto canale.

TDM DETERMINISTICO E STATISTICO

Esistono essenzialmente due metodi di multiplazione:

deterministico-> ogni canale di comunicazione è identificato dalla sua posizione in termini di slot temporali all’interno della trama. Ciò è uno svantaggio poiché, se il canale non è usato, occupa comunque il timeslot inviando un pattern idle. Non è necessaria la bufferizzazione poiché ogni frame ha la stessa lunghezza.

Statistico->non esiste correlazione fra canale di comunicazione e relativo slot. La capacità del mezzo è distribuita statisticamente fra gli utenti che ne concorrono all’uso. Ogni frame ha taglia differente dall’altro, sono quindi necessari indirizzamento e bufferizzazione. Vi è un meccanismo di arbitraggio.

FREQUENCY DIVISION MULTIPLEXING (FDM)

Ogni segnale avrà una sua frequenza e una parte di spettro, quindi non vengono mischiati i dati, poiché i segnali sono totalmente separati (nessuna interferenza).

ORTOGONAL FREQUENCY DIVISION MULTIPLEXING(OFDM)

È un FDM però con una divisione ortogonale facendo dunque in modo che al livello massimo di una portante le altre si azzerino. Quindi permettendo che due portanti si scontrino e si intreccino su alcune frequenze. Trasporto più informazioni nello spazio di frequenza, si va molto più veloce. Come si progettano portanti ortogonali tra loro? Con la trasformata di Fourier.

CODE DIVISION MULTIPLEXING (CDM)

Prendo un simbolo da trasmettere, lo moltiplico per una frequenza, questa è la lingua che conosco, però le frequenze di clipping sono progettate per essere ortogonali tra loro. Succede che se trasmettono tutti simultaneamente, dall’altro lato ricevo un segnale che è la composizione, la somma di tutto; se si moltiplica la somma per la frequenza di clipping, riuscirò ad estrarre il bit singolo che è quello che ha mandato. (si possono trasmettere più info diverse).

MEZZI TRASMISSIVI

Sono classificati in due grandi famiglie:

1)Mezzi guidati: elettrici, ottici (linee o cavi);

2) Mezzi non guidati: onde radio, laser(wireless).

Ogni mezzo è caratterizzato da:

-larghezza di banda -> capacità del mezzo;

-Delay-> ritardo: il segnale impiega tempo per passare da un estremo all’altro;

-costo-> un mezzo trasmissivo viene scelto in base al costo;

-facilità di installazione e manutenzione -> quanto il mezzo e gestibile e governabile.

I mezzi trasmissivi elettrici permettono di far passare segnali elettromagnetici. Il segnale si propaga attraverso un mezzo conduttore come un fascio diretto che viaggia da un estremo all’altro. Ci sono dei compromessi di realizzazione. L’energia che si manda da un lato all’altro ovviamente viene persa a causa del fenomeno della resistenza del mezzo, viene persa per fenomeni di errore che sono sul mezzo. Quindi il mezzo trasmissivo elettrico non è ottimale.

Distorsione -> perdita di potenza: il segnale arriva dall’altro lato con termini di potenza inferiori. Quando si tramette su un mezzo trasmissivo in rame parte dell’energia trasmessa viene irradiata nello spazio circostante.

INTERFERENZA E SCHERMATURA

EMI -> interferenza elettromagnetica. Trasformazioni tra cavi generano interferenza. Quando i cavi viaggiano insieme non possono essere vicini, a meno di utilizzare opportuni accorgimenti. Ciò può essere ridotto tramite una schermata; ovvero una tecnica che prevede la protezione elettrica del mezzo in modo da poter abbattere l’effetto dell’interferenza.

Schermata a foglio -> si può circondare il filo di rame con un isolante plastico che lo protegge e intorno mettere uno schermo di alluminio.

Scherma a calza -> treccia di fili di rame che avvolgono il cavo in due direzioni opposte. Il tipico mezzo trasmissivo in rame è un cavo che viaggia da un lato all’altro, ma non da solo. Si ha bisogno di far viaggiare i segnali su più mezzi trasmessivi paralleli e indipendenti tra di loro. Il più comune utilizzato nelle reti locali è il doppino.

Il doppino è il mezzo trasmissivo classico della telefonia e consiste in due fili di rame ricoperti da una guaina isolante e ritorti detti “coppia” ( pinati). Questi fili non viaggiano insieme parallelamente, ma sono intrecciati a coppie per evitare la diafonia, cioè un accoppiamento elettrico tra mezzi trasmissivi non isolati.

Esistono varie versioni di doppino:

-STP(shielded twisted Pair) : versione con uno schermo per ogni coppia più uno schermo globale (calza in rame);

-FTP(Failed Twisted Pair): versione con un unico schermo;

-UTP(Unshielded twisted Pair): versione non schermata.

I parametri elettrici di qualsiasi cavo variano con la frequenza. Occorre chiedersi, per una data applicazione, a quale frequenza sia opportuno operare per decidere se un cavo sia adatto all’applicazione stessa. Per questo è stata creata una classificazione di 7 categorie differenziate in termini di schermatura e di capacità di banda passante.

Il cavo coassiale tipicamente ha un portante trasmissivo in rame, ha un’anima centrale in rame, una superfice isolante e una schermatura fatta in alluminio o rame. Questo cavo ha qualità trasmissive molto superiori al doppino, però è più costoso, più pesante e più difficile da installare. Tipicamente si usa solo per le antenne.

Cavo coassiale a banda passante-> mezzo trasmissivo che consiste in un filo di rame rigido circondato da una garza metallica che funge da schermo;

Cavo coassiale a larga banda -> consiste in un cavo identico a quello in banda base, ma con un sistema di trasmissione diverso. Infatti quest’ultima avviene in analogico, cioè in modo del tutto simile alla trasmissione televisiva.

Trasmissione power line -> è una tecnologia usata per la trasmissione dati che utilizza la rete di dimensione elettrica come mezzo trasmissivo, dunque sfrutta il doppino che fa da cavo elettrico per inviare i dati tramite modulazione.

POE (power over ethernet) -> utilizza la rete dati (doppino) per portare la corrente elettrica.

Il passaggio da un conduttore all’altro, oltre a causare una perdita devastante di segnale, fa verificare un fenomeno: la riflessione , quindi c’è molto rumore.

FIBRE OTTICHE

Consistono in un cavo composto da un anima trasparente(core) di silicio (materiale vetroso, capace di condurre fasci di luce, cioè onde), avvolto in un rivestimento in silicoide, specie di vetro (mantello) in grado di condurre luce, però deve essere obbligatoriamente caratterizzato da una densità differente da quello del core, intorno a tutto questo c’è una schermatura protettiva, isolante dal punto di vista della luce, può essere sia di materiale elettrico sia in acciaio corrugato. Nello stesso cavo fisico ci si fanno viaggiare più fibre ottiche separate. Non permette più l’invio dei dati tramite elettricità ma lo fa tramite segnali luminosi, in modo da non soffrire di interferenza elettromagnetica. È anche molto veloce ed efficiente poiché gode di una grossa banda, ma soprattutto evita intrusioni. Se trasmetto dati riservati, in un cavo in rame, possono leggere quei dati senza che gli altri cavi se ne accorgono, senza interromperlo; nella fibra non è possibile perché si dovrebbe tagliare e inserirsi e questa cosa naturalmente si vede con delle tecniche che si chiamano riflettometriche (misura della riflessione). Gli svantaggi sono che la connettorizzazione e interfacciamento si fanno con apparati molto costosi, ci sono dei fenomeni di dispersione ed è oggetta di effetti non lineari quindi il rumore che caratterizza la fibra a volte non è completamente prevedibile .

Dietro la fibra ci sono le equazioni di Maxwell che permettono di stabilire come l’energia, all’interno di questa guida, si propaga in un numero discreto di configurazioni, cioè sulla stessa fibra si possono avere più vettori di propagazione dell’energia (modi di propagazione).

La fibra si basa sul fenomeno della rifrazione

RIFRAZIONE

È il fenomeno per cui un raggio luminoso (non perpendicolare alla superficie di contatto, ma incidente e quindi fa un angolo di incidenza) passando da un mezzo trasparente all’altro, anch’esso trasparente, cambia direzione sul punto in cui attraversa la superficie di separazione dei due mezzi. La legge di Snell studia la riflessione e la rifrazione di un raggio luminoso che incide sulle superfici di separazione. Questa legge dice che, scegliendo opportunamente l’angolo di incidenza, posso minimizzare la riflessione: si può controllare la quantità di energia che torna indietro e si riesce a far andare avanti il più possibile la quantità di energia utile che si chiama energia rifratta e quindi il segnale andrà avanti nel mezzo con continui passi di rifrazione. Non si deve mai superare l’angolo critico di incidenza perché superato questo angolo si ha una riflessione totale e quindi il segnale non va avanti. Si ha un certo range di tolleranza (cono d’accettazione) nello scegliere l’angolo di incidenza e se quest’ultimo è mantenuto in questo cono di tolleranza non si avrà il ritorno indietro del segnale, anzi entrerà nel core, rimbalzerà sul mantello e così via. Se vi è un cono di accettazione abbastanza ampio si possono mandare anche più segnali contemporaneamente.

Sulla base dell’apertura numerica della fibra si possono far viaggiare più modi simultaneamente facendo meno strada (fibra multimodale) o si può far passare solo un modo, ma va molto lontano (fibra monomodale).

TIPI DI FIBRA

La trasmissione all’interno dell’anima di vetro può avvenire con modalità diverse:

Fibra multimodale-> fibra il cui interno (cono d’accettazione) è abbastanza ampio da permettere diversi angoli di rimbalzo della luce trasmessa;

Fibra monomodale-> fibra il cui nucleo permette il passaggio di poche lunghezze d’onda. Questo fa comportare la fibra come una semplice guida d’onda.

Da cosa dipende se posso trasmettere un modo o più di un modo?

Dalle caratteristiche della fibra, ovvero dal rapporto tra core e cladding. Quando il rapporto tra essi è più ampio, significa che il core è un po’ più del doppio, a parità di cludding, tipicamente il cono di accettazione è più ampio, quindi la trasmissione è più precisa e posso far viaggiare più modi.

MODI DI PROPAGAZIONE

Indicano come il segnale viene rifratto sulla superficie tra il core e il cladding. Questo dipende dal passaggio da un materiale all’altro che hanno indici diversi di rifrazione.

Questo passaggio può essere violento, impulsivo (step-index) o più tranquillo ed attenuato (graded-index). La fibra ottica monomodale si comporta come una guida d’onda con una sola modalità di propagazione rettilinea.

Dispersione modale-> ogni volta che il segnale viene rifratto parte dell’energia viene dispersa.

LUNGHEZZA D’ONDA

Spettro elettromagnetico-> insieme di frequenza che descrivono le caratteristiche di un mezzo trasmissivo. Un range particolare dello spettro è lo spettro del visibile, ovvero il range in cui il nostro occhio è in grado di percepire i colori, un particolare effetto della riflessione. Per lo spettro visibile parliamo di lunghezza d’onda, ovvero la distanza tra due creste di un segnale. Esempio: onde del mare, se andiamo a misurare la distanza tra le due creste d’onda, sarà diversa.

FINESTRA OPERATIVA

Trasmettono mandando un segnale a specifiche frequenze dello spettro del visibile, quindi a specifiche lunghezze d’onda. Studiando il fenomeno dell’attivazione sulla fibra ottica, ovvero la proprietà che caratterizza la dispersione di un raggio luminoso che propagandosi nella fibra si perde e viene assorbito o riflesso dal materiale della fibra, in ragione della lunghezza d’onda a cui trasmettiamo, si può trasmettere in diversi range, più o meno range del visibile. Dobbiamo rendere minima l’attenuazione.

1° finestra -> 800/900nm

2° finestra-> 1250/1350 nm

3° finestra-> 1500/1600nm

Se trasmettiamo in 3° finestra, otteniamo che il segnale si attenua il meno possibile, percorre più strada e andrà più lontano. Ciò, però è oneroso.

TIPI DI FIBRE

Le fibre più utilizzate sono:

* Fibra standard ITU-T G.652 (ottimizzata per l’uso in 2° finestra);
* Fibra standard ITU-T G653 (ottimizzata per l’uso in 3° finestra);
* Fibra a disposizione non nulla ITU-T G.655(ottimizzata per l’uso in 3° finestra)

Quando progettiamo un impianto dobbiamo scegliere il giusto tipo di fibra per poter trasmettere in base agli apparati che scegliamo e in base alle frequenze che scegliamo.

WAVELENGHT DIVISION MULTIPLEXING (WDM)

È una variante della multiplazione a divisione di frequenza, infatti può anche chiamarsi multiplazione a divisione di lunghezza d’onda. WDM ci permette di far viaggiare un segnale su una lunghezza d’onda (colore) che non interferisce con le altre, quindi che viaggiano parallelamente lungo il cavo. In questo modo riesco ad aumentare drasticamente l’utilizzo del cavo (oggi fino a 320 lunghezza d’onda sul singolo cavo).

La WDM si può dividere in due famiglie:

Course Wavelenght Division Multiplexing (CVDM)-> la distanza fra le lunghezze d’onda è maggiore, quindi posso trasmettere meno lunghezze d’onda.

Density Wavelenght Division Multiplexing (DVDM) -> la distanza fra le lunghezze d’onda è minore, quindi posso trasmettere più lunghezze d’onda.

Inoltre, vi è la Elastic Wavelenght Division Multiplexing (EVDM) -> utilizzo una sottoportante a seconda della lunghezza d’onda.

COMPONENTI DELL’ARCHITETTURA WDM

Vi sono dei dispositivi chiamati trasponder che precedono il segnale numerico e lo traslocano su una specifica lunghezza d’onda. Il MUX (Multiplexer ) mette insieme tutti i trasponder. A questo punto le lunghezze d’onda, che viaggiano sullo stesso portante fisico, vanno in avanti dove incontrano gli amplificatori che servono a rendere il segnale più potente a discapito della sua precisione, ovvero introducendo rumore. Dall’altro lato si ha il DEMUX( De- Multiplexer) che ha dei filtri a cavità, i quali estraggono i segnali. Infine, ha altri trasponder che trasformano tutti questi segnali nei segnali digitali che vi interessano.

TRASMISSIONE SULLA FIBRA

La trasmissione attraverso la fibra ottica può essere effettuata con due modalità diverse:

-con led sulle fibre multimodali;

-con laser sulle fibre monomodale;

Il led percorre distanze minori, ma costa poco. Il laser, al contrario, percorre distanze maggiori, ma ha un costo superiore. Inoltre, vi sono i Vcsel: laser a semiconduttore, che hanno un sistema ottica il quale permette l’emissione del fascio. Laser perpendicolare alla superficie di crescita dei semiconduttori. Il più preciso è il laser.

PARADOSSO DI TANENBAUM

“Mai trascurare larghezza di banda di un furgoncino che viaggia tra una sede e l’altra”

Questo paradosso è stato sfatato dalla fibra. Questa può trasportare 4000 Gbyte/sec. Il furgoncino può trasportare 8 Pbite. Ciò vuol dire che per distanze brevi vince il furgoncino, ma per distanze che superano i 2000 sec vince la fibra.

MEZZI DI TRASMISSIONE WIRELESS

Passiamo da mezzi guidati a non guidati. Esistono varie tecnologie wireless, ma le differenzia la sezione di spettro che scegliamo. Il segnale, però, è fortemente vulnerabile (interferenza, riflessione).

Aria-> è un buon mezzo di trasmissione, in particolare per onde elettromagnetiche.

Ogni trasmissione via etere utilizza due stazioni (trasmittente e ricevente). Per indicare c’è bisogno di una antenna trasmittente che è collegata direttamente al trasmettitore e su questa può essere mandata un segnale. Il ricevitore, attraverso un’antenna ricevente capterà queste onde, le isolerà dal resto percepito che potrà essere ad esempio un altoparlante.

SISTEMA DI ANTENNA

Elemento irradiante o ricevente-> è l’antenna vera e propria che realizza la trasduzione

Feeder di antenna-> è il mezzo trasmissivo utilizzato per collegare il trasmettitore o il ricevitore con l’antenna.

Dispositivi di diramazione o circolatore -> consente di separare la trasmissione della ricezione.

LE ONDE ELETTROMAGNETICHE

Le onde elettromagnetiche si propagano nel vuoto alla velocità di circa C = 300000 km.sec (velocità della luce). Le onde elettromagnetiche sono costituite da oscillazioni del campo elettrico e del campo magnetico.

SPETTRO ELETTROMAGNETICO

Le sezioni dello spettro che vengono trasmesse in mega Hze giga Hze sono principalmente quelle che comprendono radio, microwave ed infrared.

Se viaggiamo a frequenze più basse possiamo far viaggiare pochi bit (riducendo la frequenza, riduco la velocità di trasmissione), poiché lavoriamo a frequenze più ridotte.

ASSEGNAZIONE FREQUENZE

Le frequenze sono assegnate da enti nazionali/internazionali (ITU e FCC) e poi vengono delegate ad altri enti (in Italia è competenza del ministero Poste e Telecomunicazioni). Ciò non succede se abbiamo scelto bande non regolamentate (wireless), ma nessuno ci dà garanzie sulla frequenza.

TIPOLOGIE DI TRASMISSIONE RADIO

Direct Sequence Spread Spectium (DSSS) - > trasmissione radio a larga banda, si usa la combinazione di tecniche che multiplano a divisione di codifica su specifiche frequenze su cui si fanno delle multiplazioni (WI-FI segnali deboli).

Frequency Hopping Spread Spectium (FHSS)-> il trasmettitore opera continui “salti” del segnale da un canale all’altro, quindi devo conoscere la frequenza dei vari canali.

RADIO DIFFUSIONE

I canali radio vengono trasmessi generalmente in modalità broadcast, ovvero chiunque è in grado di leggere il segnale. Ovviamente la grandezza che viene trasmessa è analogica.

Utilizza due tecniche trasmissive in funzione della regione di frequenza:

-nella regione fino al MHZ, il segnale si propaga seguendo la curvatura terrestre ed attraversa bene gli ostacoli, percorrendo anche grandi distanze;

-nella regione del MHZ al GHZ, il segnale viene assorbito dalla superficie terreste e dagli ostacoli, ma viene riflesso molto bene dalla ionosfera, percorrendo distanze minori.

TRASMISSIONE VIA PONTE RADIO

Si basa su microonde. Utilizza antenne paraboliche di dimensioni maneggevole per poter collimare e dare direzione all’emissione. Per queste tipo di comunicazioni bisogna utilizzare un allineamento ottico delle antenne: trasmissione rettilinea ed è indispensabile la visibilità tra le antenne delle stazioni comunicanti (canale radio multi-hop). Per lunghe distanze devo quindi utilizzare trasmissioni a vista; inoltre, utilizzando stazioni ripetitrici, si riescono a coprire distanze elevate.

Le connessioni a breve distanza possono utilizzare frequenze più alte per le quali si hanno i vantaggi: antenna più piccola, fascio più collimato (quindi minore necessità di potenza), minori problemi di interferenza per lo scorso utilizzo di trasmissioni in quella regione di frequenza.

UTILIZZO PUNTI RADIO

Generalmente utilizzati per trasmissioni analogiche (fonia, televisione) o digitale (reti private o compagnie telefoniche fornitrici di servizi).

TRASMISSIONE RADIO-MICROONDE

Le onde si propagano in linea retta. Usando le antenne direzionali ad alto guadagno (paraboliche) si migliora il rapporto S/N.

BANDE NON LICENZIATE

Bande ISM assegnate ad utilizzo industriale-scientifico-medico, non richiedono licenza; quindi non c’è garanzia di non interferenza.

TRASMISSIONE RADIO-INFRAROSSI

Tecnica usata per trasmissioni a distanze limitate e non attraversano oggetti. La velocità è limitata è necessario un puntamento diretto. Interferenza limitata (in particolare la luce solare).

TRASMISSIONI LIGHTWAVE

È caratterizzata da grande larghezza di banda, non richiede licenza, posso lavorare esclusivamente a vista. Non è soggetta ad interferenza radio, ma ad interferenza causata da condizioni atmosferiche (umidità, pioggia, eccessi di calore). In generale abbiamo un laser ed un fotorilevatore che lavorano con un fascio fortemente concentrato. I due punti devono obbligatoriamente vedersi perfettamente. Il laser deve essere protetto da uno specchio, vetro.

TRASMISSIONI SATELLITARI

Il satellite si comporta come una stazione ripetitiva del segnale che, viene inviato dalla stazione terrestre al satellite (uplink), che lo rimanda verso la stazione o le stazioni riceventi (downlink) tipicamente il collegamento satellitare tende ad essere asimmetrico, ovvero la capacità di uplink è inferiore a quella di downlink. Sicuramente si utilizzano frequenze diverse. Un satellite opera su più bande di frequenza, con la tecnologia FDM; i singoli canali si chiamano trasponder. Su questi, il satellite può fare TDM per gestire diverse comunicazioni. Una parte del segnale passa dalla ionosfera, un’altra ritorna. Se salgo di frequenza, l’attenuazione dell’atmosfera diventa troppo grande se scendo ottengo l’effetto di riflessione. In frequenza alta vi è assorbimento attenuazione disturbo) in frequenza bassa vi è riflessione( il segnale viene riflessa).

SATELLITI

Tre categorie:

Geo (Geostationary Earth Orbit) -> satelliti a 36000 Km ruotano insieme alla terra e hanno una posizione fissa nel cielo. Non c’è bisogno di puntare i trasponder, poiché il puntamento delle antenne è fisso. Per motivi di interferenza la distanza tra satelliti è tanta (max 180 satelliti) e latenza del segnale.

Meo (Medium Earth Orbit) -> satelliti a 18000 km di quota. Non li vediamo sempre nella stessa posizione poiché si muovono. Non adatti alla trasmissione dati (Es. GPS).

Leo (Low Earth Orbit) -> satelliti tra 750e 1500km di quota. Si muovono velocemente intorno alla terra si mettono vicino a noi, quindi il ritardo di trasmissione tra noi ed il satellite è abbastanza basso e si richiede poca potenza di trasmissione. Sono utilizzate per copertura satellitare della telefonia.

SATELLITI PER LA COMUNICAZIONE

Dipendentemente dalla distanza, cambiano anche le modalità di trasmissione. Più lavoriamo in alto, più alziamo le frequenze; viceversa più lavoriamo in basso e più abbassiamo le frequenze. La trasmissione può essere influenzata da caratteristiche atmosferiche (pioggia, nuvole, umidità ecc.). In genere le bande più basse sono abbastanza immuni a questi fenomeni, ma sono molto affollate. Tipicamente un trasponder satellitare ha una certa apertura e vi sono delle antenne di terra con un cavo di accettazione che permette di ricevere il segnale (“hub” satellitare).

SATELLITI LOW- EARTH ORBIT IRIDIUM

Vi sono 77 satelliti che formano 6 collane intorno alla terra, ogni satelliti si aggancia a 4 vicini e realizzano 1628 celle mobili lungo tutta la superficie terrestre.

SATELLITI LOW-EARTH

Come comunicano tra loro?

Relaying in space->i satelliti si possano le info nello spazio tramite dei commutatori presenti in ogni satellite e dei switch satellitari.

Relaying on the ground -> i satelliti si passano le info su fibra ottica.

SATELLITE CONTRO FIBRA

Fibra- distanza: circa 3200km -> 10 millisecondi di latenza

Satellite-distanza: circa 71000 km -> 263millisecondi di latenza

Con la fibra si impiega meno tempo per questo non si sceglie il satellite.

LIVELLO DATA-LINK

-Il data link layer (DLL)

È un livello intermedio tra livello di rete ed il livello fisico. Mentre il livello fisico dà servizi e non riceve nulla, il data link prende i servizi e li manda allo strato superiore. Il compito del DDL è quindi quello di organizzare il trasferimento dei dati tra due apparati adiacenti, ovvero logicamente connessi da un “canale”, che trasmette i bit da una porta all’altra, nell’ordine di trasmissione.

Struttura dei dati-> i bit, che vengono trasmessi come segnali, vengono visti come grandezze digitali strutturate, poiché il livello fisico sottostante ha già permesso di mandare dei bit trasformandoli in segnali e ritrasformandoli in bit. Si passa da trasmissione analogica a digitale.

Dobbiamo quindi organizzare i bit in trame(frame), ovvero l’unità di trasmissione del DLL. Ad ogni frame si aggiunge un’intestazione ed una coda (header e trailer). In ricezione il DLL riceve i dati dallo strato fisico effettua i controlli necessari, elimina header e trailer, ricombina i frame e passa i dati ricevuti allo strato di rete.

SERVZI DEL DLL

I servizi forniti allo strato di rete sono:

-trasmissione dati senza riscontro e senza connessione;

-trasmissione dati affidabile senza connessione;

-trasmissione affidabile con connessione;

Per garantire un servizio non affidabile basta solo trasmettere le trame senza badare se arrivino o meno. Viceversa, se vogliamo un servizio affidabile, dobbiamo effettuare un controllo sulle trame e bisogna scartarle in presenza di errori. In questo caso devo avere un meccanismo di riscontro (ACK positivo o NACK negativo).

Se il riscontro risulta essere negativo vi è un fenomeno di ritrasmissione per rimandare la trama daccapo. Trasmettitore e ricevitore devono essere sincronizzati, per far capire dove inizia e finisce una trama. Infine, bisogna realizzare il controllo di flusso ovvero adeguare le velocità di trasmissione alla capacità del canale.

FRAMING (tramatura)

Fare “framing” significa utilizzare meccanismi offerti dal DLL per strutturare le trame. Ciò significa delimitare esse, per poter capire il suo inizio e la sua fine.

Esistono tecniche diverse per strutturare una trama:

-conteggio dei caratteri;

-byte di flag e byte stuffing;

-bit(s) di flag di inizio e fine stuffing.

CONTEGGIO DI CARATTERI

Manda un elemento di segnalazione (un byte) che mi indicherà il numero di caratteri consecutivi che costituiranno una trama. Questa tecnica non è buona poiché vi è perdita di sincronismo, nel senso che, se perdo un carattere dovuto ad errori, non posso più fare niente.

CARATTERI DI INIZIO E FINE

Si usano sequenze di escape, ovvero codici che indicano quando inizia e finisce una trama. Sono costituite da una coppia di caratteri: un carattere di escape, DLE (data link Escape), seguito da un carattere di controllo che dice se vi è l’inizio di una trama, STX(start of text) o la fine di essa DLE ETX (end of text). Il DLE entra in uno stato di attesa e legge il carattere successivo.

Lo stuffing (riempimento di caratteri) è una tecnica che si utilizza quando il trasmettitore si trova a dover trasmettere un carattere DLE che non fa parte della sequenza di escape. In questo caso raddoppio il DLE, aggiungendo quindi un nuovo carattere fittizio all’interno della trama, poi continua a trasmettere il resto. Il ricevitore, quindi, quando nella trama riconosce un DLE si mette in attesa di un fine trama, ETX, ma se trova un altro DLE, lo scarta e scrive DLE all’interno della trama.

INDICATORI DI INIZIO E FINE

Non usiamo una sequenza di escape per inizio e fine trama, ma usiamo una sequenza specifica di bit, flag di sincronizzazione, costituito da un byte (8 bit). I bit estremi sono posti a 0 mentre i 6 bit centrali sono posti a 1.

Per avviare una trama metto, quindi, un flag, poi ci sono gli altri bit ed infine un altro flag.

Vi è un problema, ovvero la sequenza di sincronizzazione può occorrere nella mia trama. In questo caso facciamo lo stuffing di bit e non più di caratteri. Quindi, visto che la sequenza di 6 bit ad 1 non è una sequenza accettabile, visto che mi deve indicare la sequenza di sincronizzazione, non consentirà mai una sequenza consecutiva di tali bit, poiché inserirò un bit a 0 di stuffing dopo ogni 5 bit a 1 in modo da interrompere (riempimento di bit). In ricezione appena trovo una sequenza di 5 bit a 1 seguita da uno 0 tolgo lo 0.

VIOLAZIONE DI CODIFICA

È possibile segnalare l’inizio o la fine di una trama con un errore di codifica. Ad esempio, usando la codifica Manchester, potrei omettere una transizione da 1 a 0 o da 0 a 1 per far in modo che venga riconosciuto l’errore di codifica come un carattere di inizio o fine trama.

CONTROLLO DI FLUSSO

Può capitare che una sorgente sia in grado di trasmettere ad un tasso più alto della capacità di ricevere a destinazione. Senza controllo, questo implica che la destinazione inizierebbe a scartare frame trasmessi correttamente per mancanza di risorse. Il protocollo deve poter gestire questa situazione e prevedere dei meccanismi per rallentare la trasmissione. Il trasmettitore deve fermarsi quando non riceve una “via” dal ricevitore.

FRAME DATA LINK

Start flag -> flag di inizio trama;

Type -> tipo pacchetto (es: data, ack, nack);

Seq -> “sequence number” il numero di sequenza del pacchetto;

Ack -> “ack number “, indica il numero di riscontro, ovvero indica la trama che ho riscontrato;

Pacchetto-> indica la parte di dati utili;

Check sum -> insieme di bit di controllo utili per verificare se ci sono stati errori nel contesto

trasmissivo;

End flag -> flag di fine trama.

PROTOCOLLI DATA LINK

Abbiamo un trasmettitore ed un ricevitore. Il trasmettitore riceve i dati dal livello di rete, li trasforma in una trama e li manda al livello fisico. Quest’ultimo fa viaggiare i dati su un mezzo fisico, che vengono riconosciuti dal livello fisico, letti dal data-link e passati al livello di rete.

Se la trama non arriva o se non funziona, non c’è nessun controllo e viene persa o viene accettata anche se corrotta.

PROTOCOLLO STOP-AND-WAIT

Il trasmettitore riceve un pacchetto dal livello di rete, costruisce la trama, lo manda al livello fisico e la trama viene inviata. A questo punto il trasmettitore mette in attesa dell’evento di riscontro. Il ricevitore riceve la trama che, se è corretta, viene mandata sopra, incrementa di numero di sequenza attesa, prepara il riscontro al livello fisico e lo manda al trasmettitore che è pronto a ritrasmettere.

PROTOCOLLO CON TIMEOUT

Per gestire la situazione quando il riscontro non viene inviato si deve prevedere un meccanismo di segnalazione: timeout. Se inviato un pacchetto di dati ricevo un riscontro prima del timeout tutto va bene. Viceversa, se non ricevo un riscontro prima del timeout, innesco una ritrasmissione, generando un altro uguale al precedente, con lo stesso numero di sequenza e lo mando avanti. Nella trasmissione ogni volta che trasmetto un nuovo pacchetto viene inserito il numero di sequenza, il quale viene incrementato man mano che aggiungo pacchetti. Il riscontro nel campo “ack” si porta avanti il numero di sequenza del pacchetto che sta riscontrando, in modo da capire esattamente chi sta riscontrando.

Se il pacchetto è arrivato correttamente rispetto al livello superiore, ma la trama di riscontro è andata persa, il trasmettitore sarò convinto che la trama sarà andata perduta, anche se ciò non è vero. In questo caso la trama viene ritrasmessa e si innesca il fenomeno di trama duplicata ovvero che la stessa trama viene inviata due volte; se la trama è già ritrasmessa va quindi scartata, non cambia nulla.

Ruolo fondamentale in questo processo è quello del sequence number che, non ha solo il compito di gestire l’ordine di arrivo dei pacchetti, ma serve per capire quando ritorna un pacchetto dovuto ad un riscontro perduto. Facciamo un “check” del sequence number. Se quest’ultimo è uguale al precedente. Allora va scartato.

Queste famiglie di protocolli che si basano sullo scadere del timeout precedono il nome di ARQ (Automatic Repeat request), ovvero il non ricevere un riscontro permette una ritrasmissione automatica. Bisogna trovare un giusto compromesso tempistico tra timeout e riscontro.

TRASMISSIONE FULL DUPLEX

Quando il canale di comunicazione permette l’invio di dati in entrambe le direzioni contemporaneamente è possibile definire protocolli di comunicazione detti full-duplex.

ACKNOWLEDGE IN PIGGYBACKING

Per motivi di efficienza spesso si utilizza una traccia chiamata “piggybacking” (a cavalluccio) -> il riscontro viene messo a cavalluccio del pacchetto di ritorno, avvalorando il campo ACK con l’ultimo valore riscontrato.

Se però non ho nessun dato da mandare sono costretto a mandare una trama di riscontro specifica. Ciò comporta l’aggiunta di un timer. Se mi arriva la trama su cui aggiungere un riscontro entro quel timer mi va bene, viceversa se alla fine del timer allora manderò una specifica trama di riscontro.

Problema-> si può mandare più di una trama alla volta prima di fermarsi ed accettare un riscontro. Potrei mandare blocchi di trame se ho a disposizione adeguato strato di bufferizzazione e opportune risorse.

PROTOCOLLI A FINESTRA SCORREVOLE (sliding window)

Sono caratterizzati dalla dimensione della finestra che stabilisce il numero di frame che possono essere inviati prima di fermarsi ed attendere un riscontro. Le trame possono arrivare in sequenza, una dietro l’altra. Il numero di frequenza (seq) garantisce il riconoscimento delle trame. Se arriva in ricezione un blocco di trame consecutive, tutte correttamente, il ricevitore dirà che avrà ricevuto tutte le trame fino all’ultima. Quindi farà un solo riscontro per tutte. Ciò comporta che sia il trasmettitore che il ricevitore abbiano un buffer della stessa dimensione della finestra. Fino a che dei pacchetti non vengono riscontrati bisogna conservarli, solo dopo il riscontro possono essere buttati. La dimensione della finestra si può decidere a priori oppure può cambiare dinamicamente sulla base dell’andamento della rete.

In realtà si deve tener conto di che finestra:

* Finestra di trasmissione (lato trasmettitore);
* Finestra di ricezione (lato ricevitore).

La prima deve tener conservate le trame di cui non si ha ancora avuto riscontro, attraverso dei buffer. Ogni volta che si trasmette a 0 oppure a w-1 slot, mangio uno slot; il limite inferiore deve quindi avanzare di uno. Man mano quindi la finestra si chiuderà. Quando arriva il riscontro aumenta il limite superiore, dunque, la finestra che stava per chiudersi, tende ad aprirsi di nuovo. Può tornare alla dimensione di w slot, dimensione totale.

La seconda tiene conto dei frame ricevuti, deve conservali poiché ancora non ha inviato nessun riscontro. Valuta quali frame sono ancora accettabili in ricezione e quanti frame posso bufferizzare prima di inviare un riscontro. In generale il limite inferiore aumenta di 1 quando arriva una trama, mentre il limite superiore aumenta di 1 quando manda un riscontro. Non può crescere oltre la dimensione massima (numero di buffer a disposizione).

Se ricevo un frame oltre la finestra di ricezione, significa aver ricevuto un frame fuori frequenza, quindi lo scarto.

N.B. Sono uguali ai protocolli Stop-and-wait, ma erano a caso limite con dimensione della finestra a 1.

PROTOCOLLI FINESTRA SCORREVOLE CON ERRORI

Nei protocolli a finestra scorrevole, quanto più ampia diventa la dimensione della finestra tanto più il protocollo si può trovare in una situazione di criticità. Esistono due protocolli che gestiscono questa situazione: go-back-n e selective reject (ritrasmissione selettiva).

Il primo protocollo nel momento in cui ho un messaggio che interrompe la continuità della finestra, si ferma al punto dell’ultimo messaggio riscontrato e scarta tutti gli altri messaggi fuori sequenza. Se innesca automaticamente la ritrasmissione dell’ultimo messaggio e poi riavvia tutto. Lo svantaggio è che se ho trasmesso 100 frame e solo il primo è sbagliato mentre gli altri no, sarò costretto a ritrasmetterli tutti e 100 (spreco banda).

Il secondo protocollo è un segnale di stop al trasmettitore, che si manda quando il ricevitore non è più in condizione di ricevere trame. Questo stop forzato avviene fin quando non viene inviato l’ordine di sblocco.

Ci si può comportare in due modi:

1)appena arriva un frame errato, lo si deve scartare in ogni caso. Se il mittente del frame scorretto non manda nulla di successivo spira il timer e il mittente continua a ritrasmettere dal primo non riscontrato (ACK riscontro positivo).

2)se, invece, il mittente manda dei frame successivi al frame che risulta errato, si manda un NACK (riscontro negativo). A questo punto l’inviante ripartirà a ritrasmettere dal primo frame non riscontrato, senza svuotare prima la finestra e in seguito svuoterà il suo buffer.

RILEVAZIONE DELL’ERRORE

Il livello fisico offre un canale di trasmissione non privo di errori:

-errori sul singolo bit;

-replicazione di bit;

-perdita di bit.

Per la rilevazione di tali errori, nell’header di ogni frame si inserisce un campo denominato checksum, risultato di un calcolo fatto utilizzando i bit della trama. La destinazione ripete il calcolo e confronta il risultato con il checksum: se coincide la trama è corretta.

CAMPO DI GALOIS

Per capire il funzionamento degli elementi introduciamo il concetto di campo di Galois: un campo finito con un certo numero di elementi su cui sono definite 2 operazioni aritmetiche (addizione e moltiplicazione) che godono della proprietà commutativa ed associativa GF(q).

GF(q) è chiuso rispetto all’addizione e moltiplicazione: qualunque risultato di queste due operazioni cade nel campo. In generale q deve essere sempre primo o potenza di numeri primi. Le operazioni vengono fatte con l’aggiunta di un ulteriore operazione di mod q. I campi di galois ci fanno rimanere confinati in un certo range di valori (ad esempio se io ho allocato 8 bit resterò sempre negli 8 bit). Si usa per le operazioni binarie.

CODICI DI CONTROLLO: CRC (Codice a ridondanza ciclica)

(Cycle Redundace Check-sum) su GF: basato sul concetto di codice ciclico in cui permutando ciclicamente gli elementi di una qualsiasi comunicazione, si ottengono combinazioni dello stesso codice. Non è tanto efficiente.

RAPPRESENTAZIONE DI SEQUENZA DI BIT TRAMITE POLINOMI

Una sequenza di N bit può essere rappresentata tramite un polinomio a coefficienti binari, di grado n-1, tale che i suoi coefficienti siano uguali ai valori dei bit della sequenza. Il bit più a sinistra rappresenta il coefficiente del termine di grado n-1, mentre il bit più a destra rappresenta il termine noto, di grado 0. Ad esempio, la sequenza 1001011011 può essere rappresentata dal polinomio x⁹+ x⁶+ x⁴+ x³+ x + 1. Il grado del polinomio è determinato dal primo bit a sinistra di valore 1 presente nella sequenza.

CODIFICA POLINOMIALE (CRC)

La tecnica consiste nel considerare i dati (m bit) da inviare come un polinomio di grado m-1. Trasmettitore e ricevitore si accordano su un polinomio aggiuntivo fisso, ovvero il polinomio generatore G(x) di grado r indipendente dai polinomi che distinguono ogni trama. G(x) è pre-concordato tra trasmettitore e ricevitore (implementato in hardware).

Il trasmettitore aggiunge in coda al messaggio una sequenza di bit di controllo (CRC) in modo che il polinomio associato ai bit del frame trasmesso costituito dall’insieme dei dati e CRC sia divisibile per G(x). In ricezione si divide il polinomio associato ai dati ricevuti per G(x):

-se la divisione ha resto nullo, si assume che la trasmissione sia avvenuta senza errori;

-se la divisione ha resto non nullo, sono certamente avvenuti 1 o più errori.

CODICI CICLICI

Assegniamo un polinomio P di grado p-1 al messaggio che vogliamo trasmettere

M= 10100011 => P(x)= 1 (x⁷) + 0(x⁶) + 1 (x⁵) + 0(x⁴) + 0(x³) + 0(x²)+ 1(x)+ 1 (x°) cioè P(X) = x⁷+ x⁵+ x+1

Scelto G(x) di grado r< =p-1 detto polinomio generatore (conosciuto sia dalla sorgente che dall’utente), si aggiungono r zeri ai p bit del blocco da trasmettere; per esempio:

G(x) = x³+1 diviene x³P(x) = x¹⁰ + x⁸ + x⁴+ x³ cioè P= 10100011000 ho aggiunto 3 zeri

Effettuando la divisione x alla m p(x) / G(x) = x¹⁰ + x⁸ + x⁴+ x³/ x³+1

Q(x) G(x) +R(x) = x alla m P(x) cioè x alla m P(x) - R(x) = Q(x)G(x)

Poiché operiamo nel caso dei codici binari, il campo di Galois utilizzato è GF (2); quindi –R(x)= +R(x) . La formula precedente diventa x alla m P(x) + R(x) = Q(x)G(x)

Nel nostro es. diviene Q(x) = 10110101-> x⁷+x⁵+x⁴+x²+1 R(x)= 101 -> x²+1

Quindi quello che trasmettiamo è esattamente la parola corrispondente al polinomio x alla m P(x)+ R(x) che nel nostro caso è T= 10100011101 T(x)= x¹⁰ + x⁸ + x⁴+ x³+ x²+1

Per verificare la corretta trasmissione basta dividere T(x) per G(x); se il resto della divisione è zero allora non si è verificato nessun errore.

CRC STANDARD

Sono stati definiti dei polinomi di fatto usati come standard

G(x) = x¹² +x ¹¹+ x³+ x²+ x + 1 CRC-12

G(x) = x ¹⁶+ x ¹⁵+ x²+1 CRC-16

G(x) = x ¹⁶+ x¹² +x⁵+1 CRC – CCITT

G(x)= x ³²+ x²⁶+x²³+ x²²+ x ¹⁶+ x¹² +x ¹¹+ x⁸+->x⁷+x⁵+x⁴+x²+1 CRC-32

Tutti contengono x+1 come fattore. CRC-16 e CRC-CCITT riconoscono errori singoli e doppi errori con un numero dispari di bit, i burst di errori di lunghezza massima 16.

LE LAN

Il primo problema delle reti locali è che generalmente sono reti che si poggiano sull’uso condiviso (anche per questo sono a basso costo) di un mezzo trasmissivo chiamato anche il portante (DIVERSO da “la portante”). Si potrebbe condividere in maniera classica FDM o TDM, ma questa logica costa e non è efficiente in ambienti dinamici. Su queste tecnologie la fa da padrona l’allocazione dinamica, questo comporta di introdurre delle complessità per arbitrare l’accesso al mezzo, se malauguratamente due stazioni accedono contemporaneamente e iniziano a trasmettere si verifica la collisione. Nell’allocazione dinamica non si possono evitare le collisioni, quindi l’unica cosa da fare è individuarle e porre rimedio. Si fa il rilevamento collisioni (collision-Detection) perché di fatto una collisione è una connessione andata male. Quindi si può lavorare o in collision-detection oppure si lavora in collision-free cioè inventarci qualche protocollo a livello datalink tale che il fenomeno della collisione non si verifichi.

Collision-detection: la collisione viene rilevata ascoltando il canale e verificando che il segnale ricevuto corrisponda a quello trasmesso senza interferenze basta una minima sovrapposizione dei due pacchetti per farli andare persi.

CSMA

Carrier Sense Multiple Access: è il meccanismo per vedere se abbiamo il diritto a trasmettere. Il CSMA innanzitutto deve individuare la presenza di una portante (un segnale di trasmissione di qualcuno che ha una trasmissione in corso) se percepisce una portante significa che qualcun altro sta trasmettendo si ferma e ricomincia, altrimenti può trasmettere il pacchetto e poi verificare se c’è una collisione. Se c’è la collisione si attende un tempo casuale e si ricomincia daccapo a percepire una portante se c’è si continua a percepire (in loop) in maniera aggressiva. Questo approccio si chiama CSMA 1-persistente perché con probabilità uno appena percepisco una portante mi metto immediatamente a percepire se c’è una portante iterativamente. Con questo protocollo acquista grande importanza il ritardo di

propagazione del segnale tra due stazioni; infatti, quando una stazione inizia a trasmettere, una seconda stazione potrebbe voler trasmettere, ed ascolta il canale o se il segnale trasmesso dalla prima stazione non ha ancora avuto il tempo di propagarsi fino alla seconda stazione, questa troverà il canale libero e trasmetterà, generando una collisione. Maggiore è il ritardo di propagazione, più numerose saranno le collisioni. Inoltre, CSMA 1-persistente non richiede la sincronizzazione delle stazioni connesse alla rete.

Se si vuole essere meno aggressivi si deve solo cambiare l’approccio al controllo della portante: se la portante c’è aspetto un tempo casuale (se c’è la collisione funziona come CSMA1-persistente); quindi si parla di CSMA non persistente. Questo protocollo alza l’efficienza di utilizzo del canale aumenta con l’aumento del carico, cioè delle stazioni connessi alla rete. Il problema riscontrato, però, è che quando aumenta il carico, il tempo che intercorre tra l’istante in cui la stazione vuole trasmettere e l’istante in cui riesce a trasmettere può crescere enormemente.

C’è una via di mezzo statistica CSMA p-persistenza; cioè si stabilisce una probabilità p per cui ogni volta che percepiamo una portante con una probabilità p ci mettiamo immediatamente in ascolto (quindi persistente) invece con una probabilità 1-p si attende un numero casuale di slot temporali.

COME SI RILEVA UNA PORTANTE: si utilizza la codifica Manchester e sapendo che vi è una transizione di stato in ogni intervallo, quindi basta percepire le oscillazioni per percepire una portante.

CSMA/CD

Si parla di CSMA/CD perché il protocollo opera in tre diverse fasi:

• *carrier sense:* (rilevazione della trasmissione): ogni stazione che deve trasmettere ascolta il bus e decide di trasmettere solo se questo è libero;

• *multiple access*: nonostante il carrier sense è possibile che due stazioni, trovando il mezzo trasmissivo libero, decidano contemporaneamente di trasmettere; la probabilità di questo evento è aumentata dal fatto che il tempo di propagazione dei segnali sul cavo non è nullo, e quindi una stazione può credere che il mezzo sia ancora libero anche quando un'altra ha già iniziato la trasmissione;

• *collision detection*: se si verifica la sovrapposizione di due trasmissioni si ha una "collisione"; per rilevarla, ogni stazione, mentre trasmette un pacchetto, ascolta i segnali sul mezzo trasmissivo, confrontandoli con quelli da lei generati (*listen while talking*).

Alla fine di una trasmissione si può avere un periodo di contesa se 2 o più stazioni iniziano a trasmettere. L’ampiezza di ciascun slot di contesa dipende dal ritardo di propagazione

(dalla distanza delle stazioni che trasmettono in contemporanea). I periodi morti si hanno quando nessuna stazione ha frame da trasmettere. Sia T il tempo di propagazione fra le stazioni più lontane. Il tempo massimo per la rilevazione di una collisione è 2T slot di contesa.

Quando una delle stazioni si accorge di una collisione, non solo si ferma, ma deve rendere più facile all’altra il rilevamento della collisione; quindi manda una sequenza speciale che si chiama jamming, che è di fatto un’interferenza trasmissiva. Tutte le stazioni percepiscono questa sequenza e interrompono le loro attività e mandano questa sequenza per far capire che c’è una collisione.

DOMANDA D’ESAME!! DOMINIO DI COLLISIONI cioè numero di stazioni che concorrono sullo stesso segmento di rete alla logica del CSMA/CD.

PROTOCOLLI COLLISION FREE (non si usano più)

È una logica a prenotazione, si ha una divisione del mezzo trasmissivo in slot dove quest’ultimi sono prenotabili. Si crea una mappa di bit che rappresenta il numero di stazioni disponibili e che devono concorrere nell’accesso al mezzo, a questo punto appena le stazioni devono trasmettere, parte il periodo di contesa. In questo periodo le stazioni andranno a trasmettere un bit che va a riempire quello che si chiama la mappa di prenotazione; in pratica si apre il periodo di contesa e in ordini le stazioni dicono se vogliono trasmettere o no (1 se ha bisogno 0 no). Avendo a disposizione questa mappa di bit ogni stazione saprà quali sono le altre che trasmetteranno e in ordine una alla volta avrà il diritto di trasmettere. In questo modo si riesce a regolare l’accesso simultaneo al canale senza collisioni. In questo algoritmo c’è un problema perché se n (il numero di stazioni) cresce notevolmente le stazioni con indirizzo più alto dovranno attendere molto tempo. Ci può essere una variante di questo con il round robin, ma anche così si aspetta sempre n slot. Lavorando a rete piena questo protocollo diventa come un TDM statico.

Un esempio di questo protocollo è il Token Ring: un insieme di collegamenti punto-punto associati in successione per realizzare una topologia ad anello. Nell’anello gira continuamente un token, quando una stazione vuole trasmettere, si impossessa del token (lo rimuove dall’anello e cambia un bit nel byte Access Control), manda il suo frame e poi rimette in circolazione il token. Bisogna stare attenti alla dimensione del token, deve essere più piccolo, in termini di bit, rispetto alle stazioni che popolano l’anello. In condizioni di carico elevato il protocollo diventa estremamente efficiente.

STANDARD IEEE 802

È la famiglia di standard che domina la tecnologia datalink per le reti LAN. Fondamentalmente è un insieme di protocolli che prevedono l’uso del CSMA/CD e varianti basate su token. Prevede una serie di sotto elementi che vanno a definire protocolli specifici rivolti a specifiche tecnologie (es. 802.11 wireless o 802.3 ethernet).

Dei sottogruppi hanno promulgato una serie di specifiche che si chiamano ANNEX e sotto questi ci sono altri comitati di standardizzazione associati a variazioni specifiche di queste tecnologie.

IEEE 802.1

È lo standard contenente le specifiche generali del progetto 802. Questo standard lavora su due livelli: LLC (logical Link Control) e MAC (Media Access Control). Il sottolivello LLC è comune a tutte le LAN ed è l'interfaccia unificata verso il livello Network, mentre il MAC è peculiare di ciascuna LAN, così come il livello fisico al quale è strettamente associato, risolve il problema della condivisione del mezzo trasmissivo.

Il MAC

È indispensabile perché definisce tutte le caratteristiche di livello due che devono essere “coniugate” sul supporto fisico su cui si deve trasmettere, gestisce anche tutto l’indirizzamento sul mezzo trasmissivo. Si definisce anche il tipo di trasmissione che si fa: punto a punto, punto- multipunto o broadcast. Deve tener conto anche della topologia della LAN che implica leggere variazioni sulle possibili modalità di realizzazione dei vari tipi di trasmissioni.

MAC PDU

È la trama del livello datalink che si suddivide in due sottolivelli MAC –PDU e LLC-PDU che è incapsulata in quella MAC. MAC-PDU è una trama che inserisce delle info di controllo per geriste tutte le funzionalità a livello MAC. In quest’ultimo ci sono due indirizzi importanti indirizzo sorgente(MAC-SSAP) ed indirizzo destinazione (MAC-DSAP), questi permettono di individuare il punto di origine e destinazione della trama stessa.

IEEE 802.3 E ETHERNET

È nata come rete CSMA/CD in logica 1-persistente in grado di funzionare fino a 100 mbps.

La struttura del frame:

- in testa c’è un preambolo di 7 byte (che alternano 0 e 1 ) che ci aiuta a capire quando inizia una nuova trama, che genera un’onda quadra ;

-secondo campo è “start of frame “, di fatto una sequenza 101010 (identica al preambolo) però fa interrompere l’onda quadra perché ha gli ultimi due bit a 1;

-terzo campo: indirizzi fisici o MAC-ADDRESS (destinazione e sorgente), che è una sequenza di 48 bit;

-quarto campo: costituito da 4 byte che è utilizzabili in vari modi, ad esempio identificabile il tipo di trama e/o per indentificare la lunghezza della trama;

-infine c’è una parte variabile peilod (non so come si scrive).

INDIRIZZAMENTO SU ETHERNET

Sono indirizzi a 48 bit e devono permettere di fare l’invio unicast, broadcast e multicast consultato i bit di ordine più significativo: il primo bit mi dice se l’indirizzo a cui faccio riferimento è individuale (0) o di gruppo (1), il secondo bit individua lo scope di validità dell’indirizzo (globale 0 / locale 1 ). Sono tutti diversi per legge.

LUNGHEZZA DEL FRAME

Un frame valido deve essere lungo almeno 64 byte; il campo dati deve avere almeno 46 byte (eventuale padding/riempimento). La lunghezza minima di un pacchetto deve garantire che la trasmissione non termini prima che il primo bit abbia raggiunto l’estremità più lontana e sia tornata indietro una eventuale collisione.

EXPONENTIAL BACK-OFF

È un algoritmo. Si ha uno slot di contesa pari a 2 T, alla prima collisione si aspetta o 0 o 1 slot temporali, se la collisione è iterata si aspetta 0 o 1 o 2 o 3 questo viene iterato fino a un massimo di 16, se si fallisce anche il 16 si notifica l’errore di trasmissione; in questo caso c’è un’unica soluzione: ridurre le stazioni nella rete (riduco il dominio di collisione). Aumenta la latenza, ho un peggioramento delle prestazioni, ma globalmente il meccanismo continua a funzionare.

PRESTAZIONI

Essendo l’ethernet un CSMA/CD 1-persistente, quando il carico è basso la rete si comporta in maniera ottimale, limitando a minimo i ritardi; quando il carico sale, grazie al back-off esponenziale, la rete si adegua e si comporterà come un p-persistente. Ci sono delle dipendenze: numero di stazioni e dimensione media delle trame.

Con trame piccole ethernet tende a comportarsi bene, ma usare male il mezzo.

TECNOLOGIE ETHERNET

L’insieme di protocolli Ethernet domina saldamente il mercato delle LAN. La velocità di trasmissione originariamente era 10 Mbit/s su cavo coassiale, ora è evoluta su diversi mezzi trasmissivi fino a 10 Gbit/s (Gigabit Ethernet), passando da trasmissioni nel dominio elettrico a trasmissioni su fibra; conservando più o meno le stesse caratteristiche in termini protocollari. Attraverso i diversi adattamenti a livello MAC si è consentita l’adattabilità del protocollo a diversi standard trasmissivi.

ETHERNET A 10, 100, 1000, … MB/S

Ethernet a bassa velocità si parla di rete a bus con cavo coassiale condiviso, ma il bus fisico è problematico perché se ad esempio si vuole inserire una nuova stazione si deve interrompere tutta la rete. Quindi è stato reingegnerizzato invece di avere un cavo su cui tutti si agganciano ogni stazione ha un filo che va in un hub o switch che fa da bus condiviso.

Per l’ethernet si usa la codifica Manchester, però fino quello a 100 megabit perché ha un’aggressività nell’occupazione spettrale.

10 BASE 5

La prima ethernet usava un cavo giallo di grande dimensioni (chiamato thick ethernet); lo standard di riferimento si chiamava 10 base 5, quindi il MAC-LAYER si adeguava a questa specificità. Questo cavo aveva delle tacche specifiche ogni 2,5 metri (distanza per garantire il rilevamento delle collisioni) su cui era possibile inserire attraverso il transceiver (vampiro) le varie stazioni.

10 BASE 2

Per evitare che la vampirizzazione del cavo (il processo per attaccare una stazione al cavo che rischiava di rompere il cavo e interrompere l’intera rete) c’è l’alternativa della 10 base 2 (thin Ethernet) con un cavo più flessibile con un adattatore a T che interrompeva il cavo e si inseriva. Il problema di questo ethernet è che se si inseriva una nuova stazione si doveva aprire il cavo inserire una T e chiudere il cavo.

10 BASE T

È l’ethernet attuale che fa collassare tutto in un punto quindi una topologia a stella, ma è sempre un bus. Gli hub sono ripetitori di segnale che interconnettono tutte le stazioni. Usa il broadcast multi-access cioè una qualunque trama inviata su una porta viene ripetuta in tutte le porte, perciò si chiama anche repeater. Un segnale danneggiato viene letto e rigenerato completamente. Tutte le macchine collegate alle porte del ripetitore fanno parte dello stesso dominio di collisione; quindi se si collegano due ripetitori si estende il dominio di collisione.

C’è un limite al numero di ripetitori (max 4 medi) che si possono collegare perché aumentando notevolmente il numero di stazioni collegate, aumentando il dominio la reta ad un certo punto collasserà e potrei superare la lunghezza massima di una LAN : 2,5 km che è la lunghezza massima che corrisponde a 2T che è il tempo impiegato dal segnale per percorre 2,5km ; superato 2,5km non si riescono a rilevare le collisioni.

DOMANDA D’ESAME: un oggetto del genere a che livello lo troviamo? Si trova a livello fisico. Qual è il passaggio dal’ethernet classica a quella moderna? Si è passati al connettore RJ-45, pluggabile a 8 fili che permette di essere collegato direttamente al doppino che poi viene agganciato alla porta del ripetitore senza interrompere le altre stazioni.

FAST ETHERNET

Si passa quindi da 10 megabit a 100. Si usa ancora la codifica Manchester, si riduce il tempo di bit a 10ns e si hanno diversi arrangiamenti.

100 base T4 che usa tutti e 4 i doppini, ma ormai non si usa più.

100 BASE- TX E 100 BASE-FX

Il primo corrisponde a un ethernet a 100 megabit fatta su rame e l’altro su fibra. Quella su rame utilizza la classica trasmissione a 125 mhz su 2 doppini e usa la codifica 4B5B (4 bit in 5 periodi di clock) che è più redditizia della Manchester e permette di lavorare in full duplex a 100 megabit. Quando si utilizza la fibra è la stessa cosa solo che si cambia il mezzo trasmissivo; si usano due fibre una per la trasmissione e l’altra per la ricezione tipicamente multimodale.

La stessa interfaccia fisica può parlare a 10 e 100 mbps.

GIGABIT ETHERNET

Formato di trama sempre 802.3; continua a esistere il CSMA/CD, ma con dominio di collisione che diventa confinato a due singole stazioni cioè a una logica punto punto. Si va ad utilizzare uno switch che ha ogni porta in un singolo dominio di collisione quindi la rete è molto più efficiente. Funziona il half duplex e full duplex. Ha una compatibilità a ritroso, cioè questa interfaccia lavora anche a 100 e 10 mbps. La dimensione del pacchetto aumenta di un fattore10. La codifica del Giga ethernet è la 8B10B cioè una sequenza di 8 bit è codificata con 10 bit (ridondanza), si riesce ad essere più efficiente e gestire l’interferenza intersimbolica in maniera ottimale. Si utilizzano tutte e 4 le coppie del cavo in modalità full duplex. Con il giga nasce un interfaccia standardizzata che il MAC-ADDRESS offre di tipo agnostico: viene definito un sotto standard che stabilisce 4 modalità di interfacciamento fisico: 1000 base LX fibra multimodale o monomodale con laser ad alte intensità che fa fino a 500 m per la multimodale mentre fa fino a 10 km per l’altra ; 1000 base SX fibra monomodale si usa il VC-SEL e per distanze limitate; 1000 base CX, lavora su un cavo in rame schermato; 1000 base T, se voglio avere collegamenti giga in rame con cavo STP o UTP .

Il gigabit implementa in hardware un meccanismo di controllo di flusso perché, visto la compatibilità a ritroso, sulla stessa rete possiamo avere stazioni che lavorano 10 mbps e una a 1 giga. Questo meccanismo ha una trama di start e stop il frame 8808.

LIVELLI GIGABIT ETHERNET

Si ha il livello MAC poi il livello Gigabit Media Independent Interface e poi la specifica se si lavora su fibra o su cavo coassiale o su rame con i vari standard ad esempio 1000base LX.

10 GIGABIT ETHERNET

Sono state modificate delle cose: non si può più fare half-duplex, non è ammissibile il CSMA/CD. Ci sono altre soluzioni che permettono di lavorare su fibra, rame e coassiale; queste hanno più o meno le stesse caratteristiche del gigabit ethernet in termini di distanze basta mantenere le compatibilità dello stesso formato di trama, mantenere le stesse dimensioni massima e minima della trama.

DOMINIO DI COLLISIONE: insieme di macchine che sullo stesso segmento di rete concorrono nella stessa logica CSMA/CD

DOMINIO DI BROADCAST: l’insieme di macchine che sullo stesso segmento di rete quando riceve un frame di broadcast lo prende in carico.

REPEATER E HUB

Per ampliare una rete si possono mettere in serie hub e ripetitori. Se si collegano due ripetitori si estende il dominio di collisione restando nello stesso dominio di broadcast; si ha il limite di 4 ripetitori tra due transceiver.

DOMANDA D’ESAME: a che livello lavorano Bridge e Switch? a livello datalink

BRIDGE E SWITCH

Il bridge è un dispositivo multiporta (tipicamente due) che lavora a livello datalink e ci permette di interconnettere LAN che usano datalink differenti o lo stesso, segmentando le LAN, e separando i domini di collisione (è come un ponte che separa a metà un dominio CSMA/CD in due domini) . Oltre a partizionare la rete e quindi a ridurre il carico, (funzione principale) e quindi far crescere potenzialmente quest’ultima, fa un’altra cosa: controlla se tutti i frame che passano sono corretti, quindi ripulisce il traffico da eventuali errori (rende la rete più sicura). Se partizioniamo la rete in logica gerarchica con il bridge la possiamo far crescere fin quando vogliamo.

TRANSPARENT BRIDGING

Il bridge deve avere una visione topologica della rete per sapere quali stazioni stanno su un lato del ponte o sull’altro, per evitare che l’amministratore di rete si metta a controllare quali stazioni si trova su un lato piuttosto che sull’altro (impensabili per reti di grandi dimensioni) si usa il Trasparent Bridging. Questo bridging funziona in logica plug and play (nessuna configurazione), il dispositivo impara da solo la topologia della rete osservando (lavorando in modalità promiscua) il traffico che l’attraversa. Inizialmente si comporta come un repeater o hub, ma appena ci passa un frame il bridge ispeziona l’indirizzo sorgente così sa su quale interfaccia sta la stazione e mano mano il bridge si costruirà una mappa (MAC addresstable) che associa indirizzi sorgente a lati/interfaccia di bridge; quest’attività si chiama backward learning. Dopo quest’attività conosce le destinazioni quindi fa delle cross connessioni cioè dal momento che sa dove si trova quella destinazione manda la trama solo ed esclusivamente in quella porta riducendo il traffico.

SWITCHES

Dal punto di vista funzionale uno switch è un bridge multiporta, però a livello di prestazioni sono differenti, questo scala meglio perché dovendo avere apparati con un numero elevato di porte la funzionalità di switching è implementata in maniera hardware. Partiziona la rete in segmenti separati ognuno dei quali in domini di collisione indipendenti.

APPRENDIMENTO DELLA TOPOLOGIA

Per sapere su quale porta debba essere trasmesso il frame, lo switch deve creare e

mantenere aggiornata una tabella relativa alla associazione tra indirizzo di

destinazione e porta. La costruzione manuale di questa tabella sarebbe troppo costosa in termini di gestione della rete, ed è tutto plug and play. Poiché i frame contengono l’indirizzo del mittente, ad ogni frame che arriva lo switch impara che la stazione che ha inviato il frame è raggiungibile attraverso la porta da cui è’ arrivato il frame stesso; con il passare del tempo lo switch riempie la tabella e può svolgere la sua funzione in modo sempre più efficiente.

IL BACKWARD LEARNIING

Al boot(quando inizia a funzionare) le tabelle sono vuote Se un pacchetto ha una destinazione sconosciuta viene emesso su tutte le porte eccetto quella di provenienza, ma in ogni caso viene usato l’indirizzo di provenienza per definire la posizione del mittente nella tabella(MAC addresstable). Queste info non sono permanenti: periodicamente vengono eliminate le linee più vecchie.

BRIDGING E SWITCHING

Il bridging può essere software- based mentre lo switching è hardware based(ASIC).

TIPI DI SWITCH

**Cut-through switching**: il frame è letto in parte e subito reindirizzato sulla porta corretta. È apparentemente efficiente, invece non lo è perché se la trama contiene errori la si lascia passare lo stesso, quindi switch di bassa qualità (ad esempio lasciano passare una trama con meno di 64 byte e non va bene).

**Store-and-forward**: il frame è letto completamente dallo switch, viene controllato il CRC prima di inviarlo; in caso di errore il frame è scartato (permette di filtrare il traffico). Questa tipologia richiede più hardware, è più costosa, ma è migliore di qualità.

**Port-based switching**: ad ogni porta corrisponde un solo indirizzo Ethernet.

**Segment-based switching**: ad ogni porta corrispondono più indirizzi (ad esempio è collegata ad un hub).

TECNOLOGIA DEGLI SWITCH

**Shared Memory:** memorizza i pacchetti in una memoria comune a tutte le porte. Invia in pacchetti in memoria alla porta destinazione. Ha *n* inputs and *m* outputs, nella realtà tutte le porte di ingresso sono anche di uscita. L’obiettivo è di avere il massimo throughput (massimo traffico commutato per l’unità di tempo) e deve scalare rispetto a *n* (le porte) poiché il numero di porte può variare.

**Switching Matrix o Fabric:** utilizza una matrice di commutazione; in base all’indirizzo e al contenuto della tabella viene attivata la connessione necessaria (soluzione tecnologicamente migliore).

**Bus-Architecture**: ha un BUS interno condiviso ad alta velocità; la comunicazione interna usa TDMA.

SHARED MEMORY/BUS SWITCH

Logica a basso costo. Limitata scalabilità (le risorse condivise si saturano col carico), realizzati tramite componenti COTS (es. PC), in presenza di *n* porte il trasferimento Mux-memoria deve essere *n* volte più veloce della capacità del link e non scalano.

CROSSBAR SWITCH

Concettualmente semplice: ogni input connesso a ogni possibile output quindi possibili problemi di contesa. La complessità delle porte di uscita aumenta più velocemente di quella delle porte in ingresso. Un crossbar switch “perfetto” (CROSSSBAR FABRIC A LOGICA CENTRALIZZATA) può teoricamente avere tutte le linee connesse a tutte, quindi tutti possono parlare a tutti è meglio e ha la proprietà di essere *non-blocking (sempre disponibile)*, ma costa troppo e la complessità della matrice cresce quadraticamente con il numero di porte di input/output ports, *N*, i.e., cresce come O(*N2*).

LOGICA DISTRIBUITA MULTISTADIO

***Multistage interconnection network (MIN)***

La complessità cresce come O (*N* × log *N*), dove *N* è il numero di porte.

Piuttosto che avere tutti connessi a tutti si utilizzano dei moduli di switching di dimensioni inferiori, che a capacità limitata, ma interconnessi tra di loro in gerarchia, collegano tutti a tutti. La logica di semplificazione multistadio parte da una matrice completa e si divide in due sotto matrici interconnesse con uno switch piccolino 2x2 porte e così via ricorsivamente. Con l’unico difetto che se c’è una richiesta simultanea non può essere più svolta, si ha un blocco.

BLOCCO E CONTESA

Se c’è una richiesta simultanea una deve bloccarsi e attendere il passaggio dell’altra, questa cosa si gestisce attraverso la bufferizzazione.

BUFFERIZZAZIONE

A ciascuna interfaccia è associato un buffer. Se c’è una situazione di blocco la trama viene bufferizzata, appena l’altra trama è stata processata, la risorsa è libera e vado a prendere la prima trama in coda in logica FIFO o RR (round- robin) o a priorità. Ci possono essere due tipi di contesa, contesa sulle porte di ingresso o si può avere la necessità di fabric buffers interi per la contesa sulle porte di uscita. I Buffers vengono riempiti in logica round-robin (da uno **shifter**).

TOPOLOGIE CON RIDONDANZA

In ambiti dove non si possono tollerare un fermo, si deve aggiungere la ridondanza eliminando i single points of failure. Si tendono a duplicare sia i nodi della rete(switch) che gli archi, così in caso di interruzione in un punto c’è il percorso alternativo. Quindi la rete non è più rappresentata da un albero, ma da un grafo; questo però comporta dei problemi.

PROBLEMA DEI BROADCAST STORM

Se la macchina x decide di mandare una trama in broadcast, lo switch A la riceve e inoltra la trama su tutte le sue porte, quindi passa su un link e arriva allo switch B che la replica e inoltra a tutte le sue porte quindi ritorna anche allo switch A; da una trama sono diventate 2 e anche A fa lo stesso quindi ad ogni giro la trama viene replicata, si parte da una trama e si arriva a un numero indefinito (in loop fino a saturazione). La rete non funzionerà più.

REPLICAZIONE DI TRAMA

La macchina x manda una trama unicast al router Y, la trama viaggia sul segmento che, però, è connesso allo switch A che non sa chi è Y quindi replica la trama e la inoltra a tutte le porte, l’altro switch B si comporta come A quindi da una trama ne arrivano due.

INSTABILITA’ DEL MAC ADDRESS DATABASE

La macchina X manda una trama unicast a Y. Switch A and B si segnato che X sta sulla porta 0. Non conoscendo Y gli switch fanno un inoltro su tutte le porte, quindi il MAC address vede che la trama una volta arriva dalla porta 0 e una volta dalla porta 1 quindi diventa instabile.

PROBLEMA DI LOOPS MULTIPLI

Quindi in presenza di loop la LAN non funziona, ma la ridondanza è necessaria. Quindi la soluzione è che pur lavorando su un grafo deve essere trasformato in un albero.

SOLUZIONE: SPANNING TREE PROTOCOL

Si ha una topologia a grafo, ma per il tempo necessario si va a chiudere il ciclo; cioè trasformare una topologia con i loop in un loop free trasformando il grafo in un spanning tree (copre tutti i nodi senza cicli).

SPANNING TREE: FUNZIONAMENTO

Per generare un spanning tree si va a spegnere logicamente alcune interfacce finché non mi serve la ridondanza. Per fare ciò si usa l’algoritmo per il calcolo dello spanning tree che ha dei concetti fondamentali: per ogni rete si ha un elemento privilegiato chiamato root bridge che è il punto da dove si dirama lo spanning tree poi si ha una root port per ogni switch che non è il root bridge che lo conduce verso il root bridge attraverso dei link e poi si ha una designated port per segmento che è una porta che serve per raggiungere un link che non posso spegnere, mentre le porte nondesignated posso essere spente per far diventare il grafo un albero.

BRIDGE PROTOCOL DATA UNIT (BPDU)

Gli switch si parlano tra loro mandandosi delle trame specifiche: i BPDU ogni 2 secondi tipicamente. Per decide chi sarà il root bridge si vede chi ha il Bridge ID più basso che è costituito combinando il MAC-address con bridge priority.

La BPDU ha tutta una serie di informazioni che servono per eleggere il root bridge,localizzare i loops, bloccare le porte per evitare i loops, notificare i cambi di topologia, monitorare lo stato dello spanning tree. La creazione dello spanning tree è dinamico, perché in caso di rottura di un nodo dell’albero, quest’ultimo resterà diviso in due parti quindi deve essere ricalcolato in modo da unificare di nuovo tutta la rete.

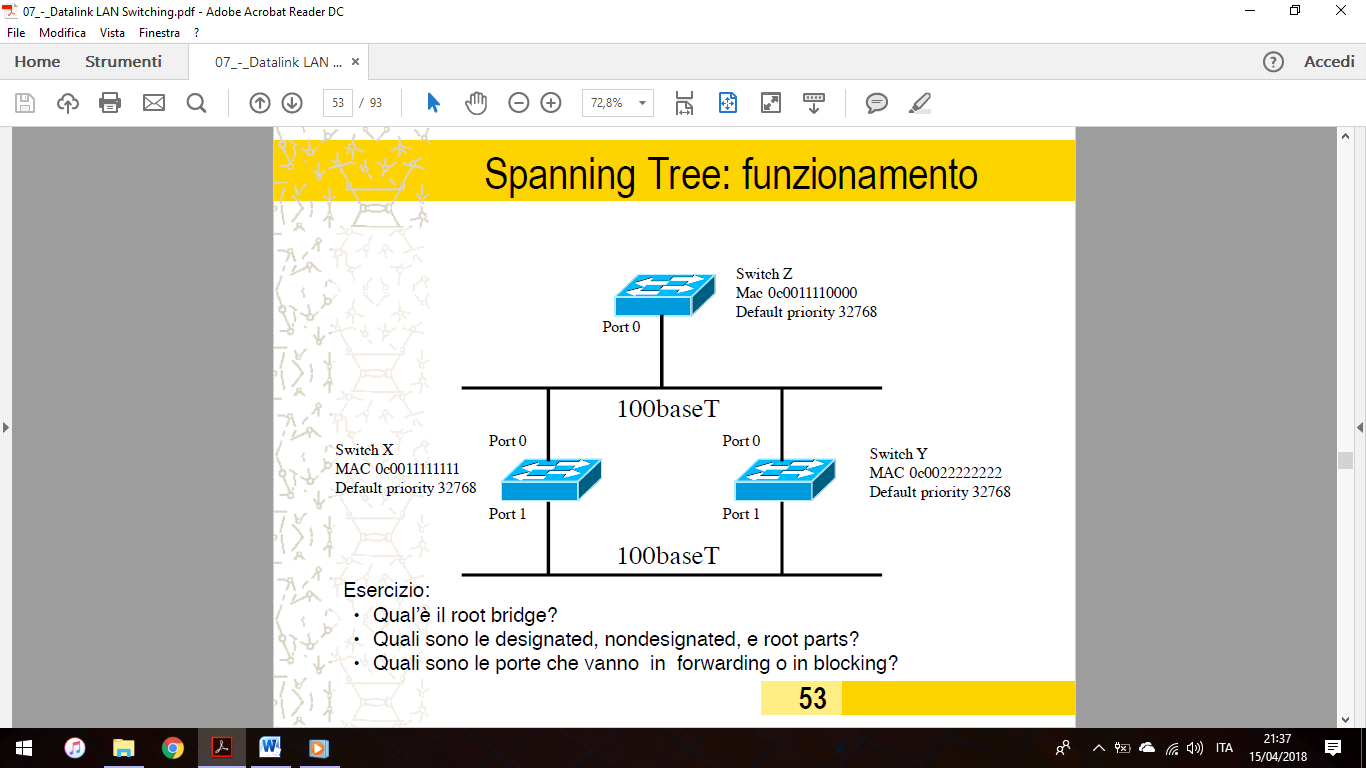
SELEZIONE ROOT BRIDGE

Alla partenza tutti mettono il proprio bridge ID come ipotetico Root ID poi man mano che si scambiano queste informazioni (BPDU) si individua il root bridge e si individua lo spanning tree ottimale ovvero quello che ha i cammini più corti tra i vari nodi che significa, cioè di costo minore (link ad alta velocità/Capacità trasmissiva migliore).

CALCOLO DEL COSTO PATH

Il costo è funzione della capacità di ciascun link ed è la somma di tutti i link attraversati da qualsiasi nodo al root bridge. L’amministratore di rete può modificare il costo dei link sovrascrivendolo e quindi scegliere un determinato cammino.

SPANNING TREE: FUNZIONAMENTO

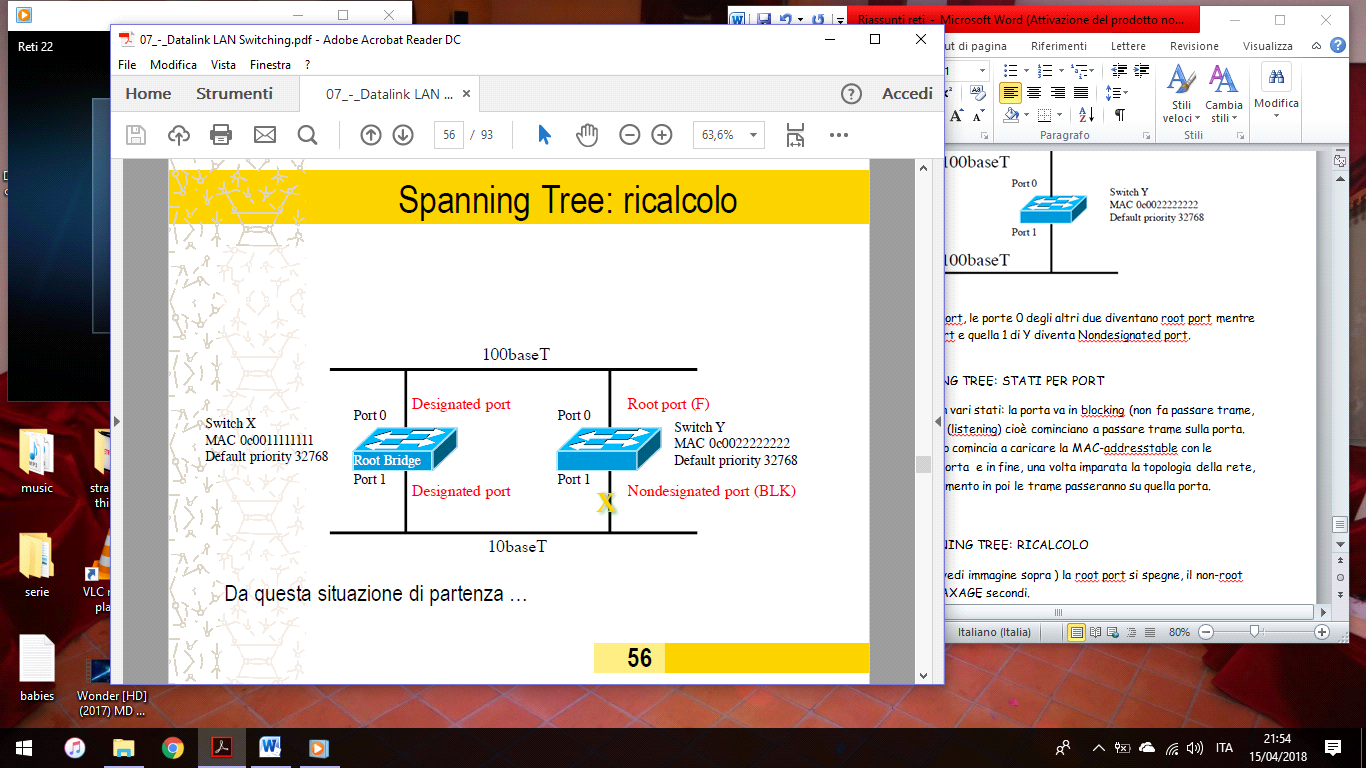


La porta 0 di Z diventa Designated port, le porte 0 degli altri due diventano root port mentre la porta 1 di X diventa Designated port e quella 1 di Y diventa Nondesignated port.

SPANNING TREE: STATI PER PORT

Nello spanning tree la porta transita in vari stati: la porta va in blocking (non fa passare trame, ma le BPDU sì) poi si mette in ascolto (listening) cioè cominciano a passare trame sulla porta. Successivamente va in learning ovvero comincia a caricare la MAC-addresstable con le corrispondenze indirizzo sorgente – porta e in fine, una volta imparata la topologia della rete, la porta va in forwarding e da quel momento in poi le trame passeranno su quella porta.

SPANNING TREE: RICALCOLO



Dalla situazione iniziale di topologia (vedi immagine sopra) la root port si spegne, il non-root bridge non riceve più BPDU per un MAXAGE secondi, passato questo tempo il root bridge non c’è più. Si rielegge il root bridge che in questo caso è l’unico rimasto e così le sue due porte diventano entrambe designated.

VIRTUAL LANS (VLAN)

Da un unico dominio di brodcast lo si va a segmentare in tanti domini, questo fa crescere ulteriormente le dimensioni della rete. Per fare ciò si usa la Virtual LAN ovvero un insieme di porte dello switch confinate nello stesso dominio di broadcast, in modo tale che se una macchina del gruppo A manda un broadcast quest’ultimo sarà ricevuto solo dalle macchine del gruppo A. Si ha l’effetto di trasformare uno switch in tanti switch virtuali ognuno dei quali con un dominio distinto.

FUNZIONALITA’ DI VLAN

Ad ogni VLAN gli verrà associato un numero. Ogni VLAN logica è equivalente a un bridge fisico, cioè se per esempio di ha uno switch a 12 porte e si hanno 3 VLAN, lo switch diventerà virtualmente 3 switch con 4 porte ciascuno. Quindi se si manda un broadcast sulla porta 1 verrà replicato solo sulla porta 2, 3, 4. A livello datalink non si vedono tra di loro, si vedono solo a livello di rete. Per garantire che la VLAN passi da uno switch all’altro (per es. nelle gerarchie) si dedica una porta speciale per interconnete due switch e far passare la VLAN che si chiama Trunk port o tagget port.

MODALITA’ DI ASSOCIAZIONE

Ci sono due possibilità per associare le macchine alle specifiche VLAN: statica e dinamica.

In quella statica ogni porta fisica l’associo a configurazione a determinate VLAN (associazione per Port VLAN). In quella dinamica vado a specificare che un determinato MAC-address deve andare su una VLAN per fare ciò c’è un server che si chiama VMPS server (vlan management protocol server). Si usa solitamente l’associazione per porta che è molto più efficiente dell’altra. Ci sono due tipi di collegamenti: collegamenti di accesso che sono associati ad una e una sola VLAN, poi la seconda tipologia di collegamenti trunk.

VLAN TAGGING

Quando una trama deve uscire da uno switch ed entra in un altro si deve aggiungere il campo tag alla trama che è la VLAN di appartenenza. I protocolli per identificare le trame sono due: ISL(proprietario) – inter stitch link: è un protocollo che ha inventato CISCO per le macchine CISCO, scarsa interazione; l’altro è IEEE 802.1 Q.

TAGGING DI TRAME: I TRUNKS

I collegamenti tra switch sono gestiti in ASIC e trasportano le informazioni relativi alle VLAN. Questa cosa non è intrusiva perché la info alla trama è taggata in uscita e staggata appena ritorna nello switch. Le info dei tag viaggiano solo su collegamenti trunk.

ISL

È un protocollo che si basa sull’incapsulamento; non modifica direttamente la trama, ma incapsula la trama aggiungendoci una testata e una coda. Nella testata ci sono vari elementi come l’ID di una VLAN e le BPDU. Le VLAN non hanno vincoli sul loro ID tranne quello che non posso usare 1 poiché quella è la VLAN management che si utilizza per tutte le attività di gestione dello switch stesso.

IEEE 802.1Q

È più “sporco”, ma allo stesso tempo più redditizio; perché piuttosto che incapsulare modifica semplicemente la trama andando ad aggiungere una componente che contiene una serie di elementi e sovrascrive il CRC. La nuova componente è costituita da 4 byte: 2 byte per il tag protocol identifier (TPID) in cui si indica che è una trama taggata (info riguardanti le VLAN) e altri 2 per tag control information (TCI) in cui vi è il VLAN ID.

TRUNK NEGOTIATION

Per capire se una porta è trunk ci sono due possibilità; o si configura manualmente o attraverso il DTP (dynamic Trunk protocol). Quest’ultimo serve per l’auto negoziazione del trunk, ovvero quando uno switch riconosce che c’è un altro switch prova a negoziare un trunk.

VLAN TRUNKING PROTOCOL (VTP)

Si possono usare i protocolli di trunking anche per far passare altre informazioni che si utilizza per risolvere un problema. Per ogni switch non solo si vanno a configurare le porte, ma si va anche a replicare la stessa VLAN (ad esempio se assegno a una VLAN il num 100, su qualsiasi switch fanno riferimento a quella VLAN dovrò assegnare num 100 ) quindi ci si inventa una semplificazione per la configurazione. Si individua uno switch master (magari quello centrale) su cui si configurano le VLAN una volta per tutte e, attraverso un meccanismo automatico (VTP) che sfrutta i trunks, si propagano le configurazioni su tutti gli switch. Con questo nasce il concetto di dominio e si parla quindi di VTP Domain. Il dominio è un insieme di switch che cooperano insieme con le stesse VLAN. Questo funziona solo al livello 2.

VTP: PROPAGAZIONE

Le info si propagano su tutto il dominio finché non si arriva a un oggetto di livello 3 dove vengono stoppate.

VTP: MODALITA’ OPERATIVE

Gli switch posso lavorare in 3 modalità: server, client e trasparent. Il server è il capo, dove si configurano le VLAN, gestisce il dominio e propaga le info. Il client riceve le info e le carica sul proprio VLAN database, mentre il trasparent non partecipa al dominio (quindi è indipendente e posso creare anche delle VLAN), ma inoltra in maniera trasparente le info inviate dal server.

VTP ADVERTISEMENTS

Il severs manda gli annunci come trame multicast:periodicamente (ogni 5 minuti) o su base richiesta o in presenza di modifiche.

SWITCHING TRADIZIONALE: LAYER 2 SWITCHING

Quando si parla di VLAN e di switching tradizionale si è a livello 2, quando si hanno problemi di scalabilità subentra il livello 3.

PROBLEMI DI SCALABILITA’ INTER-VALAN/ IL TRUNKING RISOLVE

Per ovviare al problema della scalabilità si fa parlare al router 801.Q, piuttosto che avere un interfaccia associata a ciascuna VLAN agganciata a un interfaccia del router con uno specifico indirizzo (dominio di broadcast differente) si avrà una sola interfaccia nello switch che porta le info su tutte le VLAN che si comporta come un trunk . Si avranno delle interfacce virtuali che saranno sotto interfacce di quella reale.

ROUTER ON A STICK

È l’escamotage di avere più interfacce virtuali per una reale, così risolvo il problema di scalabilità perché non ho il limite di interfacce virtuali. La fregatura è che se prima ad esempio avevo 3 interfacce con un giga ora si avrà una VLAN con interfaccia giga su cui ci deve passare il colloquio di tre VLAN quindi si ha la suddivisione del giga. Per questo motivo questa soluzione si fa su interfacce di capacità superiore.

UNA PRIMA EVOLUZIONE: LAYER 3 SWITCHING

Router on sitck scala bene solo fino a un certo punto, quindi bisogna introdurre un aiuto hardware per risolvere il problema. Si collega direttamente la parte interna del router alla fabric così le VLAN si parlerebbero ad altissime prestazioni. L’oggetto hardware si chiama Layer 3 Switching, quest’ultimo integra nella fabric(livello 2) un dispositivo di livello 3 quindi aggiunge delle funzionalità di livello 3. Quindi questo dispositivo permette di gestire la qualità del servizio, la sicurezza, controlli di flusso ed ecc. Per funzionare bene questa cosa deve essere fatta in hardware based.

DOMANDA D’ESAME: differenza tra router e switch layer 3? Lo switch di layer 3 è collegato direttamente con la fabric e quindi è tutt'uno con lo switch; è limitato dal punto di vista protocollare (parla un solo protocollo), ma è molto più capace. Il router parla diversi protocolli e non fa parte della fabric è collegato tramite interfaccia.

ANCORA MEGLIO: LAYER 4 SWITCHING

Si implementano switch layer 3 con funzionalità a livello di trasporto quindi si parla di Layer 4 Switching.

IL MODELLO GERARCHICO A 3 LIVELLI

Il livello di accesso eroga la connettività in rete agli utenti finali. In questo livello si trovano apparati di piccola capacità con un numero limitato di porte, che faranno una micro segmentazione della rete dove si andranno a configurare le VLAN e si può fare anche un po’ di filtraggio sul mac-address. Tipicamente in questo livello si lavora o in banda Shared o Switched. Per connettere questi apparati tra di loro si avranno degli apparati di raccolta/distribuzione. Il livello distribution separa accesso e core e garantisce le funzioni di raccolta e controllo al core. Questo è il livello più importante e più intelligente. Si hanno apparati che operano a livello 3. In questo livello: sono definiti i domini di broadcast, vengono configurate le VLAN, viene gestita la sicurezza e il controllo accessi, viene effettuata la manipolazione delle trame.

Tutti questi apparati si andranno a connettere al Core, che sono apparati poco intelligenti, ma con grande capacità di commutazione. In questo livello si ha la necessità di aggregare grandi volumi di traffico e di commutare ad alta velocità.

SWITCH BLOCK

È il blocco fondamentale che costituisce l’infrastruttura. Questo è costituito da una componente di accesso e una di distribuzione. Tanti switch block si mettono insieme e si connettono al core. In questi switch block c’è molta ridondanza quindi non ci sono i single point of falitures.

CORE BLOCK

Si mettono tanti switch block insieme attraverso un core block. Il traffico tra switch

blocks deve transitare attraverso il core block. Anche nel core block ci sono almeno due dispositivi. Tutta questa ridondanza produce cicli, ma lo spanning tree risolve questo problema.

COLLAPSED CORE

È una topologia semplificata. Dove non c’è la necessità di implementare due livelli distinti tra core e distribuzione si vanno a collassare in un solo livello cioè nel livello di distribuzioni si farà anche il core. Anche in questo caso si ha la ridondanza.

DUAL CORE

Sempre per la ridondanza si possono andare a combinare i collapsed core e questo si chiama dual core; si ha un doppio livello di core.

ADSL

È un modo di utilizzare strutture nate a capacità inferiore con delle tecniche a multiplazione intelligente sfruttate al massimo della loro potenzialità. Il doppino nato a 4KHz raggiunge il MHz. Con la logica della multiplazione si divide lo spettro in 256 canali da 4 KHz (kilo hertz): Il canale 0 viene riservato per la telefonia; i successivi 4 canali non vengono utilizzati per evitare problemi di interferenza tra la trasmissione dati e quella telefonica; i restanti canali vengono destinati al traffico dati. Alcuni per il traffico uscente (upstream), altri per il traffico entrante (downstream). Questo lavoro è svolto dal modem o router ADSL che riceve i dati da trasmettere e li splitta in flussi paralleli da trasmettere sui diversi canali e utilizzerà la QAM (quadratura amplitude modulation) e li modula in frequenza.

GLI STANDARD ADSL

È standardizzato dall’ ANSI mentre ITU-T ha prodotto una raccomandazione su ADSL che si chiama G. 992.1.

SUDDIVISIONE DEI CANALI NELL’ADSL

L’ampiezza di banda disponibile viene divisa 4 canali 0 e tutti gli altri sono disponibili. Ogni canale è una portante modulata in QAM, però si lavora su frequenze diverse.

I canali da 26 a 138 destinati al traffico in upstream e gli altri canali destinati al downstream. Quando si parla di ADSL si parla di asimmetrico infatti si ha una asimmetria tra upstream e down stream.

ARCHITETTURA DI ACCESSO ADSL/ADSL LITE

Si ha la stazione, si ha il modem ADSL che serve a fare la modulazione a fasciamento e un oggetto che fa da splitter (divide la parte telefonica da quella dati). In centrale si hanno due apparati diversi; la parte telefonica va a finire su una scheda, mentre la parte dati va a finire su un oggetto che si chiama DSLAM (DSL access multiplexer) che multipla tutt’un insieme di utenze DSL, le mette insieme e le porta verso la rete del gestore, ultimamente però questa cosa non viene fatta più in centrale, ma nei cabinet.

FIBRA NELLA RETE DI ACCESSO(FTTx)

Esistono molte soluzioni, in cui la fibra arriva fino ad un certo livello di “profondità” (vicinanza all’utente); da quel punto il collegamento prosegue in rame.

Con queste tecnologie cambia anche l’ADSL, ad esempio il canale 0 non viene utilizzato più per la telefonia, ma si utilizza il VOIP risparmiando così tutti gli apparati in centrale dedicati alla telefonia. Questa soluzione si chiama FTT Curb o Cabinet.

Ci sono soluzioni più moderne come FTTB cioè la fibra nel palazzo.

RETI WIRELESS

Stanno avendo successo per motivi di flessibilità e risolve tutti i problemi dovuti alla necessità di un cablaggio. Le wireless utilizzano le bande ISM (cioè intorno ai 2.4 e ai 5 GHz) che sono bande utilizzate anche per apri cancelli, telecomandi; non sono frequenze licenziate, non si può pretendere nulla, nessuna garanzia di non interferenza.

VANTAGGI DEL WIRELESS

Costi abbastanza ridotti, meno problemi relativi alle distanze, mobilità delle stazioni.

STANDARD 802.11X

L’IEEE ha definito diversi standard nel corso del tempo per le trasmissioni wireless. Si è partiti dal IEEE 802.11 liscio fino ad arrivare a 802.11ac che servono a realizzare trasmissioni con capacità e prestazioni migliori.

TECNICHE A DIVISIONE DI SPETTRO

Tutte le reti wireless utilizzano tecniche a divisione di spettro (SST). Il vecchio standard (802.11) lavora ancora con il Frequency Hopping SS; mentre ormai tutte le tecnologie lavorano in logica Direct Sequence SS o spettro espanso in sequenza diretta. In quest’ultima si introduce molta ridondanza ottenendo un’occupazione di banda più del necessario, però aumenta l’immunità al rumore e la sicurezza della comunicazione.

STRATO FISICO PER LE RETI 802.11

Con la tecnologia Frequency Hopping la trasmissione salta, ad intervalli temporali definiti, da una frequenza ad un’altra secondo una sequenza pseudocasuale nota a tutti. È abbastanza solida contro il multipath fading, cioè quando arriva il segnale riflesso la ricezione è già

spostata su un altro canale.

STRATO FISICO PER LE RETI 802.11 (DSSS) /SPREAD SPECTRUM

Si passa ad una codifica più intelligente. Si allarga lo spettro del segnale mettendolo in or esclusivo con una sequenza di Chipping (se si ha una sequenza di chipping di lunghezza x ogni bit sarà moltiplicato per x). Quando il segnale viene letto si fa il processo inverso, si fa una correlazione e si ricostruisce il segnale originario.

La banda disponibile è divisa in 14 canali di 5 MHz, a partire da 2.412 GHz; le stazioni debbono essere configurate per determinare il canale utilizzato; non tutti i canali sono disponibili in tutti i paesi.

CANALI DSSS

Si passa di 5 canali in 5 canali per evitare interferenze. Quindi si possono utilizzare solo 3 canali simultaneamente.

DS VS FH

Il vantaggio del DSSS è che si aggiunge molta ridondanza quindi immuni ai rumori, non è molto sicura e c’è uno spreco di banda. Lavora a 11 Mbps.

FHSS è più sicura, però molto limitata in banda (1 MHz) ed è impossibile usarla nel WI-FI ad alti bit-rate.

DYNAMIC RATE SHIFTING

Fallback : capacità di ridurre la capacità trasmissiva quando la potenza del segnale crolla. Si effettua ciò anche quando la potenza del segnale è forte, ma c’è molto rumore.

Data Rates adattati automaticamente alla natura del canale quando c’è rumore o per le grandi distanze e del carico.

802.11 b lavora con una codifica a 8 chip e permette di lavorare fino a 11mbps. È stata la prima ad introdurre il DSSS High Rate. Per trasmettere a velocità leggermente più superiori è nato 802.11 a, che è importante perché da 11 si è passato a 54 mbps utilizzando OFDM. L’altra novità è che ha cambiato range di frequenze, si è spostata nella sezione alta della banda ISM intorno ai 5GHz. Il vero salto di qualità è stato 802.11g i successivi sono innovazioni tecnologiche di questo. 802.11g ha risolto i problemi introducendo OFDM anche sulla 2.4 GHz. Tutti questi standard riescono a fare il Dynamic Rate Shifting. Gli standard più evoluti 802.11 n e ac hanno introdotto una tecnologia che si chiama MIMO, cioè la possibilità di utilizzare più antenne simultaneamente in modo da parallelizzare le trasmissioni, aumentando drasticamente la banda disponibile.

CSMA: STAZIONE NASCOSTA

Consideriamo tre stazioni A, B e C tali che B sia a portata di A e di C, ma A e C non possano rilevare le rispettive trasmissioni perché sono in celle diverse.

Se C sta trasmettendo dati a B, A non potrà rilevare l’occupazione del canale in quanto è fuori portata, A inizierà a trasmettere ed il suo segnale arriverà a B interferendo con i dati

che C sta trasmettendo; questo è detto problema della stazione nascosta. Se una stazione è fuori dal raggio di copertura non riesce a percepire una trasmissione che è stata iniziata da un’altra e quindi non percepisce un’eventuale collisione.

CSMA: STAZIONE ESPOSTA

Supponiamo che A stia trasmettendo verso un’altra destinazione e che B(sta nel range di A) desideri inviare dati a C. B ascolta il canale e lo trova occupato, quindi non trasmette; in realtà il canale sarebbe disponibile (nella ipotesi che la destinazione della trasmissione di A sia fuori dalla portata di B) perché in C i segnali non interferirebbero: questo è il problema della stazione esposta.

MACA

Per rendere efficace la logica CSMA nonostante le interferenze la soluzione è la MACA (Multiple Access with Collision Avoidance). Quando un trasmettitore ha bisogno di trasmettere, chiede l’autorizzazione a trasmettere (RST: Request to Send); manda al ricevente un messaggio di RST con la durata della trasmissione, cioè la lunghezza del frame. Il ricevitore trasmette un frame di conferma (CTS: Clear To Send) che contiene le stesse info del RST. Appena il trasmettitore riceve il CTS può avviare la trasmissione dei dati. Visto che si lavora in BMA il RST è inviato a una determinata stazione, ma lo vedono tutte le stazioni che sono nel raggio di copertura del trasmittente. Le stazioni nascoste non vedono il frame RTS, ma vedono il frame CTS, quindi sanno che trasmesso il CTS il ricevitore dovrà ricevere il frame di dati, di lunghezza specificato nel CTS; queste stazioni attenderanno senza trasmettere per il tempo necessario alla trasmissione del frame del trasmettitore (che loro non vedranno in quanto nascoste, ma sanno che ci sarà). Nel caso in cui una coppia di RST viene mandato contemporaneamente verso una destinazione collocata nel campo di ricezione dei due trasmittenti entrambi i frame andranno in collisione e andranno persi. In questo caso non ci sarà il CST e quindi si capirà che c’è stata una collisione. Allora si applica l’algoritmo di backoff esponenziale binario.

EXPONENTIAL BACKOFF ALGORITHM 1

Ogni stazione sceglie un numero random (*n*) compreso tra *0* e *m*. Attende (*n* x *slot time*) prima di riprovare; ad ogni collisione *m* aumenta in maniera esponenziale. La lunghezza dello slot time deve essere definita in maniera tale che ciascuna stazione possa determinare se un’altra ha avuto accesso al canale nello slot precedente; questo riduce le collisioni.

EXPONENTIAL BACKOFF ALGORITHM 2

È eseguito nei casi in cui si trova il mezzo occupato, dopo ogni ritrasmissione e dopo una trasmissione andata a buon fine. Non viene eseguito quando una stazione trasmettitrice trasmette un nuovo pacchetto ed il mezzo è libero. Si ricorre a questo algoritmo per rendere la rete più tollerante a fenomeni di conflitto

MACAW

Introduce migliorie specifiche per le applicazioni wireless. È stato introdotto l’utilizzo di frame di ACK con meccanismo stop-and-wait, quindi si ferma finché non riesce a trasmettere. Si è modificato l’algoritmo di backoff in modo da applicarlo separatamente ai diversi flussi trasmissivi.

SI PASSA A LIVELLO 3

FUNZIONI DELLO STRATO DI RETE

A livello 3 si trova l’intelligenza della rete. Lo strato di rete ha quindi come funzione quella di fornire allo strato di trasporto un servizio per la consegna dei dati in modo da mascherare l’infrastruttura della rete (la sottorete). Nel livello 3 si introduce la logica dell’indirizzamento universale, cioè anche al difuori del singolo datalink le macchine si devono vedere. Gli elementi del livello di rete sono gli host, i router (protagonisti delle azioni in questo livello) e pacchetti.

Lo strato di rete dovrà quindi occuparsi di:

– determinare quale tragitto tra quelli disponibili dovranno seguire i dati (instradamento, routing), questo può richiedere che lo strato di rete conosca la topologia della rete;

– reagire a modifiche di topologie della rete; se esiste un meccanismo dinamico per l’apprendimento della topologia, questo permetterà di apprenderne anche le modifiche nel tempo;

– evitare di sovraccaricare linee quando sono disponibili percorsi alternativi (congestione);

– risolvere i problemi connessi al transito attraverso reti differenti (internetworking).

CONNECTION ORIENTED O CONNECTIONLESS?

L’instradamento può essere fatto sia in logica connection oriented che connectionless.

Inizialmente OSI prevedeva che lo strato di rete fornisse solo un servizio connection oriented, in seguito c’e’ stata forte richiesta di introdurre nello standard

anche un servizio connectionless, e così è stato fatto.

INSTRADAMENTO CONNECTIONLESS

Il servizio senza connessione richiede che i pacchetti siano instradati indipendentemente uno dall’altro. Generalmente un router dispone di una tabella (routing table) che definisce su quale linea di uscita debba essere trasmesso un pacchetto in base alla destinazione finale: il router riceve il pacchetto, lo memorizza per analizzarlo, quindi lo trasmette in base alla tabella (store and forward). Ogni pacchetto deve quindi contenere l’indirizzo di destinazione; poiché le tabelle possono modificarsi nel tempo, non è detto che tutti i pacchetti seguano la stessa strada. Il routing è destination based.

INSTRADAMENTO CONNECTION ORIENTED

L’idea di base è di associare ad una connessione un circuito virtuale nella sottorete.

Si definisce a priori – durante la fase di inizializzazione della connessione – la

sequenza di router che i pacchetti dovranno attraversare; quindi tutti i pacchetti appartenenti alla stessa connessione seguiranno la stessa strada. L’instradamento del pacchetto sarà quindi fatto in base alla sua appartenenza ad una connessione e non alla sua destinazione finale.

CONNECTIONLESS VS. CONNECTION ORIENTED

Con la connectionless non è necessario un circuito, mentre con connection oriented sì; per l’indirizzamento nel primo si deve essere attenti ad ogni pacchetto abbia il proprio indirizzo sorgente e destinazione e agire in base all’indirizzo di destinazione, per il secondo non è necessario serve solo il numero di Virtual Circuit; per quanto riguarda lo stato connectionless non conserva nessuna informazione di stato(ogni pacchetto vive di vita propria), nell’altro caso si hanno delle tabelle che definiscono le associazioni che definiscono i percorsi; per l’instradamento il con.less è indipendente mentre in con. Oriented viene scelto all’inizio; i guasti nel caso di con.less non ci sono mentre con. Oriented se ci sono dei guasti bisogna ricostruire i percorsi; il controllo della cogestione nella prima logica è complesso mentre nella seconda è semplice.

INSTRADAMENTO ED INOLTRO

Al livello di rete si fa l’instradamento. Si possono distinguere due operazioni:

– Inoltro (forwarding): il processo che, in base all’indirizzo di destinazione o al circuito virtuale, sceglie la linea di uscita in funzione di dati noti (tabelle, stato delle linee, …). Si prende un pacchetto da un’interfaccia e si manda su un’altra interfaccia. La scelta di quale interfaccia su cui fare l’inoltro è delicata, perché condiziona il buon andamento dei pacchetti nella rete. C’è una tabella (routing table) che sulla base delle informazioni della destinazione del pacchetto permette di individuare l’interfaccia candidata per l’invio del pacchetto verso quella destinazione. Quest’attività deve essere veloce ed efficiente, è supportata da elementi hardware.

– instradamento: individuazione di percorsi multipli e complessi sulla rete per individuare la strada che deve fare un pacchetto dall’origine a destinazione, questa strada è costituita da multipli passi di forwarding. Si deve arrivare ad una convergenza. I nodi da soli si scambiano le info circa le destinazioni raggiungibili attraverso di esse (annunci di raggiungibilità), con questi annunci viene caricata automaticamente la base di conoscenza che permette di fare forwarding (tavola di routing ) di ciascun nodo intermedio. In questa maniera, ovvero condivisa vengono costruiti i percorsi sulla rete.

Se tutte le tavole di instradamento di una rete dei nodi di commutazione intermedi sono popolate in maniera coerente, cioè arrivano a convergenza , su quella rete si potranno raggiungere qualsiasi punto da qualsiasi punto.

Piano di controllo -> algoritmi e protocolli che prevedono lo scambio delle info di raggiungibilità.

Piano di commutazione -> forwarding puro.

Nelle funzionalità di un router troviamo funzionalità control plane e funzionalità di livello basso (forwarding plane).

CARATTERISTICHE DI UN ALGORITMO DI ROUTING

Un algoritmo di routing dovrebbe avere una le seguenti caratteristiche:

-correttezza;

-semplicità: meno oggetto di errori, di complessità, meno impegnativo dal punto di vista computazionale;

-robustezza: l’algoritmo deve poter far fronte alle modifiche di topologia;

-stabilità: una volta raggiunta la convergenza deve cercare di restare stabile per più tempo possibile;

-imparzialità: teoricamente la rete dovrebbe trattare tutti i pacchetti allo stesso modo (nella realtà questo vincolo viene un po’ violato);

-ottimizzazione: le decisione prese devono essere ottimali. Sia per il cliente (massima qualità possibile) che per il provider (bilanciare il carico su tutti i circuiti disponibili).

INTERNET PROTOCOL(IP)

Unico protocollo a livello di rete, è standardizzato e promulgato dalla IETF definito negli RFC 791 e 1122.

Caratteristiche:

-Ha funzione di recapito ma in totale inaffidabilità. Infatti non garantendo affidabilità, controllo di flusso, sequenza di pacchetti e rilevazione o correzione di errori, vince proprio perché ha comunque dimostrato di essere totalmente scalabile, efficiente e flessibile per quanto riguarda l’enorme quantità di variazioni topologiche presenti su Internet.

IP ha la funzione di recapitare un insieme di bit (internet datagram) dalla sorgente alla destinazione attraverso un sistema di reti interconnesse.

-Il recapito viene operato direttamente se la destinazione appartiene alla stessa

rete della sorgente, attraverso un sistema intermedio (router). Se possibile il datagramma viaggia intero, altrimenti viene spezzato in più parti, ciascuna trasportata poi individualmente; in questo caso il datagramma viene riassemblato a destinazione.

– Ip si preoccupa di trasmettere il datagramma da un host all’altro, fino alla

destinazione, una rete alla volta

• Questa definizione corrisponde ad un protocollo che fornisce un servizio

connection less inaffidabile.

INDIRIZZAMENTO IP

Per poter identificare un dispositivo, IP assegna a ciascun network attachment point(interfaccia di connessione alla rete del dispositivo) un identificativo, un indirizzo IP, univoco e costituito da 32 bit. Per gestire questo processo che garantisce univocità bisogna strutturare la gestione dello spazio di indirizzamento tramite una logica gerarchica.

E’ una gerarchia a due livelli in cui ciascun indirizzo è costituito da due componenti:

una che individua la rete (indirizzo di rete) ed un’altra host nella rete (indirizzo di rete). Tutti i nodi IP hanno un ulteriore indirizzo, detto loopback, che rappresenta

un indirizzo fittizio indicante “se stesso”, utilizzato per simulare connessioni di rete di un host con se stesso.

STRUTTURA DELL’INDIRIZZO IP

L’indirizzo IP e’ costituito da una sequenza di 32 bit, o 4 byte, generalmente rappresentati da 4 numeri decimali di valore compreso tra 0 e 255, separati da un punto. Una parte ne individua la rete mentre un’altra ne identifica l’host all’interno della rete.

PACCHETTO IP

Il pacchetto IP e’ costituito da una testata di 20 byte alla quale si aggiunge una parte opzionale (fino a 40 byte di opzioni con un tot di 60 byte di testata).

Sono presenti una serie di campi di lunghezza fissa (tranne per le opzioni):

•Il campo version contiene il numero identificativo della versione di IP;

•Il campo IHL (4 bit) contiene la lunghezza della testata. Indica quanto è lungo l’header in parole di 32 bit (quindi un massimo di 60 byte complessivi);

• Il campo type-of-service serve ad indicare diverse classi di

servizio (precedenza del pacchetto, basso ritardo, etc.), di solito ignorato dai router

• total-length indica la lunghezza totale del pacchetto in byte, che ha un valore massimo di 65535 (64k)

PACCHETTO IP: FRAMMENTAZIONE

I campi identification, DF, MF e fragment-offset sono dedicati alla frammentazione.

Un pacchetto IP può essere grande fino a 64k ma poi deve essere incapsulato nella trama di datalink che potrebbe avere una dimensione fissa. Un pacchetto è possibile che quindi non entri nella trama e a questo punto deve essere spezzato. E’ in questo caso che si parla di processo di frammentazione. Sono pacchetti IP indipendenti che alla fine sono ricomposti END TO END.

– il bit MF (More Fragments) viene impostato a 0 nell’ultimo frammento (o nel datagramma se non viene frammentato), ad 1 altrimenti

– il bit DF (Don’t Fragment) viene impostato ad 1 se il datagramma non deve essere Frammentato

– ogni datagramma IP inviato da una sorgente ha un numero identificativo differente

dagli altri, riportato nel campo identification

– se un datagramma viene frammentato, ogni frammento contiene nel campo

identification lo stesso valore, mentre nel campo fragment-offset viene indicata la

posizione del primo byte del frammento.

• in base all’identification la destinazione puo’ raggruppare i diversi frammenti, in base a

total-length ed agli offset, la destinazione puo’ valutare se si fossero persi frammenti del

datagramma.

PACCHETTO IP (cont.)

Il campo time-to-live è un meccanismo di protezione della rete che serve a garantire che i pacchetti non vadano all’infinito. E’ un numero identificativo numerico che mi caratterizza il numero max di passaggi da un router all’altro che il pacchetto può fare per arrivare a destinazione. Ogni router che fa il suo passaggio, prima di mandarlo avanti lo decrementa, quando arriva a zero il pacchetto viene cancellato. Garantisce che il pacchetto arrivi a destinazione.

Il campo protocol, indica il protocollo di livello superiore a cui sono destinati i dati del pacchetto.

Il campo checksum, controllo sulla testata (header).

Source e destination address contengono gli indirizzi a 32 bit del sorgente e del

destinatario del pacchetto.

Pacchetto IP(cont. II)

Le opzioni aggiuntive della testata si dividono tipicamente in tre settori:

-opzioni di sicurezza: che permettono di classificare il pacchetto come “non classificato” con conseguente trattamento poco speciale, oppure “top secret” usata in ambiti militari.

-record route: mi serve per conservare il path del pacchetto infatti istruisce i router a registrare il loro indirizzo nei successivi campi opzionali via via che il pacchetto transiti in rete.

-sourse routing: può essere loose o strict; tipicamente l’instradamento è basato sullo scambio di informazioni tra nodi, in questo caso invece si può inserire uno specifico percorso definito dalla sorgente, questa operazione può essere forte(strict) in cui DEVO compiere quel percorso o debole (loose) POSSO compiere quel percorso. E’ poco usato in quanto non ottimale dal punto di vista della sicurezza.

INDIRIZZI IP

Sono divisi gerarchicamente in due parti, il prefisso ne indica la rete mentre il suffisso si riferisce all’host/interface. Un indirizzo IP identifica una connessione computer-rete. E’ totalmente indipendente dal MAC ADDRESS. E’ rappresentato da un blocco di 32 bit rappresentato in binario infatti se scritto in decimale ogni elemento verrà tradotto in binario e riportato nell’ottetto corrispondente nel blocco di 32 bit.

CLASSI DI INDIRIZZI

Chi definisce qual è la parte dedicata alla rete o all’host?

DUE MECCANISMI: classfull e classless.

Gli indirizzi IP sono raggruppati in diverse categorie, dette classi.

Le classi sono 5 ma le più importanti sono la Classe A, Classe B e Classe C.

-indirizzi di classe A:

riconosciuti dal primo bit, se 0 ha valore compreso tra 0 e 127.

ES. l’indirizzo 20.9.0.200 individua l’indirizzo appartenente alla rete “20”, il cui

indirizzo di host e’ 9.0.200.

-Esistono 126 valori per la classe A in quanto le reti 0 e 127 non possono assolutamente essere utilizzate.

Ciascuna rete di classe A può indirizzare 2 alla 24 host differenti;

-indirizzi di classe B:

riconosciuti dalla sequenza di bit 10 ho valori compresi tra 128 e 191, di conseguenza i primi 16 bit costituiscono l’indirizzo di rete e gli ultimi 16 l’indirizzo di host.

Ho a disposizione quindi 65536-2 host.

-indirizzi di classe C:

primo bit ad 1, secondo ad 1, terzo a 0 con il primo byte di valore compreso tra 192 e 223.

Ho 3 byte per la rete e solo 1 per l’host.

Ho reti più piccole che possono indirizzare fino a 2 alla otto meno 2 host possibili.

-indirizzi di classe D:

indirizzi riservati, individuata guardando fino al quarto bit in quanto abbiamo una sequenza di tre uni ed uno zero “1110”, con il primo byte compreso tra 224 e 239.

Sono tipicamente riservati ai casi multicast.

-indirizzi di classe E: (non si usa in quanto classe di ricerca e sperimentazione)

E’ una classe sperimentale costituita dalla sequenza di bit “1111” con primo byte tra 240 e 255.

INDIRIZZI SPECIALI

-L’indirizzo contenente tutti “0” nel campo di host viene utilizzato per indicare la rete;

-L’indirizzo 0.0.0.0 ha significato di “questo host di questa rete”, è indirizzo di rete associato a se stesso, è utilizzato in fase di boot dai calcolatori che non conoscono ancora il proprio IP;

-L’indirizzo 255.255.255.255 (con tutti i bit 1) è l’indirizzo local broadcast (broadcast della rete locale);

-L’indirizzo con tutti 1 nel campo host rappresenta l’indirizzo broadcast della rete specificata nel campo rete. Questo caso mi serve in quanto mi permette di indirizzare un pacchetto a

tutti gli host di una rete remota (che quindi non è la mia).

INDIRIZZI DEDICATI A SCOPI SPECIALI

• La rete di classe A 127.0.0.0 e’ dedicata all’interfaccia di loopback.

• Tre range di indirizzamento stabiliti dalla RFC 1918 sono dedicati ad indirizzi privati

– 10.0.0.0 (una rete di classe A)

– da 172.16.0.0 a 172.31.0.0 (16 reti di classe B)

– da 192.168.0.0 a 192.168.255.0 (256 reti di classe C)

Perché esiste questa classificazione?

E’ un meccanismo di protezione infatti la RFC ci impone, nonostante la macchina me lo consenti, di non occupare qualsiasi indirizzo.

Gli indirizzi privati possono essere utilizzati all’interno di una rete privata, ma non

devono mai venire annunciati nelle tabelle di routing

DALLE SLIDE:

Il routing verso le macchine ad indirizzo privato deve essere fatto dal router di

interconnessione con la rete pubblica ad insaputa del resto della rete

– lo scopo degli indirizzi privati e’ quello di poter utilizzare la tecnologia TCP/IP in una realta’

locale senza dover necessariamente chiedere ed utilizzare indirizzi pubblici

– una tecnica diffusa che fa uso di questi indirizzi per dare connettivita’ senza sprecare indirizzi

pubblici e’ il NAT (Network Address Translation) che vedremo in seguito

ASSEGNAZONE DEGLI INDIRIZZI IN INTERNET

L’assegnazione è svolta gerarchicamente:

L’ ICANN è un organismo che gestisce tutto lo spazio di indirizzamento ma delega blocchi specifici a determinate organizzazioni regionali(Europa, America…) che riassegneranno di conseguenza nel loro interno delegando altri enti (Europa: RICE NCC/Italia:GARR)

Perché questa divisione? Per tener limitata la dimensione delle tavole di routing.

L’ICANN è l’autorità centrale che garantisce l’unicità delle assegnazioni degli indirizzi per Internet

CARENZA DI INDIRIZZI (NON L'HA SPIEGATO)

Lo spazio di indirizzamento disponibile conta due miliardi di indirizzi, raggruppabili in 16500 reti di enormi dimensioni e 2 milioni di reti di piccole dimensioni

Sembrava impossibile esaurire lo spazio di indirizzamento, ma la 100000-sima rete si è connessa in Internet nel 1996.

Tre i fattori che hanno determinato l’insorgere di problemi:

– lo spazio di indirizzamento delle classi A, e spesso anche quello delle classi B, è troppo vasto: nessuna rete può contenere 16 milioni di nodi distinti, o anche solo

65000; un enorme numero di indirizzi rimangono inutilizzati, una azienda o campus a cui è stata assegnata una classe A che deve estendere la sua rete per interconnettere diversi dipartimenti su reti locali distinte hanno bisogno di altre reti, benchè il numero di indirizzi disponibile ecceda di gran lunga la necessità di

indirizzi di host;

– la connessione punto-punto tra due router richiede l’utilizzo di una rete IP, per la quale sono utilizzati solo due indirizzi

– lo spazio di indirizzamento delle reti di classe C risulta troppo piccolo con il

crescere delle reti locali.

CALCOLO INDIRIZZI DISPONIBILI IN UNA RETE

Il numero massimo di host dipende dalla classe; la A è la più grande, poi vi è la B ed in fine la C.

SUBNETTING (NON L'HA SPIEGATO)

Per risolvere il problema della carenza di indirizzi è stata sviluppata la tecnica del subnetting. Ad esempio si può suddividere una rete di classe A in gruppi più piccoli. Se per esempio la rete assegnata è la 100.0.0.0 la si può dividere in 100.1.0.0 e in 100.2.0.0, però il router dovrà annunciare verso l'esterno la sola rete di classe A. Per implementare le sottoreti è necessaria un'info aggiuntiva agli indirizzi di rete, che specifichi i quali bit definiscano l'indirizzo della sottorete e quali definiscano gli host.

NETWORK MASK (NON L'HA SPIEGATO)

Si utilizza una "maschera" per identificare quali bit definiscono la rete e quali gli host, costituita da 32 bit. Chiama anche VLSM (Variable Length Subnet Masking) è una tecnica che permette la suddivisione ricorsiva dello spazio di indirizzi di un'organizzazione, al fine di utilizzarlo in maniera più efficiente. Tramite questa pratica, una subnet può essere partizionata in ulteriori subnet, attraverso l'utilizzo di parte dei bit destinati all'host number; si crea così un subnetting a più livelli.

Se un bit della maschera vale 1, il corrispondete bit dell'indirizzo fa parte dell'indirizzo della rete. Se un bit della maschera vale 0, il corrispondente bit dell’indirizzo fa parte dell’indirizzo di host.

Con la maschera si fa and tra la maschera e indirizzo per ottenere la componente network.

Quindi gli indirizzi della classe A hanno maschera 255.0.0.0, quelli di B 255.255.0.0 e quelli della C 255.255.255.0 .

Utilizzando le maschere è possibile sperrare una rete in sottoreti, ad esempio la 100.1.0.0 con maschera 255.255.0.0 indica una rete che può indirizzare gli host da 100.1.0.1 a 100.1.255.254 .

Per indicare la maschera si mette in coda all’indirizzo il numero di bit che costituiscono l’indirizzo di rete, ad esempio la rete 131.154.20.0 255.255.255.0 si indica anche con la notazione 131.154.20.0/24: i primi 24 bit costituiscono l’indirizzo di rete; un altro esempio, la subnet 193.206.144.64 255.255.255.192 si indica con 193.206.144.64/26 (26 bit per l’indirizzo di rete).

Se ad esempio si vogliono indirizzare 6 macchina si avrà una maschera /29 o 255.255.255.248 perchè gli ultimi 3 bit a 0, il primo indirizzo (quello con tutti 0 ) è il network addres, l'ultimo (quello con tutti 1 ) è il broadcast address e i 6 bit intermedi sono tutti utilizzabili .

La sottorete più piccola deve avere almeno un campo di 4 indirizzi: uno per indicare la sottorete, uno per indicare il broadcast, ed almeno uno per indirizzare un host; poiche’ al campo host vanno assegnati un certo numero di bit,

un bit non è sufficiente, quindi ne servono almeno due, che forniscono due indirizzi per host; questa tecnica è utilizzata per assegnare indirizzi di rete alle connessioni punto-punto tra i router, risparmiando il maggior numero di indirizzi possibile.

Si deve gestire lo spazio disponibile in modo che non ci sia frammentazione interna.

Con queste maschere scompare un po' il senso delle classi, ora ad esempio se si referenzia un indirizzo di classe naturale A è semplicemente un indirizzo /8 , per la B è /16 , classe C /24 ,tutte le reti intermedie non avranno più una maschera naturale, basta far avanzare o arretrare la dimensione della subnet mask .

Tutte le netmask ammisibili devono avere il primo blocco (quello che indica la componente network) costituita da un insieme di 1 contingui.

INDIRIZZI BROADCAST PER SUBNETS

L'indirizzo 255.255.255.255 è indirizzo di broadcast della rete locale. Per ottenere il broadcast diretto si fa l'OR tra l'indirizzo e il negato della maschera di rete. Questo indirizzo serve quando si deve mandare un broadcast fuori la rete locale.

AGGREGAZIONE DI RETI

Utilizzando le maschere prolifera il numero di entry in una tavola di routing, questa cosa crea un problema a livello prestazionale dei router. Ogni volta devono andare a cercare l'interfaccia di destinazione, nella fase di forwarding,in una tabella di 10 milioni di entry e questa cosa non va bene.

Per ridurre il numero di possibili entry si ricorre alla tecnica di aggregazione, ovvero facendo l'operazione opposta del subnetting: il supernetting. Si prende un insieme di sottoreti e si aggregano in una sola rete, ad esempio si ha una classe C, che va da 193.206.144.0 a 193.206.147.0 cioè 4 reti a disposizione.

Se si scrivono queste reti in binario si nota che differiscono solo per gli ultimi due bit, ( il valore binario di queste reti è

11000001 11001110 10010000 00000000

11000001 11001110 10010001 00000000

11000001 11001110 10010010 00000000

11000001 11001110 10010011 00000000 ).

Quindi se si prende la maschera naturale /24 e si fa il supernetting si ottiene un aggregato di rete quindi si indica come 193.206.144.0/22, questo /22 rappresenta in un'unica entry un aggregato di 4 entry.

Questa tecnica ha evitato la proliferazione del numero di entry nella tavola di routing e si chiama supernetting o ( in gergo tecnico ) CIDR che sta per Classless InterDomain Routing.

CLASSLESS INTERDOMAIN ROUTING (CIDR)

Per gestire questo nuovo schema di indirizzamento il modo di gestire le tabelle di routing da parte del router deve cambiare, infatti si è introdotto un nuovo standard col nome di CIDR.

Secondo questo standard ogni record della tabella di routing specifica l’indirizzo della destinazione con la sua maschera.

Problema potenzialmente grave:

Il cidr ci permette di ripartire geograficamente lo spazio di indirizzamento di Internet.

Con l’aumento delle reti indirizzabili si va incontro alla possibilità di far esplodere la dimensione delle tabelle di routing che dovrebbero contenere milioni di record. Per questo motivo gli indirizzi vengono assegnati a blocchi alle varie organizzazioni regionali e locali che a loro volta devono annunciare verso l’esterno della loro area solo una rete. Questa rete costituisce fondamentalmente l’aggregato delle sottoreti al suo interno. Ciò ha permesso l’utilizzo continuo delle routing table, altrimenti saremmo andati incontro ad un utilizzo mostruoso di entry e non avrebbero “scalato” bene in termini prestazionali.

IPv4 però è agli sgoccioli nonostante tecniche esistenti come il subnetting, il nat ecc…si arriverà quindi al momento in cui si spegnerà definitivamente la versione quattro per passare ad IPv6.

INSTRADAMENTO E CIDR(LONGEST PREFIX MATCH)

Come si fa il matching con i prefissi? Deve mascherare.

Quindi prendo i miei indirizzi, prendo la maschera, li metto in end e li vado a matchare con l’entry che sta nella mia routing table, ottenendo l’indirizzo di rete.

LONGEST PREFIX MATCHING: regola che permette nel momento in cui esistono più match nella routing table, vince il più specifico cioè con la maschera più lunga.

Infatti i pacchetti IP non sanno nulla delle maschere: come si può instradare?

Supponiamo di dover instradare un pacchetto indirizzato a 130.251.61.129, e di

avere nelle tabelle di routing:

– 130.0.0.0/8 verso l’interfaccia 1

– 130.251.0.0/16 verso l’interfaccia 2

– 130.251.61.0/24 verso l’interfaccia 3

– 130.251.61.64/26 verso l’interfaccia 4

• La scelta viene sempre fatta verso la rete (adatta) che ha la maschera piu’ lunga quindi la quarta in quanto:

• 1000010 1111011 0011101 10000001 (indirizzo di destinazione)

• 1000010 (130.0.0.0/8)

• 1000010 1111011 (130.251.0.0/16)

• 1000010 1111011 0011101 (130.251.61.0/24)

• 1000010 1111011 0011101 01 (130.251.61.64/26)

CIDR: Hierarchal Address Allocation

Il CIDR è il meccanismo di base per la scalabilità di Internet

– Indirizzi vengono allocati e distribuiti in blocchi contigui (prefix blocks)

– I protocolli e I meccanismi di routing lavorano su questi prefissi

– Aggregando si riesce a contenera la dimensione dalle routing tables

IL FUTURO:IPv6.

IPv6 fa OFFLOADING, elimina tutte le funzionalità superflue delle vecchie versioni e ha esteso lo spazio di indirizzamento passando da 32 a 128 bit.

//IPv5, sperimentazione non presa in considerazione.

Con la versione 6 considera pacchetti decisamente superiori rispetto ad ipv4.

Inoltre il pacchetto di ipv6, elimina le opzioni presenti in ipv4, ma permette di avere una struttura di lunghezza fissa alla quale si possono agganciare una serie di iter in maniera tale da consentire l’equivalente delle opzioni con maggiore flessibilità introducendo un meccanismo che lascia lo spazio a possibili estensioni del protocollo.

Quindi: ipv4 aveva il limite dei 16 byte di dimensione e iter di dimensione variabile; ipv6 ha iter di dimensione fissa con pox di agganciare più iter in maniera tale da ottenere meccanismi di estensione del protocollo. Supporta l’aggancio a protocolli di livello superiore.

OBIETTIVI DI IPV6.

Indirizzamento illimitato

• Semplicità del protocollo per ridurre i tempi di

elaborazione nei router

• Sicurezza

• Supporto per pacchetti di grosse dimensioni

• Gestione del tipo di servizio

• Prevedere evoluzioni future del protocollo

• Supportare i protocolli di livello superiore che si

appoggiano ad IPv4

INDIRIZZI IPv6.

IPv6 prevede l’utilizzo di indirizzi a 16 byte (128 bit)

• La notazione utilizzata e’ una sequenza di otto blocchi a 16 bit di quattro cifre

esadecimali, separate da “:”

8000:0000:0000:0000:0123:4567:89AB:CDEF

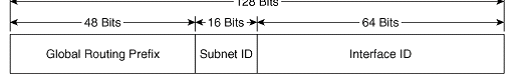
Per rappresentare più comodamente gli indirizzi si possono utilizzare

ottimizzazioni:

– si possono omettere gli zeri ad inizio di un gruppo (:0123: diventa :123:)

– si possono omettere gruppi di zeri consecutivi, rappresentati da una sequenza “::”

DIMENSIONE DELLA MASCHERA rappresentata attraverso la rappresentazione slashed cioè slash qualcosa, dove quel qualcosa è la dimensione della maschera. ((((((: spiegazione di merda. La maschera è ovviamente l’unica cosa che verrà sempre rappresentata in decimale.



INDIRIZZI IPv6 compatibili IPv4.

Vi sono indirizzi compatibili IPv4 supportati da IPv6, a 32 bit per l’indirizzo Ipv4 e poi il resto tutto a 0, proprio per questo li riconosciamo. Sono indirizzi riservati alle operazioni di transizione.

Un indirizzo compatibile IPv4 consente a un host che supporta IPv6 di

parlare IPv6 anche se il router o i router locali non parlano IPv6

• Gli indirizzi compatibili IPv4 avvisano il software del mittente di creare

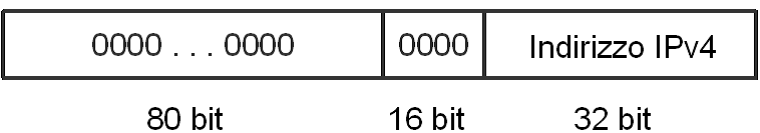
un tunnel, incapsulando il pacchetto IPv6 in un pacchetto IPv4

• Gli indirizzi IPv4 sono rappresentati con 6 gruppi di zeri, e due gruppi

che rappresentano l’indirizzo IPv4 (rappresentabili anche in notazione

decimale):

– ::89AB:CDEF oppure ::137.171.205.239

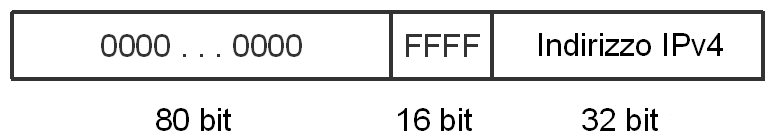


Indirizzo IPv6 mappato IPv4.

C’è la possibilità di mappareIPv6 su indirizzi IPv4, ci servono per saltare fra host che supportano sia ipv6 che v4 e farli parlare.

1Gli indirizzi mappati IPv4 consentono a un host che supporta sia IPv4 sia IPv6 di comunicare con un host che supporta solo IPv4

• L’indirizzo IPv6 si basa completamente sull’indirizzo IPv4 e consiste di 80 bit posti a 0 seguiti da 16 bit a uno, seguiti da un indirizzo IPv4 a 32 bit



Indirizzi IPv6(cont.)

Come per IPv4 l’indirizzo contiene una informazione di rete ed una informazione di host

• La notazione per definire quale parte dell’indirizzo e’ dedicato alla rete e’ quella di specificare la lunghezza in bit dell’indirizzo di rete dopo un “/” in coda all’indirizzo (come in IPv4)

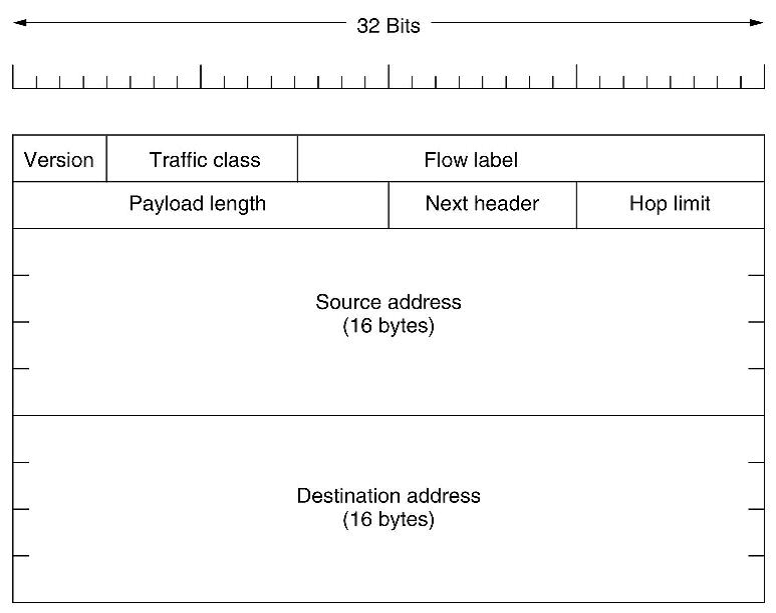
• Anche in IPv6 la “rete” e identificata dall’indirizzo con tutti “0” nel campo di indirizzo dell’host

Pacchetti IPv6

Il pacchetto IPv6 e’ costituito da un header di lunghezza fissa (40 byte) ed un campo dati; il campo dati puo’ opzionalmente contenere altri header prima dei dati veri e propri

Abbiamo detto che in IPv6 è presente una lunghezza fissa,il primo campo contengono la versione, invece del TOS qui abbiamo il concetto di traffic class(concetto uguale al tos ma con possibilità di creare un numero di classi maggiore), altro campo “flow label” a 20bit (mette un etichetta a tutti i pacchetti che fanno parte dello stesso flusso e quindi che devono essere trattati tutti allo stesso modo), lunghezza del Peyload (rappresentata in blocchi a 32 bit con un pacchetto che può raggiungere davvero grandezza consistente), next header (campo puntatore che si usa per agganciare alla testata di un pacchetto, un’altra testata che porta altre informazioni), Hop limit (funziona proprio come il TTL), infine l’indirizzo sorgente e quello di destinazione entrambi di 16 bytes.

Il concetto di frammentazione è completamente eliminato, check sum eliminato



HEADER IPv6.(Slide saltate dal prof)

La lunghezza dell’Header non c’è più siccome è fissa.

Il campo version non cambia significato, ed assume il valore 6

• Il campo traffic class serve ad identificare i pacchetti che necessitano di un instradamento particolare

– essenzialmente introdotto per supportare il traffico prioritario, o il traffico di tipo voce o video stream che richiede ritardi costanti

– un campo simile esiste nell’header di IPv4, inutilizzato

• Il campo flow label e’ stato introdotto per identificare in qualche modo i pacchetti appartenenti allo stesso flusso trasmissivo

– sempre al fine di supportare meglio il traffico voce/video

– e’ un tentativo di identificare il flusso di dati di una “connessione” in un protocollo connection less

– attualmente in fase sperimentale

Il campo payload length indica la lunghezza del pacchetto in byte, esclusi i 40 byte fissi dell’header

– la lunghezza massima del pacchetto e’ di 65536 bytes (+ 40)

• Il campo next header indica

– il protocollo del livello di trasporto a cui sono destinati i dati (TCP o UDP) se non c’e’

intestazione estesa

– il tipo di intestazione estesa successiva utilizzata (se c’e’): in questo caso sara’ il

corrispondente campo dell’header dell’ultima intestazione estesa a specificare il protocollo di trasporto di destinazione

• Il campo hop limit e’ equivalente al campo time to live dell’header IPv4, ma ora ha

l’esclusivo significato di conto degli hop

– viene decrementato ad ogni hop; raggiunto lo zero il pacchetto viene scartato

– ha la stessa funzione del corrispondente campo IPv4: evitare che un pacchetto rimanga troppo a lungo in rete in caso di problemi di routing

• Gli ultimi campi sono gli indirizzi sorgente e destinatario del pacchetto

COSA NON C’E’ PIU’.(dalle slide+ spiegazione del prof)

Il campo IHL (Internet Header Length) che rappresenta la lunghezza dell’header

– non e’ piu’ necessario, perche’ la lunghezza dell’header e’ fissata a 40

• Il campo protocol e’ sostituito dal campo next header

**• I campi riguardanti la frammentazione**

– IPv6 non prevede che i router eseguano frammentazione, perche’ fa perdere tempo

– i nodi IPv6 tentano di identificare la dimensione corretta dei pacchetti da scambiarsi in modo dinamico

– non basta: se il router non puo’ inoltrare un pacchetto, invia un messaggio

(ICMP) indietro per notificare il fatto e butta il pacchetto

– di fatto risulta piu’ efficiente fare in modo che l’host di partenza invii i

pacchetti di dimensione corretta che non frammentare nei router

• Il campo checksum

– IPv6 non utilizza checksum sui suoi pacchetti, per motivi di efficienza

– pur nel caso ridotto di un checksum dedicato all’header, il controllo della correttezza risulta un processo molto costoso per i router

– essendoci meccanismi analoghi a livello di data link ed a livello di trasporto, IPv6 ne fa a meno

Abbiamo opzioni riguardanti la sicurezza e opzioni riguardante l’autenticazione end to end e riguardanti la cifratura dei pacchetti.

TRANSIZIONE da IPv4 ad IPv6

Problema che deve essere affrontato perche’ mentre l’IPv6 puo’ essere costruito compatibile con IPv4 nel senso che puo’ spedire, instradare e ricevere datagram IPv4, IPv4 non e’ in grado di gestire datagram IPv6. Intanto esiste la possibilità di “impacchettare” un pacchetto ipv6 all’interno del payload di ipv4.

DA OPZIONE: NODI DUAL STACK A PRINCI DEL ROUTING IP NON HA SPIEGATO

INSTRADAMENTO DIRETTO

Quando parliamo di instradamento in IP, parliamo di un instradamento completamente connectionless che procede in best effort con completa indipendenza per ciascun pacchetto che viene instradato. Abbiamo due tipi di instradamento: DIRETTO e INDIRETTO.

* Per l’instradamento DIRETTO:

Passiamo da un IP ad un altro, entrambi localizzati sullo stesso datalink(subnet);

E’ molto semplice, vi è solo un’operazione da svolgere, l’ADDRESS RESOLUTION( che vuol dire traduzione dall’indirizzo IP al datalink, fa parte del protocollo ausiliario ADDRESS RESLUTION PROTOCOL);

Viceversa, quando non siamo sullo stesso datalink e sullo stesso subnet abbiamo la necessità di passare attraverso dei relay intermedi. Cioè abbiamo la necessità di attraversare dei dispositivi che prendano in qualche modo dei pacchetti da un’interfaccia, attraverso un istradamento diretto, in un secondo momento compiano uno step interno di forwarding (primo passo di indirezione) e ci passino su un’altra datalink dove ci sarà un altro instradamento diretto che o arriva a destinazione o avrà un altro passo indiretto.

Il processo funziona in maniera destination based.

Sappiamo che ogni datagramma contiene un indirizzo di destinazione e proprio sulla sua base viene compiuto l’instradamento. Come identifico quindi la rete di destinazione? Mettendola in end con la netmask e machandola con la routing table. Se in END con la netmask mi rendo conto che sono sulla stessa rete, devo fare l’instradamento diretto altrimenti indiretto.

• Non coinvolge router intermedi

• Il trasmettitore IP risolve l’indirizzo fisico dell’host destinatario (tramite il protocollo ARP),

incapsula il datagramma nell’unità dati della rete fisica e lo invia verso destinazione

• Utilizza i meccanismi propri della rete fisica in questione per inviare il datagramma

* INDIRETTO: (Dalle slide siccome il prof non si è minimamente scomposto a spiegare)

L’ host di destinazione non è sulla stessa sotto-rete del mittente

• Il mittente deve identificare un router a cui inviare il datagramma; il router deve inviare il

datagramma verso la sotto-rete di destinazione.

• Il router esamina il datagramma IP ricevuto e, se l’host di destinazione non si trova in

una sottorete a cui il router è direttamente connesso, decide il router successivo verso

cui instradarlo

– l'instradamento attraverso la sotto-rete che connette i due router avviene secondo i

meccanismi della sotto-rete

• Il processo si ripete di router in router sino alla sotto-rete di destinazione

FORWARDING DI DATAGRAMMI IP.

• E’ il processo che consente a un pacchetto di essere trasferito da un ingresso a una uscita del nodo e di nodo in

nodo di essere trasportato dalla sorgente alla destinazione

• Ipotesi

– Ogni datagramma contiene l’indirizzo IP della destinazione

– La parte di rete identifica in modo univoco la rete nell’ambito di Internet

– Host e router con lo stesso indirizzo di rete si scambiano i pacchetti

su quella rete

– Ogni rete che e’ parte di Internet ha almeno un router collegato ad

un’altra rete

FUNZIONAMENTO.

• L’host o il router stabilisce per confronto con il proprio indirizzo di rete

se la destinazione appartiene o meno alla rete o alle reti a cui e’

connesso

• Se la risposta e’ positiva si innesca la procedura ARP per

l’individuazione dell’indirizzo fisico

• Se il nodo e’ connesso a una rete diversa occorre che il datagramma

venga inviato a un router (next hop router)

INSTRADAMENTO LOCALE:ARP

Per instradare un pacchetto IP verso una destinazione appartenente alla stessa rete del mittente viene incapsulato il pacchetto IP in un pacchetto dello strato di data link sottostante. Il problema da risolvere e’ come fare a sapere a quale indirizzo

di data link (Ethernet) inviare il pacchetto. Per risolvere questo problema si usufruisce

dell’ADDRESS RESOLUTION (che vuol dire traduzione dall’indirizzo IP al datalink, fa parte del protocollo ausiliario ADDRESS RESLUTION PROTOCOL).

ARP

Come funziona?

E’ una logica REQUEST RESPONS, in broadcast con messaggio unicast di ARP response. Quando un pacchetto individua la necessità di fare l’instradamento diretto, attraverso l’ARP, manda un frame in broadcast a tutta la sua sottorete chiedendo chi possiede l’indirizzo IP x, solo chi ha l’indirizzo IP giusto risponde. Conosciuto il MAC ADDRESS, saranno in grado di passarsi a livello datalink i pacchetti.

Questo mapping viene inserito nella local arp table.

ARP CACHE

E’ un’operazione del tutto bidirezionale infatti entrambi dopo l’operazione di ARP hanno una visione l’uno dell’altro memorizzando gli entrambi gli indirizzi nella cache. L’ARP cache, è una struttura delicata. In alcuni casi la posso anche esplicitamente andare a pulirla. Può dare problemi di sicurezza.

Dalle slide:

• Per migliorare le prestazioni, ARP puo’ gestire sull’host locale una cache in memoria

• Ogni volta che viene appresa una nuova associazione IPaddress-Hwaddress, viene

memorizzata nella cache

• Quando ARP deve individuare un indirizzo HW, prima controlla nella cache: se

l’informazione e’ presente viene utilizzata senza inviare pacchetti sulla rete

• Le entry nella cache di ARP hanno un tempo di scadenza, per evitare che eventi quali

sostituzione di schede di rete o reindirizzamento degli host possano rendere

impossibile la comunicazione

– alla scadenza del tempo di validita’ l’entry viene rimossa dalla cache, ed una successiva

richiesta per quell’indirizzo provochera’ una nuova emissione di ARP request sulla LAN

• Alcuni sistemi permettono di definire nella cache di ARP delle entry manuali prive di

scadenza

– talvolta necessarie, qualora l’host di destinazione non supporti correttamente il protocollo ARP

– questa tecnica puo’ essere utilizzata anche per motivi di efficienza

– in ogni caso difficile da mantenere aggiornata la cache delle macchine: meglio evitare

REVERSE ARP

Esiste un meccanismo duale all’ARP, il REVERSE ARP. Se ho una macchina senza possibilità di memorizzare il proprio indirizzo IP. Se vuole averlo quando carica, questa macchina fa un’operazione di REVERSE ADDRESS RESOLUTION: manda un pacchetto in broadcast chiedendo l’indirizzo IP, viene servito dall’ARP comunicando l’indirizzo IP.

DHCP

Standard in RFC 1531

Permette alle macchine di avere una configurazione da un server

Elimina costose configurazioni manuali

Funzionamento:

La macchina che ha bisogno dell’indirizzo, manda un pacchetto di dhcp discovered, manda un messaggio in broadcast per capire chi sono i vari server. Essi risponderanno al dhcp disc offrendo disponibilità, la macchina farà un dhcp reques e otterrà un arck noleg (da chiedere a qualcuno, non esiste da nessuna parte) che gli permetterà di avere l’IP, netmask, default gateway(ind IP del router che mi collega alla rete esterna) e indicazioni sui DNS.

ICMP

ICMP, serie di funzionalità per la gestione sulla rete. Ha una propria testata che ha un header che contiene il tipo di messaggio, il codice associato al messaggio, check sum, identificatore e numero di sequenza. Esistono una dozzina di messaggi ICMP destinati ad avvisare i router o gli host di qualche evento specifico della rete

• ICMP non ha lo scopo di rendere IP affidabile, ma di notificare allo strato di

rete problemi non transienti nella comunicazione a livello 3 in modo da attivare

quelle reazioni dinamiche al malfunzionamento della rete necessarie, ad

esempio, a ridisegnare dinamicamente la topologia utilizzata per l’instradamento

• ICMP utilizza IP come protocollo di trasporto per instradare i propri messaggi

MESSAGGI ICMP.

I messaggi principali ICMP:

-destinazione irraggiungibile: questo messaggio e’ inviato dai router agli host

sorgenti di un pacchetto IP per notificare che la destinazione non e’ raggiungibile

– time exceeded: viene notificato alla sorgente di un pacchetto che il pacchetto ha

raggiunto la scadenza del time-to-live

– problema di parametri: un router annuncia al router che gli ha inviato un pacchetto

che i parametri dell’header sono inconsistenti

– source quench: utilizzato (in passato) per rallentare la sorgente che trasmette

troppo velocemente in caso di congestione; l’evoluzione del TCP/IP ha spostato

pero’ il controllo della congestione sul livello di trasporto

– redirect (reindirizzamento): il router avvisa l’host sorgente che ha inviato il

pacchetto iniziale secondo un instradamento errato (ad esempio: se ci sono due

router sulla LAN, ed un pacchetto viene inviato da un host verso il router sbagliato)

– echo ed echo reply: utilizzati per verificare la raggiungibilita’ di un host:

• quando un host riceve un ICMP ECHO da una sorgente, deve immediatamente rispondere con un ICMP ECHO REPLY

• molte utility fanno uso di questo messaggio ICMP (ad esempio ping)

– timestamp e timestamp response: analoghi ai messaggi ECHO/ECHO REPLY, inseriscono nei pacchetti informazioni di tempo per valutare il ritardo della connessione.

NAT.

“Cos’è il NAT? Una porcheria.” Cit. (No Maria, io esco)

E’ un meccanismo nato per coprire dei grossi buchi, quando non vi sono più indirizzi utilizza indirizzi riservati e li traduce in pubblici esterni. Può lavorare anche in logica overload, mi permette più indirizzi interni di essere mappato sullo stesso indirizzo esterno.

Come funziona? (E’ na grossa porcheria cit. “ma che è sta cafonata”)

Il router costruisce una tabella di corrispondenza tra indirizzi interni e porte ed indirizzi esterni e porte.

NAT INSIDE:

Prende gli indirizzi inside local e li rimappa in inside global.

L’indirizzo interno quando esce attraverso il nat viene fatto corrispondere in un determinato indirizzo esterno e porta. La tavola viene ricercata ogni volta che passa un pacchetto. La gestione quando la tavola è molto grande è estremamente pesante.

OUTSIDE:

O. Local e Global, la prima serve a fare un rimappaggio di indirizzi IP assegnati ad un host sulla rete esterna come vengono visti dagli host sulla rete interna mentre per il secondo serve come rimappaggio di indirizzi ip assegnati dall’host sulla rete esterna.

ROUTER IP

Un router può interconnettere reti che usano diverse tecnologie.

ROUTER- LE SUE PARTI

Il router, tipicamente realizzato in architettura special purpose, è configurato o attraverso una porta di console o via telnet e va inizializzato caricando un sistema operativo (IOS) nella sua memoria.

Il router ha:

-porte di Ingresso / Uscita;

-blocco di commutazione, che collega le porte di ingresso con quelle di uscita

-processore di instradamento: esegue protocolli di routing, aggiorna tabelle di routing;

-memorie: ROM (codice per Bootstrap [avvio] e POST [Power-On Self Test = diagnostica e manutenzione hardware]), RAM (tabelle di routing), NVRAM (configurazioni di avvio e il registro modalità di avvio), Flash (immagine IOS).

COLLEGAMENTI TRA ROUTERS

Per prima cosa si deve accenare al concetto di sistema autonomo (Autonomous System) che è un insieme di router e di reti che sono sotto il controllo di un'unica autorità amministrativa che li governa; questi router cooperano all'instradamento dei pacchetti all'interno di un sottosistema di rete abbastanza complesso. All'interno di quest'organizzazione si parla una lingua comune che si chiamano IGP (Interior Gateway Protocol). Si possono avere più di un protocollo di routing interno differenti. Se si parla tra AS differenti si parla di protocolli diversi EGP (Exterior Gateway Protocol). I router che fanno da “ ponte di collegamento “ tra AS diversi cioè sono il punto di ingresso e di uscita verso altri AS vengono detti Border Router.

TABELLE DI ROUTING

Scambiandosi queste informazioni i router devono caricare in modo corretto le tabelle di routing. Quest'ultime contengono vari campi che indicheranno la rete interessata, l'interfaccia usata per raggiungere quella rete, il next stop su quell'interfaccia con cui aggiungo quella rete e altri elementi per andare a fare la scelta del percorso migliore.

Quindi nelle tabelle di routing si ha l'IP di destinazione (indirizzo- maschera), il next stop, l'interfaccia, un tempo e soprattuto la metrica. La metrica individua, fondamentalmente, il costo di quella specifica scelta/next stop.

ROUTER DI DEFAULT (DEFAULT GATEWAY)

Per evitare che tutti i router abbiano una visione completa della routing table, si delega l'instradamento a un router di livello più alto. Quindi si identifica una default route indicata con 0.0.0.0/0 perché così fa match con tutti, ma per ultima. Questa è una chance estrema quando non si hanno le informazioni necessarie nella routing table.

LONGEST PREFIX MATCHING

Per valutare se un host con indirizzo X appartiene ad una sottorete con indirizzo

Y/M si effettua l’operazione di matching. Se coincide si fa l'instradamento diretto altrimenti si va a cercare sulla tavola di routing e si prende il prefisso più lungo che andrà a soddisfare quel matching.

OPERAZIONI DI INSTRADAMENTO

Instradamento effettuato dal router X:

1) estrae l’indirizzo IP di destinazione dal datagramma (Y);

2) se l’indirizzo di destinazione Y coincide con X (la destinazione è il router X), estrae il contenuto informativo e lo consegna al protocollo indicato;

3) decrementa il Time To Live del datagramma; se il Time To Live è arrivato a

zero scarta il datagramma e ne da comunicazione all’host mittente;

4) confronta la componente X and M con Y and M, se sono uguali inoltra il datagramma direttamente ( ARP);

5) Per tutte le righe della tabella di instradamento [N,M,NH,I] confronta se Y and M = N and M (N indirizzo della sotto-rete, M maschera di sotto-rete, NH indirizzo prossimo router ed I interfaccia d’uscita). Inoltra il datagramma verso il router NH relativo alla corrispondenza con la maschera più lunga;

6) altrimenti (non c’è nessuna corrispondenza) inoltra verso il default router se

ne è stato specificato uno oppure scarta il datagramma e dichiara errore di

instradamento.

STRATEGIE DI INSTRADAMENTO

L'instradamento può essere implementato in due modi: staticamente, precalcolando i percorsi e in questo modo le cose funzionano, e dinamicamente, i router si scambiano autonomamente le informazioni circa la raggiungibilità delle varie destinazioni e sulla base di queste info costruiscono la propria tavola di routing.

QUANDO USARE ROUTE STATICHE

Il routing statico è estremamente banale, ma poco flessibile. Ha senso solo quando non si hanno altre opzioni ad esempio un router con un'unica connessione.

LA ROUTE DI DEFAULT

Quando si parla di routing statico si può utilizzare anche la default route che collega l'unica connessione con il mondo esterno. La route di default specifica l’instradamento di tutti i pacchetti per i quali la tabella di instradamento non fornisce una route esplicita. Si specificano rete e mask con “0.0.0.0 0.0.0.0” oppure “0.0.0.0/0”. La rete 0.0.0.0/0 risulta sempre ultima nel matching (longest prefix match) ma corrisponde sempre.

ROUTING DINAMICO- PROTOCOLLI DI ROUTING

Quando ci sono più di un router è fortemente sconveniente/insensato usare il routing statico. La soluzione è di utilizzare protocolli di routing dinamico che aiutano, attraverso lo scambio di informazioni , la costruzione delle tabelle di routing. I protocolli scelgono i percorsi in base alle metriche.

METRICHE

La Metrica serve per selezionare il percorso “migliore”, ovvero più corto o meno congestionato o più ampio o meno costoso. Le metriche si comportano anche in maniera abbastanza dinamica, cioè reagiscono alle possibili anomalie come guasti, modifiche ai parametri, variazioni nel carico dei link.

Diversi protocolli usano metriche differenti come il protocollo RIP usa Hop Count, OSPF utilizza la capacità di banda, IS-IS condiziona i link con un costo, BGP va a definire il numero di AS da attraversa per arrivare a destinazione.

Si possono avere metriche composte.

DISTANZA AMMINISTRATIVA

Oltre alla metrica c'è un elemento importante da considerare, la cosiddetta distanza amministrativa. La distanza amministrativa quantifica l’attendibilità dell’informazione di instradamento; più il valore è basso, più l’informazione è “sicura”. Se il router riceve da fonti diverse route alternative verso la stessa rete, userà la distanza amministrativa per decidere quale rendere attiva.

Ad esempio una rete direttamente connessa ha come distanza amministrativa 0 perché è molto affidabile.

CLASSIFICAZIONE ALGORITMI DI ROUTING

Il protocollo definisce le regole comuni da utilizzare e l'algoritmo è la logica procedurale che il protocollo deve utilizzare per raggiungere un determinato risultato. Gli altoritmi di dividono in non adattativi e adattativi. I primi procedono sempre nello stesso modo, i secondi aggiornano e calcolano le tabelle di instradamento, sono dinamici e non deterministici.

ALGORITMI DI ROUTING NON ADATIVI

Ci sono due tipi:

-Fixed Directory Routing: l’algoritmo prevede che ogni nodo abbia una tabella di instradamento che metta in corrispondenza il nodo da raggiungere con la linea da

usare. Queste entry sono puramente statiche, poiché è il gestore che si occupa di determinarle e di configurare il router. Il gestore ha così il completo controllo sul traffico ed è necessario un suo intervento in caso di guasto.

-Basati su Flooding: ciascun pacchetto che arriva ad un router viene instradato su tutte le porte, eccetto quella da cui è arrivata. Questo metodo, concepito per reti militari, massimizza la probabilità che i dati arrivino a destinazione, ma produce un altro volume di traffico sulla rete.

ALGORITMI DI ROUTING ADATIVI

Ci sono tre possibilità di adattamento:

• Routing Centralizzato. Un RCC, Routing Control Center, conosce la topologia di tutta la rete, calcola e distribuisce le tabelle di instradamento di ogni router. La gestione permette tabelle calcolate con algoritmi sofisticati, ma necessita un

gestore a livello mondiale.

• Routing Isolato. Ogni router calcola le proprie tabelle di instradamento in modo indipendente.

• Routing Distribuito. E’ fusione dei due metodi precedenti, realizza le funzionalità RCC in ogni singolo nodo della rete. Le tabelle vengono aggiornate dai routers scambiandosi informazioni di servizio mediante apposito protocollo.

ROUTING E GRAFO DI RETE

Per rappresentare una rete si utilizzano solitamente grafi orientati dove ogni nodo rappresenta un router ed ogni arco rappresenta una linea di comunicazione.

L'obiettivo è di trovare i percorsi più brevi.

ALGORITMI BASATI SUL PERCORSO PIU' BREVE

Non esiste il percorso migliore in assoluto, ma migliore secondo una determinata metrica. Se la metrica è basata sulla distanza, il migliore sarà quello con la distanza geografica minore; se la metrica è l'Hop Count quello migliore sarà quello che attraverserà meno router ed così via a seconda della metrica o di un insieme di metriche. Definita una metrica, le linee potranno essere etichettate con un numero (peso o metrica): piu’ basso e’ il numero, “piu’ breve” e’ la linea.

Dopo questa operazione si fa girare sul grafo un algoritmo (come Dijkstra) che individua il percorso ottimale.

ALGORITMO DI DIJKSTRA

L’algoritmo di Dijkstra (1959) lavora su grafi orientati, che hanno pesi non negativi sui collegamenti. Questo algoritmo trova i percorsi più brevi tra un nodo di partenza e tutti gli altri.

PROCEDIMENTO

I nodi vengono messi in due insiemi: esaminati e non esaminati. Ad ogni nodo i, devono essere associate due etichette, COSTO[i] che indica il peso totale del cammino (la somma dei pesi sugli archi percorsi per arrivare al nodo i-esimo) e PRED[i] che indica il nodo che precede i nel cammino minimo.

Il nodo sorgente è il primo nodo attivo. Si esaminano tutti i nodi i connessi al nodo attivo j e per ciascuno di essi si pone: PRED[i] = j e COSTO[i]=COSTO[j]+LINK[j,i] .

Il nuovo nodo attivo è quello con il costo più basso tra quelli esaminati e viene marcato come permanente.

Possiamo lavorare con Dijkstra quando si ha una visione completa del grafo.

PERCHE' FUNZIONA?

Supponiamo di aver trovato ABE come percorso minimo, se esistesse un altro percorso AXYZE a costo piu’ basso ci sarebbero 2 possibilita’:

– Z è un nodo permanente

• E è già stato esaminato e AXYZE e’ gia’ stato individuato

– Z è un nodo provvisorio

• O la sua label è > di quella di E e quindi non rappresenta il percorso minimo

• O la sua label è < di quella di E e quindi Z sarebbe il nodo attivo

Le precedenti considerazioni portano a concludere che la procedura individua il percorso a costo minimo. La complessità è O(|V|al quadrato).

DISTANCE VECTOR(BELLMAN-FORD)

Se non vediamo tutto il grafo Dijkstra non si può utilizzare, mentre con Bellman-Ford no. Si costruisce il grafo step by step. Si parte dal nodo di origine e si guardano i vicini uno per uno assegnandogli un costo per raggiungerli e si itera l'operazione per tutti i nodi, ottenendo così il percorso di costo minimo per raggiungere una destinazione. Ha una complessità temporale O(|V| |E|), |E| numero di archi del grafo.

Ad ogni linea è assegnata una distanza, valutata in base ad una metrica, indicata anche col nome di costo.

Le informazioni di routing vengono scambiate con tutti i router adiacenti.

Ogni nodo acquisisce una visibilità della rete indiretta, mutuata dai vicini. In base alle informazioni ricevute dai vicini viene ricostruita la tabella di routing nuova, quindi il processo di convergenza con questo algoritmo impiegherà un bel po' di tempo. Si deve limitare il numero di passi per evitare di andare in giro all'infinito.

Per valutare le distanze si calcola i costi che congiuno un nodo ai suoi adiacenti; per fare ciò ogni router costruisce i propri vettori di distanze.

ALGORITMI DISTANCE VECTOR

Il Distance Vector associato a ciascuna linea, contiene informazioni ricavate dalla tabella di instradamento del router collegato all'altro estremo della linea.

Il calcolo delle tabelle di instradamento dipende da tutti i distance vector associati alle linee attive del router. Quando un router calcola una nuova tabella, la invia ai ruoters adiacenti sotto forma di distance vector.

Quando un nodo riceve più opzioni differenti verso la stessa destinazione sceglie quella a minor distanza da lui.

Ciascun router riceve la tabella di instradamento dai suoi vicini direttamente connessi

Ogni entry è composta da quattro parametri, indirizzo (prefisso + maschera) , hops, costo e linea, e la tabella contiene entry relative ad ogni nodo presente in rete. Il Distance Vector da inviare al router adiacente è composto dalle prime tre colonne.

Ogni volta che un nodo riceve un Distance Vector deve verificare se deve effettuare varie modifiche nei vari campi nella propria tabella, la fusione avviene selezionando tra le entry di uguale indirizzo quella a minor costo. A parità di costo è scelta quella con minor numero di hops.

Questo algoritmo reagisce molto bene quando il costo migliora mentre se peggiora il costo reagisce male. Distance Vector è sconsigliato per reti vaste perchè è lento a convergere.

FLOODING

Tutti i pacchetti sono inviati a tutti tranne al nodo da cui è arrivato.

Ha dei meccanismi di protezione come dotare il pacchetto di un contatore settato con il massimo di hop che dovrà fare e quando questo contatore vale 0 il pacchetto verrà eliminato. Un altro meccanismo è dotare i pacchetti di un numero di sequenza, i pacchetti ricevuti vengono conservati un database , quando arriva un nuovo pacchetto si fa la ricerva nel database se si trova una corrispondenza si elimina il pacchetto invece di rimandarlo.

Il flooding può essere fatto in maniera cieca, ovvero mandandolo a tutti i nodi oppure in maniera selettiva, i pacchetti in arrivo vengono replicati ma solo sulle linee che approssimativamente vanno nella direzione richiesta dalla sorgente (non garantisce l'inoltro sicuro). Si può fare anche broadcast statistico cioè decidere con che percentuale mandare un pacchetto a tutti gli altri o eliminarlo.

Se si devono valutare gli altgoritmi di instradamento il metro di paragone è il flooding perchè sceglie sempre la strada più breve.

ALGORITMO FLOODING

Gli aspetti negativi di questo algoritmo sono essenzialmente legati alla inefficienza, c'è troppo traffico nella rete, si spreca la banda, carico di lavoro sui nodi che trattano il pacchetto.

Aspetti positivi sono: qualsiasi pacchetto arrivera’ nel tempo piu’ breve possibile, estremamente resistente a modifiche della topologia, non richiede una conoscenza a priori della topologia della rete.

CLASSIFICAZIONE DEI PROTOCOLLI DI ROUTING

Distance Vector: RIP e IGRP .

Link State: OSPF e IS-IS.

AGGIORNAMENTI IN DISTANCE VECTOR

Gli aggiornamenti presenti nell’intera routing table sono inviati solo ai vicini direttamente connessi, viaggiano al cambiare della topologia e periodicamente.

AGGIORNAMENTI LINK-STATE

Gli aggiornamenti sono propagati uno ad uno a tutti i nodi nel dominio di routing attraverso il flooding periodicamnete e al cambiamendo della topologia.

DISTANCE VECTOR NETWORK DISCOVERY

Con solo 3 router la rete per raggiungere la convergenza impiega 2 minuti, quindi è instambile per tutto questo tempo: non va bene!

INSERIMENTO DI UN NODO

Nei distance vector si verifica un problema quando si inserisce un nodo, poichè si devono aggiornare tutti i router e come abbiamo visto nel paragrafo precedente ci vuole molto tempo e la rete resta instabile per troppo tempo. Ma non è il problema più grave.

PROBLEMI CON ROUTING DISTANCE VECTOR

Il problema più grave è quando un nodo viene estratto, ovvero un router si spegne, un datalink muore, uno switch si spegne quindi quando qualche informazione va a cambiare si possono verificare cose abbastanza sgradevoli.

ROUTING LOOPS E CONTO ALL'INFINITO

Ad esempio si hanno 3 router ognuno con la propria routing table. Supponiamo che A si disconnetta dalla rete, B riconosce che A non risponde e che il suo vicino è a distanza 2 da A quindi pone erroneamente a 3 la sua distanza da A. L’informazione errata si propaga agli altri nodi e i costi vanno all’infinito.

ROUTING LOOPS

Ad esempio abbiamo 3 router A, B, C e sono a convergenza. Ad un certo punto la rete 10.4.0.0 si spegne (quindi va "down") che era a distanza 0 da C ma ora quest'ultimo non la vede più e di conseguenza non l'annuncia più al suo vicino.

Essendo a convergenza i router B ce l'ha e l'annuncia a C che la salverà a distanza 2. Così inizia a propagarsi l'infomazione errata e il router A aggiornerà la sua routing table ponendo 10.4.0.0 a distanza 4 e B a distanza 3.

SINTOMI: COUNTING A INFINITO

L'infomazione errata rimbalzerà tra i vari router e l'Hop Count per la 10.4.0.0 tenederà a infinito. La metrica salirà fino ad arrivare a 255 poi si blocca perchè capisce che c'è un problema(si riscontra il problema dopo 255 per 30 secondi) .

SOLUZIONE: LIMITARE L'HOP COUNT

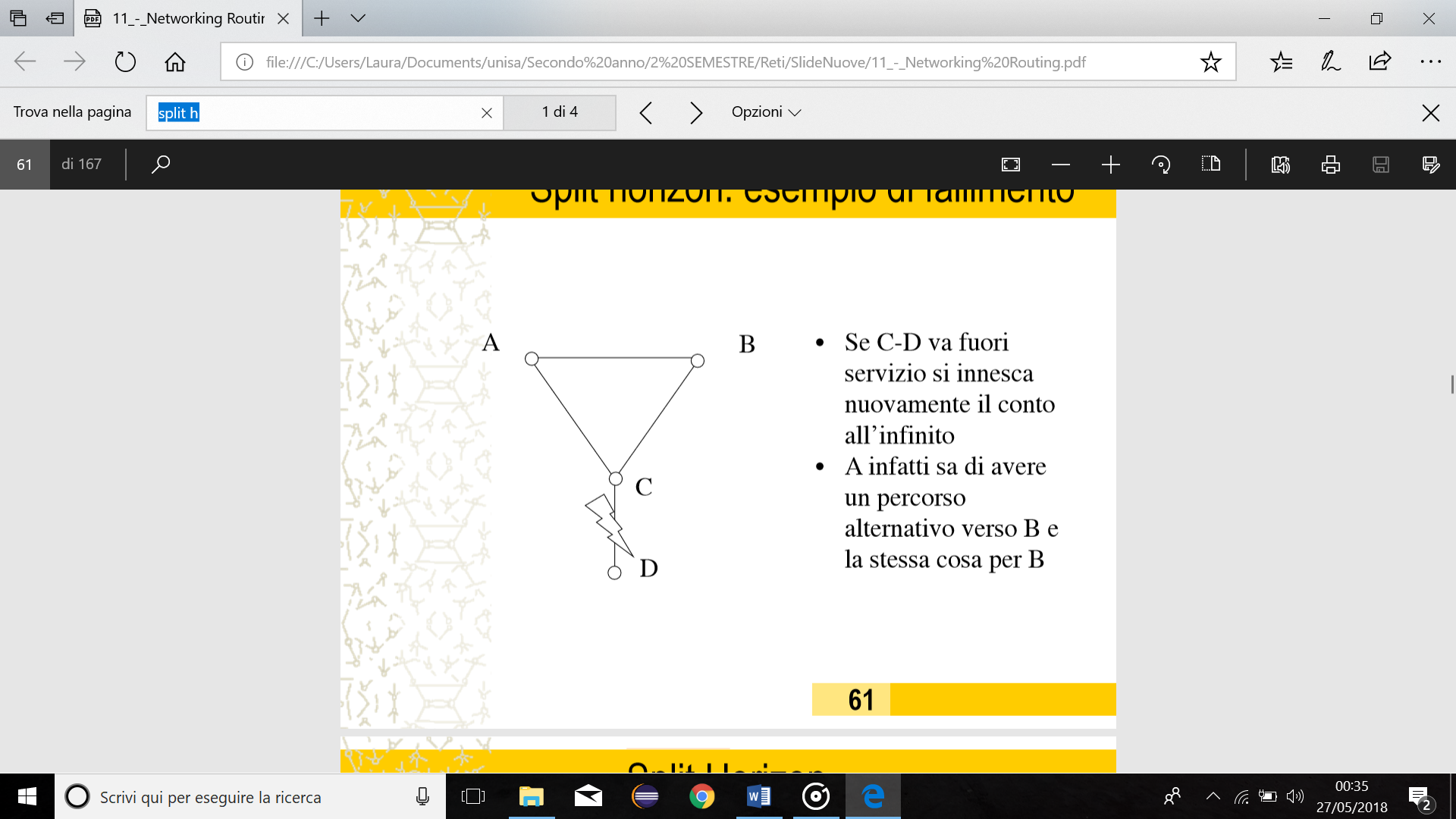
La soluzione è abbasare la possibile soglia. In modo da ridurre il tempo per riscontrare che c'è stato un problema. Questa soluzione non è ottimale perchè comunque ci vuole troppo tempo.

UNA SOLUZIONE: SPLIT HORIZON

Questa soluzione impedisce a un router X di inviare un'info di routing all'interfaccia da cui è stata appresa. Teoricamente risolve il problema del routing loop perchè non ritorna indietro l'informazione.

SPLIT HORIZON: ESEMPIO DI FALLIMENTO

Se C-D va fuori servizio si innesca nuovamente il conto all’infinito. A infatti sa di avere un percorso alternativo verso B e la stessa cosa per B.



Quindi lo split horizon non risolve tutti i problemi.

ROUTE POISONING

Route Poisoning (avvelenamento delle route) nel momento che ad esempio 10.4.0.0 si spegne invece di metterla "down" e non annunciala più si mette a metrica infinita, in modo tale che annunciandola ad infinito l'altro router capirà che c'è un problema.

POISON REVERSE

Per riscontrare i Poisoning si usa il meccanismo Poison Reverse. Quando si riceve una rete con metrica "infinity " invece di spegnerla definitivamente si mette in uno stato particolare chiamato "Possibily Down" e si manda a ritroso il Poison Reverse.

Queste varie soluzioni non sono mutuamente esclusive: si sommano poichè ognuno risolve un problema.

HOLD-DOWN TIMERS

Per gestire il problema delle fluttuazioni, ovvero un circuito può "cadere " e "risalire" in pochissimi secondi.

Quando una route è down invece di spegnerla definitivamente si attiva un timer e finchè il timer non è espirato la route non viene eliminata dalla routing table. Questo evita di instradare traffico in presenza di una fluttuazione, cioè evita di propagare inutilmente informazioni riguardanti la rete andata giù solo per pochi secondi.

TRIGGERED UPDATES

Se ad esempio 10.4.0.0 cade il router invia immediatamente l'aggiornamento della routing table. Succesivamente tutti i router attivano il timer di Hold-Down e mandano il Poinson Reverse. Nel mentre arrivano pacchetti per la 10.4.0.0 e quest'ultima è ancora nella routing table, quindi questi pacchetti vengono fatti passare; improvvisamente la route ritorna "up" e partono i Triggered Updates che spengono i rispettivi timer. In questo modo il traffico ha continuato a fluire risparmiando un sacco di tempo per la convergenza. I pacchetti inviati sono andati persi solo se la rete era ancora "down " quando gli arrivavano i pacchetti.

Tutto questo fa capire perchè gli algoritmi Distance Vector sono poco efficienti.

ALGORITMI DI ROUTING LINK STATE

Sono migliori dei Distance Vector e sono nati dopo proprio per sostituirli.

Questi algoritmi si basano sull'invio continuo delle informazioni che servono per costruire il grafo di rete e quindi il database topologico. Queste info viaggiano in flooding, cioè ognuno vede le stesse cose degli altri(questa è la forza dei routing distribuito).

LINK STATE PACKET

L’informazione è propagata ai router della rete con un messaggio definito Link State Packet (LSP) o Link State Advertisment. Questi pacchetti vengono fatti viaggiare direttamente dai nodi ai nodi vicini e poi propagati in logica flooding. La mappa della rete si costruisce fondendo ogni LSP in un database.

PASSI FONDAMENTALI

-Individuazione dei nodi vicini e dei relativi indirizzi

- Misura del ritardo e del costo verso ciascun vicino

- Costruzione dei pacchetti con le informazioni di routing

- Invio dei pacchetti a tutti gli altri router

- Calcolo del cammino piu breve verso ciascun router(Dijkstra)

INDIVIDUAZIONE DEI NODI VICINI

Un nodo manda un messaggio di HELLO quando si inserisce in rete a cui tutti i nodi vicini sono obbligati a rispondere indicando il proprio indirizzo. Una volta che sono arrivate le risponde si costruisce la tavola dei vicini e viene misura la distanza mandando pacchetti ECHO a cui e’ richiesta una risposta immediata per misurare il round trip time (il tempo che ci mette il pacchetto per andare avanti e tornare indietro) la cui metà è una stima del ritardo sulla linea. La valutazione del ritardo puo’ comprendere o meno il ritardo di coda.

PACCHETTI LINK STATE

Il pacchetto inizia con l’identificativo di chi lo manda seguito da un numero di sequenza. Vengono inviati sia periodicamente(ogni 30 min tipicamente) o anche sulle variazioni di stato. Si usa il flooding per la distribuzione e si costruisce il grafo di rete.

REQUISITI DEGLI ALGORITMI LINK STATE

In una rete con n router e k nodi vicini per router la memoria richiesta in ciascun nodo è proporzionale a kn. Su reti molto grandi questa cosa può diventare onerosa e quindi si ricorre alla divisione gerarchica. Con questa divisione diminuisce l'area di flooding e il grafo di rete diminuisce di dimensione.

PROTOCOLLI DI ROUTING GERARCHICO

Si ha una logica Link State vincolato alla singola area e le aree parlano tra loro attraverso delle aree comuni che non avranno la visione del grafo completo. La divisione gerarchica permette di gestire reti molto grandi senza nessun problema.

HA SALTATO DELLE SLIDE

PROTOCOLLI IGP: RIP

Il RIP (Routing Information Protocol) è un protocollo basato sull’algoritmo distance vector. Si usa su reti molto piccole.

Usa numero degli hop come metrica per il costo dei link: tutte le linee hanno costo 1; il costo massimo è fissato a 15, quindi impone il suo uso su reti di

estensione limitata. Ha una logica costituita da messaggi di annuncio e risposta.

La struttura del pacchetto prevede un Header con un campo che contiene una serie di componenti tra cui la versione, AFI (prefisso) e il next stop accompagnato dalla metrica.

Vi sono due versioni:

1)classfull(lavora con le classi, guardando i primi bit dell’indirizzo ma non al concetto della netmask) ;

2) seconda versione che porta con se la netmask

Ha un struttura protocollare abbastanza semplice con una testata ad 8 bit di comando, la versione del protocollo (1 o 2), l’AFI (prefisso), un indirizzo IP del nextstop e una serie di elementi opzionali che possono essere utilizzati per il traffic engineering.

Aspetti fondamentali: i messaggi vengono mandati sia in maniera periodica (ogni 30sec) e per la versione 2 vi è anche la possibilità di inviare RIP Advertisment(quando qualcosa si guasta parte un messaggio di avviso per notificare il problema/questo fattore non è presente nella versione 1. Questi elementi possono avere vettori di distanza fino ad una dimensione di 25 reti di destinazione, nel caso in cui ne avessi più di 25 devo utilizzare due messaggi consecutivi(poco efficiente ovviamente).

Perché il RIP e non l’OSPF? E’ un protocollo OPEN, quindi disponibile quasi ovunque, e pesa molto poco quindi dal punto di vista delle risorse richiede molto poco.

PROCOLLI IGP:OSPF.

Nato nel 1988, poco dopo il RIP, definito nell’RFC 2328. Su una rete seria non si può che utilizzare l’OSPF. Unico competitore è l’IS-IS, protocollo di routing sviluppato per la pila di protocolli OSI che si pensava sarebbe stato il sotituto dell’IP ma che per eccesso di complessità è morto.

Come funziona OSPF?

-è OPEN;

- ha metriche sofisticate e flessibili per definire il costo di ciascun circuito, possiamo infatti utilizzare la distanza fisica, il num di hop, il relay, costo della linea, banda oppure combinazione di esse;

-è un link state e per definizione converge bene;

-reagisce dinamicamente e rapidamente alla variazione della topologia;

-ci permette di fare routing basata sul tipo di servizio;

-permette di bilanciare il carico su diversi cammini(o diversi circuiti);

- implementare sicurezza;

CONNESSIONI DI OSPF

OSPF è un protocollo complicato che permette di gestire tre tipi di connessione:

-punto a punto

-BMA, broadcast multi Access

-rete geografica multi accesso, definite da OSPF, NBMA=Non broadcast Multi Access…cioè più nodi sullo stesso segmento però non broadcast.

La rete è vista come un grafo diretto

– ogni linea fisica e’ costituita da due archi, uno per ogni verso

– una rete multiaccesso e’ considerata come un punto del grafo, connessa a

ciascun router della rete da una coppia di archi

Ogni arco ha il suo costo, che è la metrica di OSPF, definisce il cammino più breve.

I nodi non hanno uno specifico peso e quindi non partecipano alle decisioni se non oltre ad essere down o up. L’unico elem decisionale è il peso sugli archi.

FUNZIONAMENTO OSPF

Ogni nodo quando si connette alla rete deve comunicare a tutti i suoi vicini quello che ha connesso e quindi manda in flooding degli LSA(Link state advertisment) relativi allo stato dei suoi collegamenti. Sulla base degli LSA ogni nodo OSPF si costruisce il database topologico, LSDB->LINK STATE DBASE. Una volta che tutti hanno ricevuti le info per costruire il DBTopologico parte il Dijkstra e il tutto si conclude. Vengono costruite da tutti i percorsi migliore. Qui siamo in logica pienamente distribuita, senza possibilità di errore.

Eventuali modifiche vanno segnalate a tutti i nodi nell’area (broadcast/flooding)

OSPF:MESSAGGI

Esistono una serie di messaggi:

d’ Aggiornamento: Link state update;

cambiamento dello stato del link

ogni messaggio ha un numero di sequenza

i messaggi vengono riscontrati (LS ACK)

Richiesta esplicita di informazioni: Link state Request

-riceverò ovviamente dai vicini una link state update che mi aggiorna di ciò che è successo

Trasferimento delle informazioni: DataBase Descriprion

E’ una copia del LS DB usata per sincronizzare un nuovo nodo

OSPF: le aree

OPSF supporta una divisione gerarchica in aree: l’area zero è un’area dorsale a cui sono collegate tutte le altre aree. All’interno delle aree è tutto link state, fra aree la visibilità è instance selector.

OSPF: tipi di router

Come vede i router OSPF?

Divisione in 4 famiglie:

-router interni(collegato al concetto di gerarchia) router che sono fissi in un’area

-router di confine(border router), a cavallo di più aree(una è sempre l’area zero)

-router di dorsale(backbone router), interni alla sola area zero

-router di confine dell’ASBR (boundary router), che si collegano agli altri sistemi autonomi

Naturalmente le funzioni possono sovrapporsi

– un router di confine e’ anche router interno

– un boundary router e’ anche un backbone router

– un backbone router non connesso ad altre aree o ad altri AS e’ un router

interno (per l’area 0)

OSPF: Instradamento fra aree/costruzione delle tabelle non l’ha spiegate

I SISTEMI AUTONOMI

E’ un Insieme di router e scelte protocollari, che operano sotto il controllo di una sola autorità amministrativa. E’ un’organizzazione che governa un insieme di circuiti di circuiti, di reti stabilendo le proprie regole.

NB. Internet non è altro che un insieme di sistemi autonomi; è fondamentalmente un insieme di organizzazioni che controllano blocchi di router e circuiti, che lo connettono, e che fanno delle scelte interne a livello protocollare e che devono comunicare tra loro.

Come si parlano i Sistemi Autonomi?

All’interno di un SAUTONOMO, si fanno delle scelte.

1Qual è l’obiettivo di un sis.Aut.?

Far funzionare tutto, cioè convergere velocemente.

Chi gestisce problemi?

La singola organizzazione che decide.

Quando si parla di Sistemi Autonomi Differenti parliamo di un’organizzazione sotto il controllo di entità strategiche differenti che poxono avere obiettivi economici contrastanti ma che sono costrette a parlare per costituire la global Internet.

Mentre all’interno di un sis.Autonomo si è d’accordo per definizione, fra sistemi autonomi differenti invece, avendo entità strategiche differenti, conta il rispetto di regole, accordi e la mutua invisibilità.

SLIDE SALTATE

L’INSTRAMENTO TRA SIS. AUT.

Abbiamo certamente bisogno dell’instradamento che fa parlare i sis autonomi anche se risulta un protocollo un po’ più complicato. Governa le politiche di mutua visibilità. Questi protocolli si chiamano EGP(EGP/CGP/BGP). BGP è l’unico collante di Internet facendo parlare i sist autonomi tra loro. Abbiamo bisogno di una logica di instradamento che vada a mascherare i fatti locali per la rete. Parlando di Global Internet abbiamo bisogno di un protocollo di routing che annunci ciò che vi è all’interno del sistAutonomo ma che mi rende invisibile la struttura all’interno del sistautonomo stesso. All’interno di un AS quindi ci può essere una topologia particolarmente articolata ma nascosta, l’unica cosa che si vede è il peering points.

Peering points, sono dei router di bordo che fanno parlare un AS con un altro e stabiliscono una sessione EGP che permette due AS di interconnettersi anche tramite n connessioni. E’ importante infatti creare ridondanze.(riNdondanze ahaha)

L’interconnessione di SistAutonomi

Quando più organizzazioni si uniscono per formare una Inter-rete, occorre stabilire tra loro punti di collegamento o di peering.

Dobbiamo mettere due entità strategiche in condizione di comunicare, in questi casi si parla di peering cioè collegamento tra pari. In realtà si presuppone che tutti i sisautonomi sono alla pari tra loro, creando collegamenti altrettanto alla pari. LA realtà non è questa, succede che qualcuno potrebbe avere un ruolo più strategico rispetto ad un altro che a sua volta ricopre un ruolo di sudditanza. E’ questo il caso definito “Customers e providers relationship”.

In caso di ruolo alla pari però parliamo di peering.

Accordi di peering: si possono avere due finalità.

1. Annuncio ciò che ho dentro, rendo visibili le reti del mio sisautonomo
2. Diritto di transito, l’elemento centrale (provider di transito) permette alle altre strutture di passare attraverso se stesso. Fa da ponte tra due AS. Si parla di AS di transito.

Peering per la connettività Tier

Le strutture possono essere abbastanza articolate, parliamo di tiering.

Parliamo di livelli di operatività. Abbiamo un

-Tier più basso in cui ci sono i clienti;

-Tier 2, provider regionali;

-Tier 1, abbiamo provider che fanno parlare altri provider cioè di “provider di provider” che mantengono viva la Global Internet.

EGP

Per le reti annunciate, il protocollo EGP che nel nostro caso è il BGPv4 le annuncia come se fossero reti locali (quindi senza comunicare come e dove).

Non abbiamo più visibilità del grafo di rete ma l’AS graph. I nodi sono gli AS e non i router e gli archi sono gli accordi di peering e non i link.

BGPV4

Unico protocollo utilizzato, garantisce la comunicazione tra i sisautonomi, coordinamento, lavora in logica next stop routing, si basa su una logica di trasporto cioè il TCP.

Invia messaggi periodici di keep alive.

Questi protocolli in genere si parlano solo in certe situazioni e quando le cose cambiano significativamente per cui in genere sono in silenzio. Come capisco se il collegamento è caduto?

Si usano i pacchetti di keep alive, notificare che il link sia up and running.

Il BGP supporta il CIDR, autenticare i messaggi in modo da non mandare informazioni fake.

NUMERAZIONE DEGLI AS

L’AS è di fatto un numero che deve essere assegnato univocamente dalla stessa autorità che indirizza gli Indirizzi IP. BGP richiede un numero identificatico per ogni AS (Autonomous System Number, asn) trac 1 and 65,535

• numeri maggiori di 64,511 sono detti “privati”

• Un asn può essere ottenuto da

– asn globale – all’autorità internet regionale: ripe,

arin, apnic

– asn privato – all’isp

FUNZINALITA’ BGP

I protocolli di BGP hanno una struttura protocollare complicata perché si apre il peering, c’è l’invio dei messaggi e poi di verifica del funzionamento.

Tipicamente i messaggi inviati sono 4:

1 di apertura, 1 di update con doppia valenza: advertisment cioè annuncio di nuovo prefisso o cancellazione del prefisso. 1 Notification risposta ad un evento e 1 di keep alive.

INTESTAZIONE MESSAGGI BGP

Naturalmente il BGP ha come struttura un header, marcatore che identifica il tipo di protocollo, lunghezza, tipo e le info riguardo i prefissi annunciati o cancellati.

IMPO: PEERING TRA DUE AS

abbiamo un peering tra due sist autonomi

Gli annunci (le informazioni) sono inviati e/o accettati (quindi scambiati) solo se alcune condizioni sono verificate cioè che una sessione di peering sia attiva.

Quando si annuncia che una rete è disponibile, l’effetto è la cattura di traffico. Appena si annuncia la rete libera, si manda il traffico verso la rete. L’annuncio in uscita si traduce in traffico entrante.

• Gli annunci possono essere filtrati sulla base di:

– Una lista di prefissi validi, che io posso accettare.

– Una lista di numeri di AS, non voglio ricevere traffico che passa per uno specifico AS

PATH ATTRIBUTER

Gli attributi possono indicare:

– Sistemi autonomi attraversati verso la destinazione

– Provenienza delle informazioni sull’instradamento: locali (igp)

o apprese da altri sistemi autonomi (egp)

Le Attribuzioni del cammino sono delle caratteristiche che individuano la specifica destinazione che viene annunciata e ne possono caratterizzare il comportamento.

Attributes presi in considerazione:

-l’origine (cioè chi mi ha annunciato l’informazione)

DOMANDA D’ESAME:

-AS PATH, il cammino degli as attraversati lungo il percorso. Ogni annuncio porta la lista degli as attraversati.

- il Next stop (che hanno tutte le roots)

-il MED

-LOCAL PREFERENCE

-Community, mi serve per evidenziare certi specifici percorsi con determinate caratteristiche

-ID dell’AS che ha riunito i percorsi.

Come lavora il BGP?

La sua scelta è data dal momento in cui ho

-più root per raggiungere una destinazione

Come sceglie? Si basa sulla local preference, se localmente l’amministratore di rete dice che preferisce raggiungere una root per un determinato percorso, sarà proprio questa la scelta. A parità di local preference, si sceglie il cammino più breve in AS attraversati (AS path più breve)

AS PATH

ALTRA DOMANDA IMPORTANTE: come funziona l’AS PATH

Un prefisso appena viene originato, l’as path si porta l’originatore.

Viene annunciato ad un secondo AS che viene immediatamente aggiunto in testa, così via con i suo vicini. Lo stesso annuncio attraverso AS diversi avrà percorsi diversi.

L’AS PATH non ha legami con la lunghezza fisica del percorso.

Il path più corto non corrisponde necessariamente al percorso di rete realmente più breve

breve

METRICA E MED

Il MED(Multi-Exit-Discriminator) serve per dare indicazioni circa il collegamento attraverso il quale si può essere raggiunti dall’esterno. Il valore di default del MED è 0. Avendo multipli punti di uscita si può condizionare come fluisce il traffico in questi punti.

Ogni AS(Autonomous System) può decidere come far uscire il traffico, ma non è facile decidere come farlo entrare. Il traffico entrante si può influenzare annunciano o meno su una determinata uscita. Ad esempio se si hanno due uscite e si annuncia su entrambi(per avere la ridondanza) si può influenzare mettendo su un link una metrica più bassa in modo tale da far capire agli AS esterni che si preferisce quel link al posto dell’altro, se gli AS esterni accettano il “consiglio” e usano quel link è meglio altrimenti va bene lo stesso.

N.B. Metrica è un costo e si preferisce quella più bassa, mentre la Local Preference è una preferenza e si sceglie quella più alta.

LOCAL PREFERENCE

Attraverso la Local Prefereces si possono controllare gli annunci in ingresso e gestire le politiche sul traffico in uscita; ad esempio avendo due AS collegati da due link si stabilisce una Local Preference più alta per far capire quale link preferire al posto dell’altro.

Con la Local Preferences a differenza della metrica DECIDO come gestire il traffico in uscita, ovvero mano mano che entrano gli annunci si imposta una Loc-Pref più alta su dei link rispetto ad altri il traffico che uscirà utilizzerà il link con la Loc-Pref più alta.

AS PATH PREPEND

Il traffico uscente può essere gestito attraverso la Loc-Pref, ma per quello entrante con la MED si dà solo un consiglio quindi non si ha la certezza che gli altri AS lo rispettano.

All’interno dello stesso AS non può mai ricorrere più volte lo stesso ASPATH altrimenti si verifica un loop tranne in un caso: quando il numero di AS è consecutivo. Con questo trucco posso inserire in un link un ASPATH con un solo numero mentre nell’altro ripeterlo più volte in modo tale che gli altri AS sono costretti a scegliere il link con ASPATH più corto.

LIMITI DI BGP

BGP non decide sulla base della distanza fisica; non decide in basa al numero di link attraversati, decide sempre e solo in base alle politiche di organizzazione degli AS (Bada a fatti a organizzativi). Il BGP può fare anche bilanciamento di carico(può essere di flusso e di sessione), ovvero se non si sceglie nessun link come preferenziale il traffico sarà suddiviso tra i vari link. Ci vuole coerenza nello schema per l’annuncio della raggiungibilità dei vari AS.

CLASSIFICAZIONE DELLE RETI

Stub Network: è una rete collegata una sola volta in relazione coustomer – provider.

Multi-Homed Stub Network: è una rete che comunque ha un collegamento a un singolo provider (quindi un singolo AS), però ha due collegamenti a scopi di backup o per divisione di carico.

Multi-homed network: una rete con più collegamenti a provider differenti.

STUB NETWORK, ARCHITETTURA

Un router della rete è scelto come gateway di default è connesso ad un singolo router provider con una o più connessioni.

INSTRADAMENTO STATICO PER STUB NETWORK

Per le Stub Network un instradamento statico è sufficiente non c’è bisogno di usare il BGP.

MULTI-HOMED STUB NETWORKS

Si ha una rete con due collegamenti allo stesso provider, ma così si ha il single point of failure quindi si può optare per due router collegati due volte allo stesso ISP (provider).

INSTRADAMENTO

È necessario utilizzare il BGP. In questo caso un pacchetto può passare attraverso un link o l’altro o addirittura entrare da un link e uscire da un altro.

POLITICHE DESIDERATE- BACKUP

Tipicamente con due link uno fa il backup per l’altro oppure bilanciare il carico.

ALTERNATIVE A BGP

Si potrebbe utilizzare un protocollo interno perché essendo sempre una rete Stub non si ha il bisogno di annunciare la rete a due organizzazioni quindi non è obbligatorio il BGP. Si possono anche utilizzare cammini statici. Tipicamente si usa il BGP perché fa molte più cose.

LA STRATEGIA USATA DA BGP

Con il BGP si può utilizzare l’aggregazione; si possono annunciare degli aggregati sui link e in caso di fallimento in uno dei due link si annuncia sull’altro e non si interrompe mai la connettività.

MULTI-HOMED NETWORK

La rete è collegata con due providers differenti si è obbligati ad usare il BGP.

INSTRADAMENTO/PARTIZIONE DEL CARICO

Si può scegliere di utilizzare un solo link o entrambi anche con asimmetria, cioè il traffico potrebbe uscire da un link e entrare nell’altro Un pacchetto in uscita può essere inviato attraverso uno dei due link per raggiungere Internet. Si potrebbero utilizzare entrambi per la divisione del carico: annunciando metà indirizzi IP da un lato e metà dall’altro; anche così resta la funzione di backup, cioè si annuncia la rete da entrambi i lati, ma con Local Preferences e MED diversi.

USO DI BGP PER IL PARTIZIONAMENTO

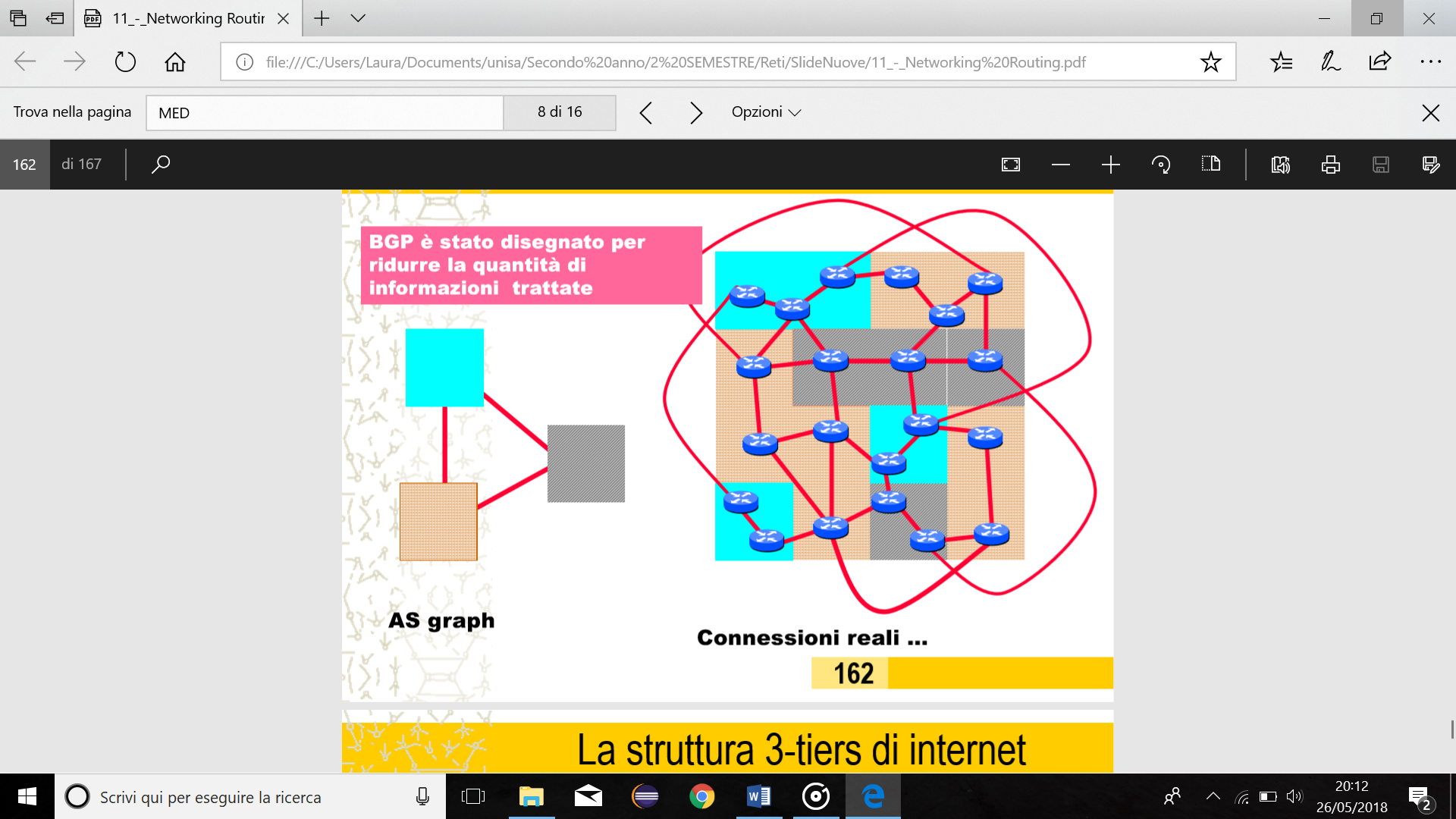
Ad esempio si ha una rete /19 su ogni link, si partizione e si annuncia due /20 per ogni link oppure annunciare entrambe da tutte e due i lati ma con MED e Local Preferences differenti in modo tale che viene scelta in condizioni normali quella data come preferita, ma in caso di guasto di uno dei collegamenti si sfrutta solo l’altro.

AS GRAPH

Quando si parla di BGP si vede AS GRAPH in cui i nodi sono gli AS e gli archi sono gli accordi di peering.

AS GRAPH VS INTERNET TOPOLOGY

La rappresentazione di un AS Graph corrisponde in termini di grafo di rete ad una struttura molto più complessa.



LA STRUTTURA 3-TIERS DI INTERNET

Questa struttura è la più realistica. Ci sono i tier1 che sono i grandi providers intercontinentali, i tier2 che sono i providers regionali a grande copertura e spesso si hanno i tier3 che sono i provider locali e poi ci sono i clienti. Tra questi si possono trovare accordi di peering o di coustumers- providers.

IL CLUD DEI TIER 1

I tiers1 comandano la rete; si collegano tra loro solo tramite peering.

PUNTI DI INTERSCAMBIO: IX E NAP

### I Network Access Point(NAP ) o Internet Exchange sono i punti di interscambio; sono dei punti neutrali in cui i vari providers a vari livelli si incontrano a scopo di realizzare dei punti di peering. Fisicamente si realizza attraverso uno switch ad altissime prestazioni che interconnette diversi providers. Deve essere un’entità che governa alla pari tutti gli altri; questi punti sono i crocevia importanti. I providers possono interconnettersi l’uno all’altro quasi in full-mesh pagando una connessione fisica attraverso IX. Questi sono i punti più importanti di internet.

### ANCORA UNA VISIONE GERARCHICA

### Ci sono i clienti sotto poi i providers in genere AS, si hanno dei providers di livello alto e altissimo, ma interconnessione avviene attraverso dei punti neutrali NAP.

### IL PUNTO DI PARTENZA E QUELLO DI ARRIVO

### Il disegno della prima Internet era costituita da 4 nodi e ora conta molti milioni di nodi (i nodi sono i routers).

### LIVELLO DI TRASPORTO

### FUNZIONE DEL LIVELLO DI TRASPORTO

### Il livello di trasporto ha lo scopo di fornire allo strato superiore un servizio di trasferimento dei dati end to end. Per assolvere le sue funzioni lo strato di trasporto utilizza i servizi dello strato di rete La porta è l’indirizzo a livello di processo che noi troviamo erogato come servizio di multiplexing e demultiplexing a livello di trasporto.

### SERVIZIO DI TRASPORTO

### I servizi dipendono dalle applicazioni ad esempio possono essere connectionless o connectio oriented. Questo livello offre sia un trasporto connectionless senza nessuna caranzia e controllo, ma ci permette di puntare verso lo specifico processo (non si manda più alla macchina, ma al processo sulla macchina); sia un servizio connection oriented con garanzia assoluta di inoltro, affidabilità e ordine di sequenza.

### Per il servizio connection oriented vi sono vari operazioni:

### – LISTEN: ci si mette in ascolto su una determinata porta che individua un processo;

### – CONNECT: lo strato superiore chiede allo strato di trasporto di effettuare una connessione (si traduce nell’invio da parte del trasporto di un messaggio “Connection Request” al destinatario)

### – SEND: lo strato superiore chiede al trasporto di inviare dati

### – RECEIVE: lo strato superiore chiede allo strato di trasporto di trasmettergli i dati in arrivo – DISCONNECT: lo strato superiore chiede di chiudere la connessione (si traduce nell’invio da parte dello strato di trasporto di un messaggio “Disconnection Request”) •

### Per il servizio connectionless, le due primitive SEND e RECEIVE possono essere sufficienti.

### In questo livello si ha la gestione dei riscontri, le ritrasmissioni, il go-back n, il selective reject ed altri controlli.

### PROTOCOLLI DI TRASPORTO

### Non gestiscono l’indirizzamento( lo prendono dal livello di rete), introducono il controllo degli errori, i numeri di sequenza e il controllo di flusso. Si introduce anche il concetto di service port, ovvero il meccanismo di multiplexing e demultiplexing che presi tutti i pacchetti individua la porta giusta ( il processo ) e glieli affibbia o viceversa i pacchetti che partono dalla stessa porta li mette tutti insieme e li manda a livello di rete.

### In questo livello si può gestire anche una necessità di bufferizzazione. I protocolli che lavorano in questo livello sono TCP (Transmission Control Protocol) che offre servizi affidabili (connection oriented) e l’altro UDP (User Datagram Protocol) che offre servizi inaffidabili (Connectioless).

### TCP E UDP

### Il TCP è standardizzato da varie RFC come 793 poi 1122 e 1323 sono 3 perché questi protocolli evolvono quindi è stata standardizzato dalla 793 poi esteso dalle altre due.

### Mentre per il UDP abbiamo una solo RFC 768 poiché è meno sofisticato.

### FUNZIONALITÀ DEL TCP

### Riceve flussi datagram da un’applicazione, li organizza in un’unità (segmento) che sono grandi massimo 64kb e li spedisce al livello IP. In ricezione riceve i datagram IP, risolve tutti gli errori e tutto procede senza errori.

### HEADER TCP

### Nella testata del TCP si trovano gli indirizzi sorgente e destinazione delle porte che sono di 16 bit; poi c’è il numero di sequenza che serve per ricostruire l’ordine giusto; il numero di Acknowledge , cioè il riscontro “rimorchiato”, l’ultimo elemento riscontrato. C’è la window size, ovvero la dimensione della finestra scorrevole (più la rete va bene più si allarga la finestra viceversa si rimpicciolisce fino ad arrivare ad 1 e poi lavora come diventa un protocollo stop-and-wait); poi il checksum; c’è urgent pointer cioè se ci sono dei dati che devono essere gestiti prima degli altri si mette un puntatore a questi dati in modo tale da trattarli subito; c’è la lunghezza della testata perché non è di lunghezza fissa, ci possono essere delle opzioni. Ci sono vari bit che servono elementi di segnalazione. Questi bit sono flag URG per i dati urgenti; Flag ACK quando il segmento trasporta un riscontro; Flag PSH serve per evitare ulteriori attese; Flag RST quando qualcosa è andato male si fa il reset della connessione; Flag SYN (IMPORTANTE!) serve per stabilire una negoziazione infine c’è il Flag FIN quando si vuole chiudere una connessione.

### HEADER OPZIONALI

### Le opzioni si possono usare ad esempio per far terminare i pacchetti ad una specifica lunghezza (padding). C’è MSS per adeguare la dimensione del segmento alla MTU ed evitare le frammentazioni; poi Window Scale per far cambiare dinamicamente le dimensioni della finestra scorrevole; Selective Acknowledge per gestire il selective reject in alternativa al go-back-n ed infine un TimeStamp per fare i calcoli sul tempo che il pacchetto impiega per arrivare o non arrivare.

### INDIRIZZAMENTO

### Un indirizzo di trasporto identifica l’host e la specifica connessione sull’host. La porta è un numero di 16 bit(da 1 a 65535; la porta 0 non è utilizzata). Il multiplexing e demuliplexing viene garantito dalle porte.

### COMUNICAZIONE FRA TCP/IP STRACKS

### Si ha una comunicazione end to end tra due livelli di trasporto, cioè si vede la prima astrazione dell’altro lato.

### LE PORTE

### Le porte si associano ai singoli processi che devono comunicare. Le porte sono assegnate dall’autorità centrale IANA (Internet Assigned Numbers Authority). Hanno stabilito che un range di porte Well-Known vengono assegnate a specifici servizi standard; ad esempio la porta 21 di TCP corrisponde al servizio FTP, la porta 80 di TCP a HTTP. Le porte TCP sono distinte da quelle UDP; ogni protocollo ha il suo range di porte.

### PORTE NUMBERS/ PROTOCOL PORT NUMBER/LE PORTE DEL CLIENT

### Le prime 1024 porte sono assegnate Well-known, poi ci sono alcune porte per determinati servizi e ci sono porte effimere. Ad esempio se si deve stabilire una connessione TELNET ad esempio da client port 23443 si punta alla porta 23 del server.

### APERTURA DELLA CONNESSIONE

### Quando si vuole stabilire una connessione si una il protocollo 3-way handshaking. Se la macchina uno e la macchina due vogliono comunicare chi decide di aprire la connessione manda un segnale di sincronizzazione comunicando il sequence number di partenza ad esempio SYN (SEQ=x); la macchina dall’latro lato quando riceve questo segnale si sincronizzazione deve notificare che l’ha ricevuto e quindi manda un altro segmento che ha sempre il bit SYN e ACK ad esempio SYN(SEQ=y, ACK = x+1) a questo punto la prima macchina deve mandare un messaggio di riscontro del SYN e ACK precedente e quindi manda ad esempio ACK=y+1. Solo dopo questi 3 scambi entrambi sono certi che potranno stabilire la connessione.

### Se il TCP ricevente non verifica la presenza di nessun processo in attesa sulla porta destinazione manda un segmento di rifiuto della connessione (RST).

### UN ESEMPIO DI CONNESSIONE

### Connessione Telnet fra da 10.6.1.9 a 10.6.1.2 catturata con tcpdump \* porta client 4548 -porta server 23 (telnet).

### 10.6.1.9.4548 > 10.6.1.2.23: S 2115515278:2115515278(0) win 32120 <mss 1460,nop,nop,sackOK,nop,wscale 0> (DF)

### 10.6.1.2.23 > 10.6.1.9.4548: S 1220480853:1220480853(0) ack 2115515279 win 32120 <mss 1460,nop,nop,sackOK,nop,wscale 0> (DF)

### 10.6.1.9.4548 > 10.6.1.2.23: . ack 1220480854 win 32120 (DF)

### CHIUSURA DELLA CONNESSIONE

La connessione è full duplex e si deve chiudere in entrambe le direzioni indipendentemente. Si hanno due strette di mano a due vie o 4 way handshaking. Ad esempio Host 1 manda un segnale di FIN riscontrando l’ultimo pacchetto riscontrato FIN(SEQ=x, ACK=z) , dall’altro lato manda il proprio sequenze number e ACK (SEQ=v, ACK=x+1). Ora da dall’host 1 a 2 è chiusa la connessione; quando host 2 finisce di trasmettere anch’esso quando FIN(SEQ=v+1, ACK=x+1), appena è ricevuto da host 1 quest’ultimo manda (ACK=V+2) ed è chiusa la connessione da entrambi i lati.

IL TIMEOUT MSL

Il Maximum Segment Lifetime (MSL=2 min in RFC 793) indica il massimo tempo per il quale un segmento TCP può sopravvivere nella rete prima di essere scartato. Attendere 2MSL nello stato TIME WAIT garantisce che tutti i segmenti relativi alla connessione siano spariti dalla rete. Nello stato TIME WAIT si impedisce che nel client possa aprirsi una connessione con lo stesso indirizzo di quella appena chiusa.

CASO DI PACCHETTI DUPLICATI

Avendo il sequence number ci si accorge se un pacchetto è fuori sequenza e viene scartato; questo è garantito sia dalla lunghezza del numero stesso sia dal time to live dei segmenti che non fa coesistere due segmenti con lo stesso numero. Quando si riceve un pacchetto duplicato si manda un reset.

ACK RITARDATI

In caso di un ritardo di riscontro, avendo la finestra scorrevole, si tiene conto di tutti pacchetti che non sono stati ancora riscontrati e la finestra non viene chiusa finché tutti i pacchetti non vengono riscontrati ovviamente entro un timer(tipicamente 200ms); se il pacchetto non arriva entro lo scadere del timer si chiede la ritrasmissione di quel pacchetto.

### L’ALGORITMO DI NAGLE

### Si accumulano i dati fino a che non si riceve l’ack per il segmento inviato in precedenza In alcuni casi deve essere disabilitato. Con questo algoritmo posso cambiare le dimensioni della finestra. Con una finestra grande si riduce overhead poiché può capitare che con un solo riscontro riesco a riscontrare più segmenti. Adatta la finestra rispetto alla qualità della trasmissione, questa qualità si valuta in base ai pacchetti perduti.

### SEQUENCE E ACK NUMBERS

### I sequence number da un lato e l’altro non hanno nessun legame cioè ogni host genera i propri. L’importante è che nei riscontri i sequence number siano quelli giusti; ad esempio se host 1 manda un pacchetto con sequence number 10, host 2 quando risponde deve mandare ACK relativo a 10 che è 11 (10+1) anche se host 2 ha il sequence number che è 1.

### TRASMISSIONE DI FLUSSI DI DATI

### TCP usa una finestra di ricezione e una di trasmissione che possono cambiare di dimensioni in ragione della qualità del link stesso. La capacità della finestra si traduce nella capacità di bufferizzazione dei due lati (mittente ricevitore); più aumenta la dimensione della finestra più aumenta la capacità di bufferizzazione di frame inviati e non riscontrati o di frame ricevuti e di cui non è stato ancora inviato il riscontro.

### WINDOWING

### Se si ha una finestra di dimensione 3 si possono inviare i tre pacchetti senza ricevere riscontro; il ricevitore manderà il riscontro relativo all’ultimo pacchetto ricevuto e magari sulla base che ha perso un invio potrebbe ridurre le dimensioni della finestra. Attraverso questo meccanismo si controlla la cogestione.

### TCP TIMEOUT E RITRASMISSIONE

### Quando scade il time out si provvede anche alla ritrasmissione dei dati. Per determinare il valore del time out si utilizza l’algoritmo Round- Trip Time.

### CONTROLLO DI CONGESTIONE

### Il TCP adatta la velocità di trasmissione alla capacità della rete utilizzando una finestra di congestione. La dimensione della finestra di congestione è ridotta se scade il time out di ritrasmissione.

### USER DATAGRAM PROTOCOL

### Questo protocollo garantisce un servizio inaffidabile. Ha una testata di 8 byte che permette di mandare il pacchetto direttamente ad una porta di destinazione. Di fatto costituisce semplicemente una interfaccia ad IP, con l’aggiunta di fare multiplexing del traffico delle applicazioni su IP.

### ORIENTATO AL DATAGRAMMA

UDP gestisce un datagramma alla volta, indipendentemente uno dall’altro senza controlli e garanzie. Il segmento viene passato al livello inferiore per quella che è la sua dimensione, quindi potrebbe essere frammentato se è troppo grande.

IL SEGMENTO UDP

Il segmento UDP è costituito da un header di lunghezza fissata (8 byte) più il campo dati, che deve avere dimensione massima tale da stare dentro il campo dati di IP.

UDP HEADER

L’header è costituito da quattro campi di due byte: porta sorgente e destionazione: le porte di associazione alle applicazioni mittente e destinataria dei dati; length: lunghezza del segmento in byte (compreso l’header) ; checksum: l’utilizzo del campo checksum è opzionale (dipende dalle implementazioni) e l’applicativo può decidere di non utilizzarlo.

CARATTERISTICHE DI UDP

UDP è inaffidabile però è fondamentale perché è molto efficiente e veloce. Viene utilizzato quando non è necessario il setup della connessione per esempio la comunicazione streaming video/audio; se si perde qualcosa non succede nulla. È utilizzato molto anche per la trasmissione broadcast per mandare ad esempio streaming televisivi. Overhead di protocollo è bassissimo quindi la redditività è molto alta.

APPLICATIVI STANDARD SU UDP

Il DNS usa UDP per essere veloce ed efficiente si preferisce rimandare la richiesta che fare il setup della connesione. Altri applicativi che usano UDP ad esempio TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), NTP (Network Time Protocol), NFS (Network File System).

**LIVELLO APPLICATIVO**

Sul livello applicativo non facciamo altro che usufruire dei servizi che il livello di trasporto ci mette a disposizione per realizzare servizi applicativi noti: Terminal Emulation, Accesso a portali Web ecc..

APPLICAZIONE

Programmi applicativi usati dagli utenti:

DNS (Domain Name System), servizio infrastrutturale che permette di fare la traduzione tra nomi simbolici rispetto gli Indirizzi IP ovviamente impossibili da ricordare;

Posta Elettronica;

Resto del mondo che appartiene al Web.

DOMAIN NAME SYSTEM (DNS)

Traduzione in nomi simbolici.

Si realizza tramite un grande database distribuito chiamato DNS, meccanismo che ci permette di svolgere query.

Per comunicare su rete serve l’indirizzo IP!

Quando gli host sono pochi la tabella di conversione può essere memorizzata

localmente ad ogni host (file /etc/hosts in Unix)

Il DNS è distribuito: ogni sito mantiene il suo database relativo agli host locali

eseguendo su una macchina il server DNS che può essere interrogato da altri

sistemi su Internet

IL RESOLVER

E’ la componente che si occupa di formulare la query e tipicamente essa viene formulata da un’entità esterna che si chiama SERVER o DOMAIN NAME SERVER che si occupa di gestire la risposta della query.

Cosa fa il resolver? Componente applicativa del sistema che ha bisogno di due elementi. Gli indirizzi IP di almeno due server in grado di risolvere le query che il resolver vuole svolgere.

Il resolver fa una query sulla porta UDP 53 chiedendo di risolvere uno specifico problema.

La gestione gerarchica nasce da un partizionamento dello spazio dei nomi anch’esso gerarchico che parte dalla radice.

Sotto la radice vi sono vari sottodomini, corrispondenti ad una zona di autorità. La zona di autorità è un insieme di info relative a quello specifico dominio, ci possono infatti essere informazioni di tipo A, ADDRESS, indirizzo di un host contenuto in quel dominio. (17)

INTERROGAZIONE RICORSIVA

Query ricorsiva.

Come funziona? Il resolver propaga la query al name server di livello superiore che fa lo stesso negoziando con i vari server di gerarchia.

Perché la gerarchia di name server?

Ognuno di questi name server quando ottiene le risposte, le conserva in una cache e le riusa senza reiterare le risposte ogni volta. A questo punto, l’ultimo name server che deve effettuare la query ricorsiva, parte dal top level domain cioè parte da una lista scritta su un file (che contiene gli indirizzi IP dei root server). I root server sono i server autoritativi per il root domain, conoscono tutto ciò che è in esso cioè i domini top level. Fondamentalmente un qualsiasi server parte dal root domain, pesca uno dei root server e richiede chi è autoritativo per il top level interessato (IT)

INTERROGAZIONE ITERATIVA

Caso di query iterativa. Nella query iterativa la negoziazione con i vari name server autoritativi per le zone interessate è gestita direttamente dal resolver.

La query ricorsiva per il resolver locale è molto più vantaggiosa.

LA POSTA ELETTRONICA

La posta elettronica nasce ancor prima di Internet tramite un protocollo model to modem UNIX to UNIX copy.

Si basa sul modello agent-server.

Un agente associato a ciascun utente e un agente di trasferimento associato alla funzionalità di relay.

STRUTTURA:

-mittente (utente finale) che si aggancia all’agente utente.

Il mittente prepara il suo (in binari ecc) file di testo (l’agent lo trasforma in messaggio di testo) che viene messo nella coda di posta da spedire dell’agent di trasferimento(Mail Transfer Agent MTA). Periodicamente scorre la coda, prende i messaggi e stabilisce una connessione con l’agente di trasferimento dall’altro lato. Come sa chi è l’agente di trasferimento dall’altro lato? Legge IND DI DESTINAZIONE, lascia il dominio (lo estrae) , fa una query al DNS chiedendo un oggetto di tipo MX che gli fornisce l’indirizzo IP di link e mail transfer agent di quel dominio.A questo punto stabilisce una connessione TCP e a questo punto si passa da un lato all’altro. Quando questo file viene ricevuto, viene messo dall’MTA in una mail box dell’utente e a questo punto l’agente utente attraverso una serie di protocollo (es POP) va a consultare la mail box per leggere il singolo messaggio.

I relay agent possono essere annidati.

La coda è utilissima perché il protocollo SMTP garantisce l’inoltro certo del messaggio.

FORMAT DEI MESSAGGI

E’ definito in RFC 821 - RFC 822. I campi di intestazione consistono in linee di testo ASCII contenenti il nome del campo seguito dal carattere : e poi da un valore

L’agente utente costruisce il messaggio e lo passa all’agente di trasferimento

che utilizza alcuni campi dell’intestazione per l’invio

MIME

Multipurpose Internet Mail Extensions, estensione che aggiunge intestazioni testuali al mio messaggio che mi permettono di strutturarlo e dividerlo in sezioni.

Aggiunge dei campi di intestazione per definire la struttura del corpo del messaggio

(è gestita dall’agente utente)

Mime-Version

Content-Type

Content-Transfer-Encoding

Content-ID

Content-Description

SMTP

Il protocollo SMTP definisce la sequenza di comandi (inviati in ASCII) necessaria

per il trasferimento dei messaggi

• Insieme minimale di comandi usati dal client

HELO <host>

“Saluta” il server

MAIL From: <indirizzo>

indica il mittente del messaggio

RCPT To: <indirizzo>

Indica il destinatario (recipient)

DATA

Invio corpo del messaggio terminato da un . su una linea

QUIT

Chiude la connessione

E’ un protocollo ovviamente insicuro.

IL WEB

Nato nel 1989 al CERN di Ginevra come mezzo per scambiare informazioni.

Esperimento in cui si è trovato il modo di interconnettere risorse eterogenee tra loro in una struttura di rete semantica in cui un dato si aggancia ad un altro sulla base di un’affinità o collegamento.

Perché WEB?

E’ inteso come ragnatela, fili che mettono in comunicazione due risorse (tipicamente sono documenti rappresentati in uno schema generalmente ipertestuale rappresentato in HTML/XML ecc). Questi collegamenti logici vengono a realizzare sulla Global Internet una ragnatela di agganci definiti hyperlink.

PUNTI FONDAMENTALI QUINDI:

Ci troviamo ad operare con un grafo in cui i nodi sono contenuti collegati tra loro da puntatori(hyperlink) e la maggior parte dei documenti sono rappresentate in un linguaggio Markup che ci permette di utilizzare anche altri formati come .pdf.

HTTP

Ogni sito Web ha un processo server in ascolto su una porta TCP

La porta standard è la numero 80

Il protocollo alla base di quello che è l’accesso alle risorse è basilare definito http.

HTTP definisce un protocollo di comunicazione basata su una logica client-server, dove fondamentalmente abbiamo un client, che può essere un browser, che può chiedere l’accesso ad una risorsa disponibile presso un server chiedendone il trasferimento.

L’http è utilizzato per trasferire ogni tipo di risorsa su WWW.

Una risorsa è un’entità individuata da un URL (uniform Resource Lacator)

Utilizzo del modello client-server:

Il server ricevuta la richiesta la trasmette, la concede a questo punto il client la rappresenta e la offre all’utente.

Da un client aggancio un server e fare una query ad un server circa l’ottenimento delle risorse. Tutta la transazione viene gestita dall’Hyper Text Transfer Protocol.

Il protocollo è senza stato, stateless (non c’è memoria delle transazioni).

Ogni risorsa è rappresentata in un formato standard, URL.

FORMATO DEI MESSAGGI http

Si basa su una struttura che prevede una Linea Iniziale (diversa tra richiesta e risposta)

E una serie di testate

Una linea vuota

Infine il corpo del messaggio

RICHIESTE http

La richiesta ha tre componenti:

un metodo di richiesta

il percorso locale a cui faccio riferimento

versione protocollare che sto usando

METODI http

I metodi definiscono le operazioni possibili su una risorsa

GET: trasferimento di una risorsa

HEAD: richiede le intestazioni

POST: si può inviare per mandare dei contenuti dall’altro lato

RISPOSTA http

La linea iniziale di una risposta costituisce una linea di stato.

Contiene:

-il protocollo utilizzato

-un codice di risposta

-headers

INTESTAZIONI

Seguono il formato specificato in RFC 822 anche per l’email

• HTTP 1.0 definisce 16 header (tutti opzionali)

• HTTP 1.1 definisce 46 header (obbligatorio solo l’Host)

COMUNI:

User Agent che identifica il browser

Server che identifica il server

Last Modified identifica la data dell’ultima modifica per la risorsa

Content-Type: definisce il tipo MIME

Content-Length: lunghezza in byte del corpo del messaggio