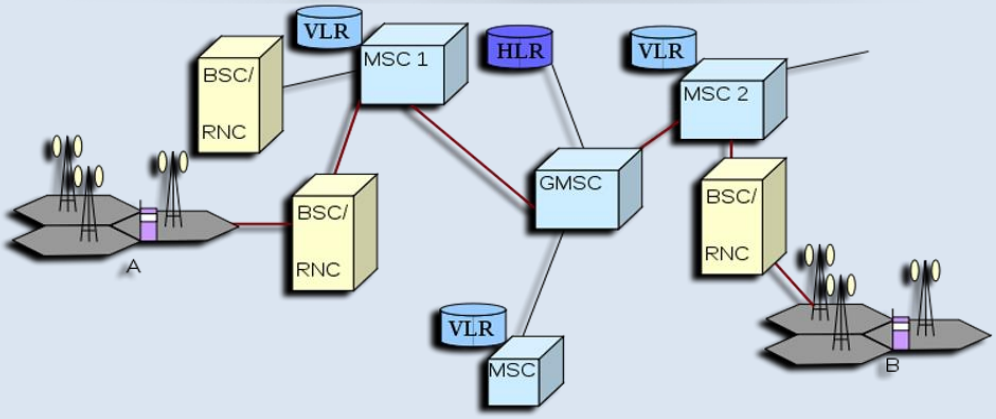
Reti e TeleComunicazioni
Guida alle BASI della



Lezioni di Reti e Telecomunicazioni (TLC)

Lezione 1

Le applicazioni di rete : cosa sono e quali sono le diverse Architetture

Nel modello **ISO/OSI** e **TCP/IP** il livello applicativo è quello che si occupa di implementare applicazioni di rete che verranno utilizzate dall'utente finale. Il principale scopo delle reti, sia in locale che in remoto, è proprio quello di condividere dati mediante applicazioni. Il livello applicazione è lo strato protocollare che mette a disposizione i protocolli mediante i quali le applicazioni possono comunicare tra host remoti presenti in rete.

Alcuni esempi di protocolli del livello applicativo sono **:**

- **SMTP** Simple Mail Transfer Protocol (Porte 25/587);
- **POP3** Post Office Protocol (Porta 110);
- **FTP** File Transfer Protocol (Porte 20/21);
- **HTTP** HyperText Transfer Protocol (Porta 80);
- **DNS** Domain Name System (Porta 53).

Oltre alle applicazioni pubbliche su Internet, sulla rete è presente un infinito numero di applicazioni proprietarie, sviluppate all'interno di organizzazioni.

Applicazione di Rete

Un'applicazione di rete è un insieme di programmi che vengono eseguiti su due o più computer contemporaneamente che operano interagendo tra loro utilizzando delle risorse comuni, accedendo ai database, mediante la rete che li connette. **L'applicazione di rete viene anche detta applicazione distribuita, dato che non viene eseguita su un solo elaboratore.** Affinché un processo, su un host, invii un messaggio ad un altro processo posizionato su qualunque altro host il primo deve essere in grado di identificare in maniera univoca il destinatario, l'identificazione univoca avviene attraverso un **socket**, del quale l'IP specifica l'host e la Porta specifica il processo, ossia il servizio offerto. L'applicazione di rete può essere vista come composta da due parti **:**

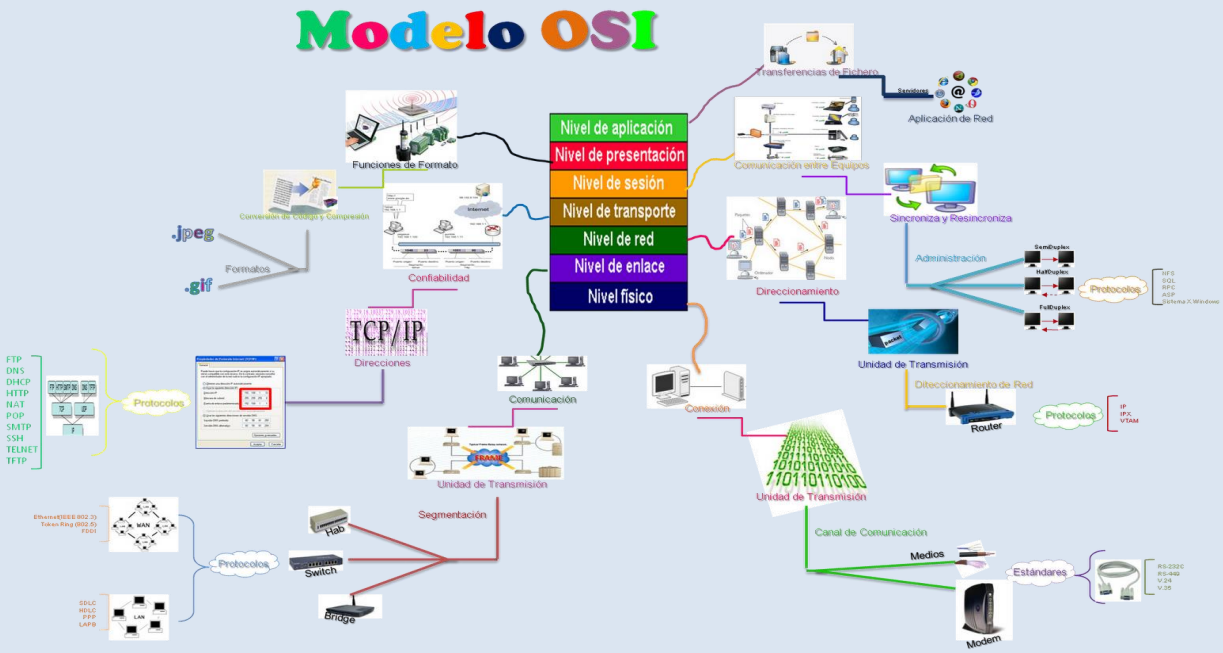
- **User Agent**, che funge da interfaccia tra l'utilizzatore dell'applicazione e gli aspetti comunicativi;
- **Implementazione dei Protocolli** che permettono all'applicazione di integrarsi con la rete.

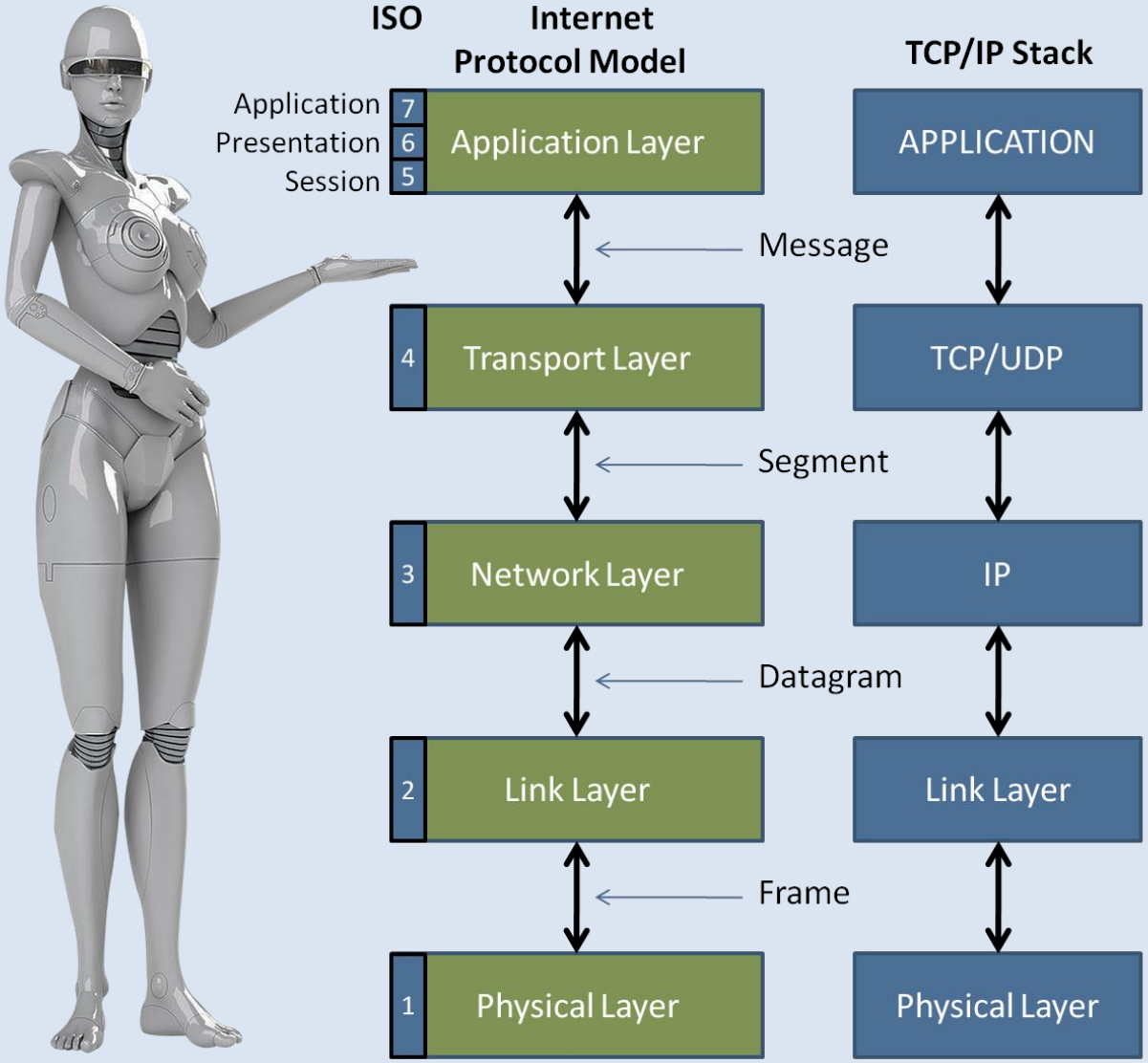
Architetture per le applicazioni di rete

Il primo passo che un programmatore deve effettuare per realizzare un'applicazione di rete è scegliere la sua architettura, le principali architetture ad oggi usate sono:

- **Client/Server**
- **Peer-to-Peer (P2P)**
- **Architetture ibride (dove convivono client-server e P2P)**

Modello OSI Rete di Computer e Protocollo Internet





Differenza tra UDP e TCP

TCP e UDP sono protocolli utilizzati per l'invio di bit di dati, noti come pacchetti, su Internet. Essi sono sopra il protocollo internet IP quindi, se si sta inviando un pacchetto tramite TCP o UDP, quel pacchetto viene inviato sicuramente a un indirizzo IP. TCP e UDP non sono i soli protocolli che lavorano su IP, tuttavia sono quelli più ampiamente utilizzati. Se un'applicazione utilizza il protocollo TCP o UDP dipende dal suo sviluppatore e non si può cambiare. La maggior parte dei programmi vogliono la correzione degli errori e preferiscono la robustezza del protocollo TCP, mentre alcune applicazioni hanno bisogno di velocità e si affidano a UDP. Il TCP è molto affidabile e i pacchetti sono tracciati in modo che nessun dato venga perso o danneggiato durante il transito. Questo è il motivo per cui i download di file non vengono danneggiati anche se si utilizza una rete lenta o che si interrompe spesso. una comunicazione UDP non dà alcuna garanzia di ricezione dei dati, ma ha il vantaggio che i computer possono comunicare tra loro più rapidamente.

Differenza tra Client e Server

Con il termine server si indicano tutti quei dispositivi terminali o programmi che assumono il ruolo di fornitore della risorsa o di un servizio all'interno di un insieme di servizi. Con il termine client si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server.

Peer-to-Peer (P2P)

Nelle architetture P2P abbiamo coppie di **host chiamati peer** che dialogano direttamente tra loro. Ogni peer è un'entità autonoma, capace di auto organizzarsi; i peers tra loro condividono un insieme di risorse distribuite presenti all'interno di una rete. **Il sistema utilizza tali risorse per offrire funzionalità in maniera totalmente decentralizzata. In sintesi nei sistemi P2P ogni host (peer) fornisce una risorsa e ottiene in cambio altre risorse.** Gli esempi più noti sono in ambito di condivisione file, come Emule e Gnutella.

Architettura Client/Server

La caratteristica principale è che **deve sempre essere presente un server attivo** che offre un servizio, restando in attesa che uno o più client si connettono ad esso, per potere rispondere alla richieste che gli vengono effettuate. Il server deve essere attivo e possedere **l'indirizzo IP, al quale poter essere raggiunto, fisso ossia statico**, contrariamente a quello dei client che generalmente è dinamico. Un client non è in grado di comunicare con altri client, ma solo con il server, più client possono comunicare contemporaneamente con lo stesso server. Se un server riceve troppe richieste contemporaneamente potrebbe entrare in **stato di congestione**, quindi si rende necessaria la virtualizzazione della risorsa mediante una **server farm**. Ossia un server con un unico hostname ma con più indirizzi IP, trasparenti rispetto ai client, sui quali vengono dirottate le richieste di connessione. **Un esempio di questa architettura è il WWW.** Per maggiori informazioni su questa architettura leggete **questo articolo sul modello client/server.**

P2P Decentralizzato

Nella architettura completamente decentralizzata ogni peer ha sia funzionalità di client che di server (hanno funzionalità simmetrica e sono chiamati **servent**), ed è i**mpossibile localizzare una risorsa mediante un indirizzo IP statico**, quindi si rende necessario l'uso di nuovi meccanismi di indirizzamento definiti a livello superiore rispetto all'IP. **I peer possono condividere qualunque tipo di risorsa** (dati, memoria, banda, etc) ed **il sistema P2P è capace di adattarsi ad un continuo cambiamento dei nodi partecipanti (churn)** mantenendo prestazioni e connettività accettabili senza necessitare di alcuna entità centralizzata.

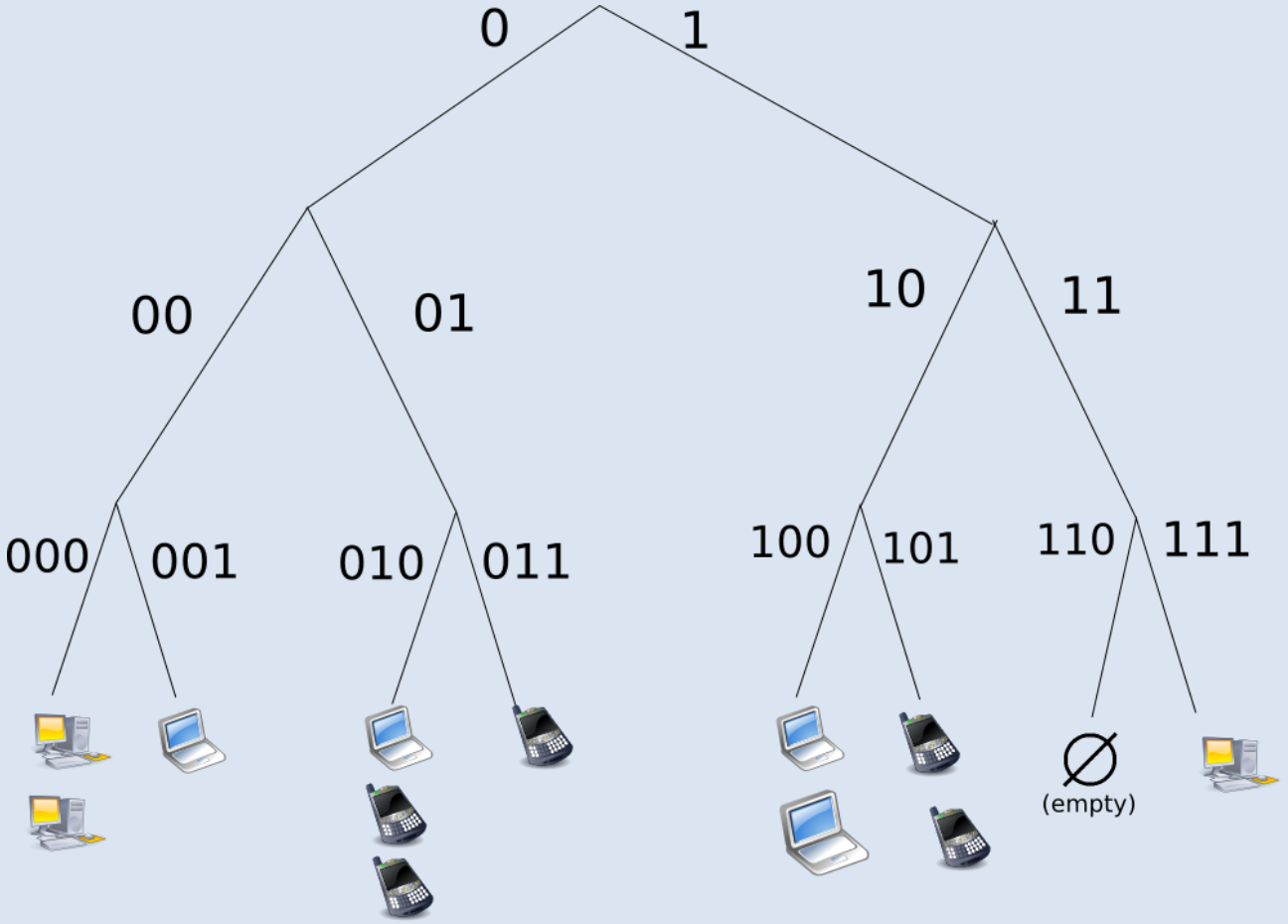
P2P Centralizzato

In questa architettura **è presente un server centrale (directory server)** che **conserva le informazioni sui peer** e risponde alle richieste su quelle informazioni effettuando la ricerca in modalità centralizzata. **I peer sono responsabili di conservare i dati e le informazioni**, in quanto il server non memorizza file, e di informare il server dei file che intendono condividere e di permettere ai peer che lo richiedono di scaricare le risorse condivise. L'implementazione più famosa è Napster, dove gli utenti si connettono ad un server centrale nel quale pubblicano i nomi delle risorse che condividono.

P2P Ibrido

Il P2P ibrido è parzialmente centralizzato. Sono presenti alcuni peer chiamati **ultra-peer** determinati dinamicamente che hanno anche la funzione di indicizzazione, gli altri nodi sono chiama **leaf peer**.

Diagramma di Rete Computer P2P - Tabella Hash Distribuita



Nella Figura sopra, vediamo il **Sistema Ottale = {000, 001, 010, 011, 100, 101, 110, 111}** equivalente a **{0, 1, 2, 3, 4, 5, 6, 7}** e con lo stesso principio possiamo costruire il **Sistema Esadecimale Hex = {0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111}** equivalente a **{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}**

Ampiezza di banda

Alcune applicazioni per funzionare hanno bisogno di avere una **garanzia sulla larghezza di banda minima disponibile**, cioè possono chiedere un **throughput garantito**, come per esempio le applicazioni multimediali. **Throughput sta per Portata o Produttività**

I Numeri delle Porte TCP e UDP | TCP Wrapper

TCP/UDP Port Numbers

7	Echo	**554**	RTSP	**2745**	Bagle.H	**6891-6901**	Windows Live
19	Chargen	**546-547**	DHCPv6	**2967**	Symantec AV	**6970**	Quicktime
20-21	FTP	**560**	rmonitor	**3050**	Interbase DB	**7212**	GhostSurf
22	SSH/SCP	**563**	NNTP over SSL	**3074**	XBOX Live	**7648-7649**	CU-SeeMe
23	Telnet	**587**	SMTP	**3124**	HTTP Proxy	**8000**	Internet Radio
25	SMTP	**591**	FileMaker	**3127**	MyDoom	**8080**	HTTP Proxy
42	WINS Replication	**593**	Microsoft DCOM	**3128**	HTTP Proxy	**8086-8087**	Kaspersky AV
43	WHOIS	**631**	Internet Printing	**3222**	GLBP	**8118**	Privoxy
49	TACACS	**636**	LDAP over SSL	**3260**	iSCSI Target	**8200**	VMware Server
53	DNS	**639**	MSDP (PIM)	**3306**	MySQL	**8500**	Adobe ColdFusion
67-68	DHCP/BOOTP	**646**	LDP (MPLS)	**3389**	Terminal Server	**8767**	TeamSpeak
69	TFTP	**691**	MS Exchange	**3689**	iTunes	**8866**	Bagle.B
70	Gopher	**860**	iSCSI	**3690**	Subversion	**9100**	HP JetDirect
79	Finger	**873**	rsync	**3724**	World of Warcraft	**9101-9103**	Bacula
80	HTTP	**902**	VMware Server	**3784-3785**	Ventrilo	**9119**	MXit
88	Kerberos	**989-990**	FTP over SSL	**4333**	mSQL	**9800**	WebDAV
102	MS Exchange	**993**	IMAP4 over SSL	**4444**	Blaster	**9898**	Dabber
110	POP3	**995**	POP3 over SSL	**4664**	Google Desktop	**9988**	Rbot/Spybot
113	Ident	**1025**	Microsoft RPC	**4672**	eMule	**9999**	Urchin
119	NNTP (Usenet)	**1026-1029**	Windows Messenger	**4899**	Radmin	**10000**	Webmin
123	NTP	**1080**	SOCKS Proxy	**5000**	UPnP	**10000**	BackupExec
135	Microsoft RPC	**1080**	MyDoom	**5001**	Slingbox	**10113-10116**	NetIQ
137-139	NetBIOS	**1194**	OpenVPN	**5001**	iperf	**11371**	OpenPGP
143	IMAP4	**1214**	Kazaa	**5004-5005**	RTP	**12035-12036**	Second Life
161-162	SNMP	**1241**	Nessus	**5050**	Yahoo! Messenger	**12345**	NetBus
177	XDMCP	**1311**	Dell OpenManage	**5060**	SIP	**13720-13721**	NetBackup
179	BGP	**1337**	WASTE	**5190**	AIM/ICQ	**14567**	Battlefield
201	AppleTalk	**1433-1434**	Microsoft SQL	**5222-5223**	XMPP/Jabber	**15118**	Dipnet/Oddbob
264	BGMP	**1512**	WINS	**5432**	PostgreSQL	**19226**	AdminSecure
318	TSP	**1589**	Cisco VQP	**5500**	VNC Server	**19638**	Ensim
381-383	HP Openview	**1701**	L2TP	**5554**	Sasser	**20000**	Usermin
389	LDAP	**1723**	MS PPTP	**5631-5632**	pcAnywhere	**24800**	Synergy
411-412	Direct Connect	**1725**	Steam	**5800**	VNC over HTTP	**25999**	Xfire
443	HTTP over SSL	**1741**	CiscoWorks 2000	**5900+**	VNC Server	**27015**	Half-Life
445	Microsoft DS	**1755**	MS Media Server	**6000-6001**	X11	**27374**	Sub7
464	Kerberos	**1812-1813**	RADIUS	**6112**	Battle.net	**28960**	Call of Duty
465	SMTP over SSL	**1863**	MSN	**6129**	DameWare	**31337**	Back Orifice
497	Retrospect	**1985**	Cisco HSRP	**6257**	WinMX	**33434+**	traceroute
500	ISAKMP	**2000**	Cisco SCCP	**6346-6347**	Gnutella		
512	rexec	**2002**	Cisco ACS	**6500**	GameSpy Arcade		
513	rlogin	**2049**	NFS	**6566**	SANE		
514	syslog	**2082-2083**	cPanel	**6588**	AnalogX		
515	LPD/LPR	**2100**	Oracle XDB	**6665-6669**	IRC		
520	RIP	**2222**	DirectAdmin	**6679/6697**	IRC over SSL		
521	RIPng (IPv6)	**2302**	Halo	**6699**	Napster		
540	UUCP	**2483-2484**	Oracle DB	**6881-6999**	BitTorrent		

Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

Servizi offerti dallo strato di Trasporto alle Applicazioni di Rete

Tutti i protocolli, sia standard che specifici, hanno in comune una particolarità: trasferire dei messaggi da un parte all'altra della rete. Ogni applicazione deve scegliere tra i protocolli di trasporto quale deve adottare in base ai servizi che sono necessari alle **specifiche esigenze dell'applicazione**, che possono essere riassunte in :
:

- **Trasferimento dati affidabile**
- **Ampiezza di banda**
- **Temporizzazione e Sicurezza**

Trasferimento Dati Affidabile

Si intende un servizio che garantisca la consegna corretta dei dati. Alcune applicazioni come quelle di riproduzione audio/video possono tollerare qualche perdita senza compromettere lo scopo dell'applicazione, altre invece come i trasferimenti di file richiedono che la consegna del file sia garantita al 100%. A tale scopo il livello di trasporto mette a disposizione due principali protocolli:

- **UDP (User Datagram Protocol):** protocollo non orientato alla connessione, da utilizzare quando la perdita di dati è un fatto accettabile, **in quanto non affidabile non offre il controllo del flusso, della congestione, del ritardo e una banda minima.**
- **TCP (Transmission Control Protocol):** protocollo orientato alla connessione **da utilizzare quando la perdita dei dati non è tollerabile**, ovvero quando il trasferimento deve essere affidabile. Dà la garanzia di un trasporto senza errori o perdita di informazioni, effettua il controllo del flusso, in quanto si adatta alle velocità di server e client, esegue anche il controllo della congestione ma non dà garanzie di banda minima.

Ampiezza di Banda

Alcune applicazioni per funzionare hanno bisogno di avere una **garanzia sulla larghezza di banda minima disponibile**, cioè possono chiedere un **throughput garantito**, come per esempio le applicazioni multimediali. **Throughput sta per Portata o Produttività**

Temporizzazione

Alcune applicazioni, come la telefonia VoIP, i videogiochi e gli ambienti virtuali per funzionare correttamente **ammettono solo piccoli ritardi**. Essendo i protocolli di trasporto sia TCP che UDP temporalmente inaffidabili è stato sviluppato un protocollo in tempo reale ad hoc chiamato **RTP (Real Time Transport Protocol)**. Questo è in grado di studiare i ritardi di rete e calibrare i collegamenti per garantire di restare in certi limiti di tempo, scegliendo alternativamente quando usare UDP e quando TCP.

Sicurezza

Un'applicazione può richiedere allo strato di trasporto la **cifratura di tutti i dati trasmessi** in maniera da garantire la riservatezza e ridurre l'efficacia delle attività di sniffing. Quindi è possibile che possano essere richiesti dei servizi di sicurezza da applicare per garantire l'integrità dei dati e l'autenticazione end-to-end.

Classificazione

Un **host di** rete è un qualsiasi dispositivo o hardware del computer connesso a una rete tramite Internet. Un **server**, d'altra parte, può essere un programma per computer o un hardware che "serve" funzionalità a cui altri dispositivi ad esso collegati possono accedere attraverso il modello e l'architettura **client-server**.

Definizione di LAN

Local Area Network (**LAN**) è una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti

Processo di Rete Comunicante

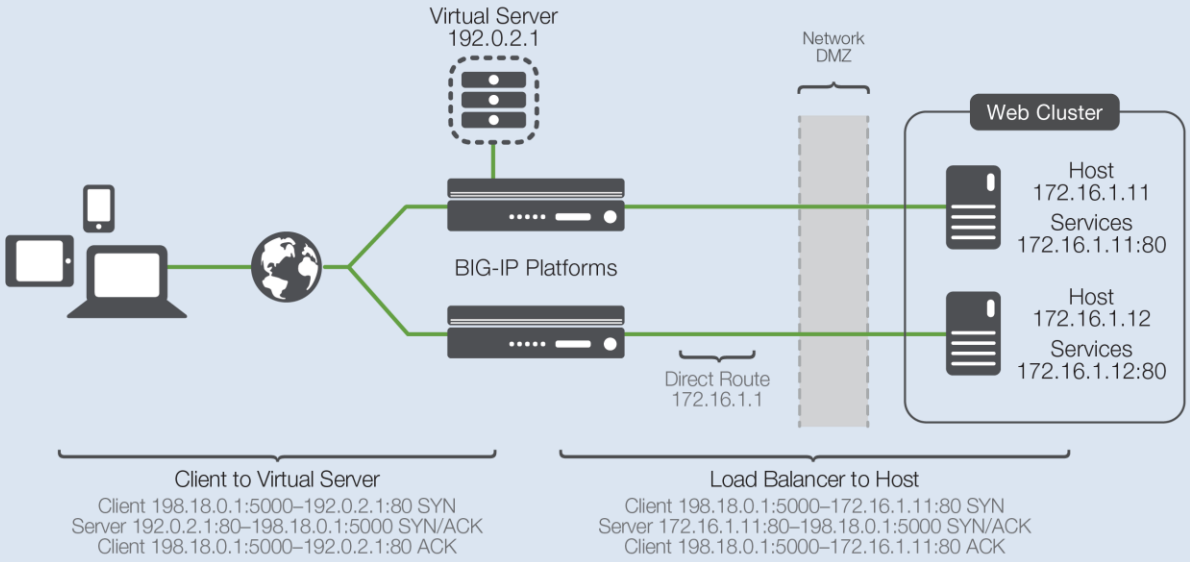
Le applicazioni nello stesso host o su host diversi comunicano tra di loro mediante processi (che sono piccoli programmi). I processi su host differenti comunicano attraverso lo scambio di messaggi invece nello stesso host, due processi comunicano utilizzando schemi interprocesso (definiti dal SO).

Lezione 2

Differenza tra Client e Server

Il client è la parte dell'applicazione distribuita, tipicamente i browser, ma anche client di posta, file transfer ecc., che effettua la richiesta di un servizio. Il server è la parte che fornisce il servizio. Il Client entità che richiede un servizio nel paradigma client/server. Il **Server è l'entità** che risponde alla richiesta di un servizio nel paradigma client/server.

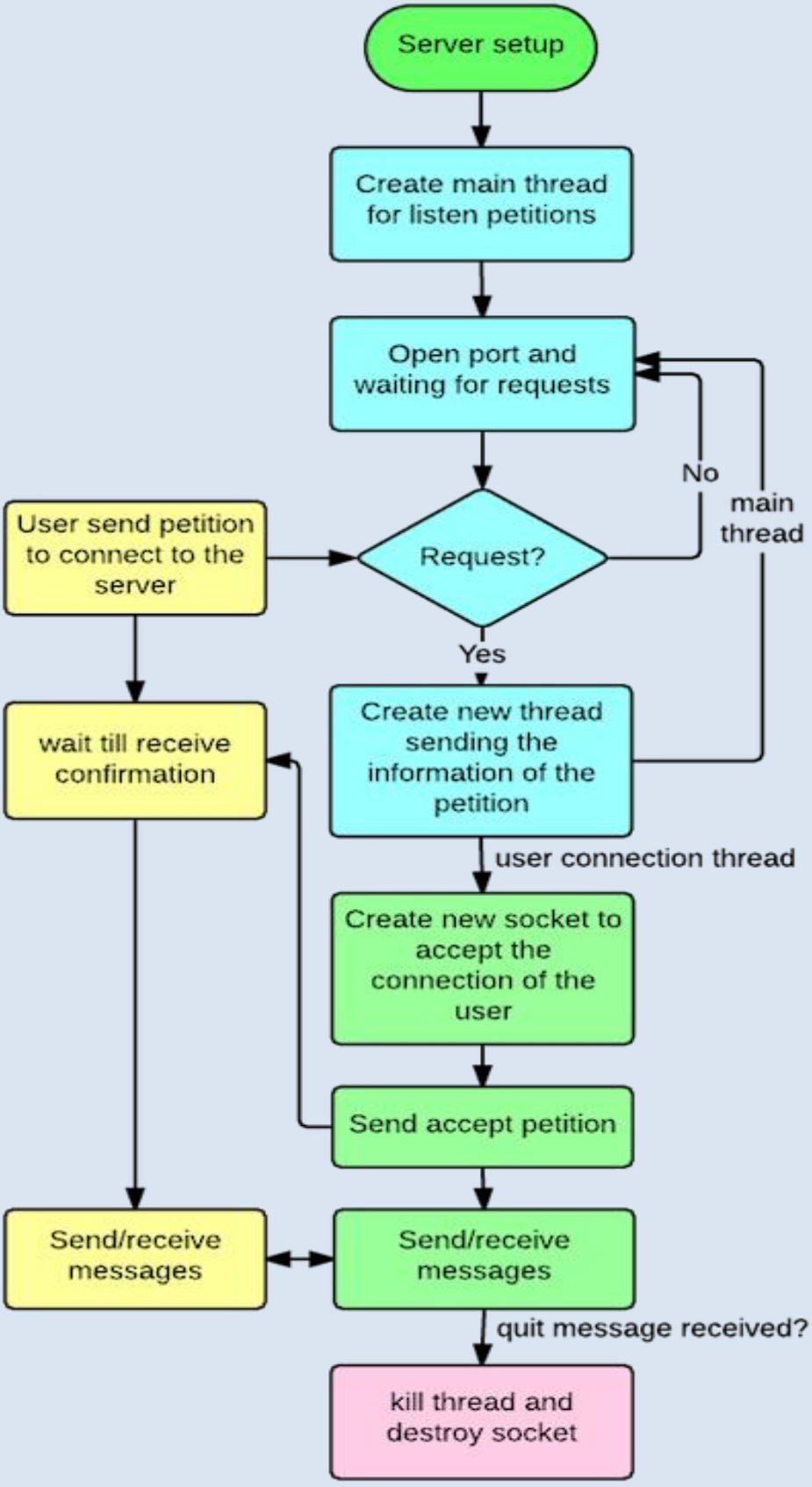
Schema di Comunicazione Client/Virtual Server



Cosa è il Protocollo

Si tratta di un insieme di **regole procedurali** su come instaurare una comunicazione tra due o più interlocutori per cui tutti devono attenersi pena errori di **comunicazione.** Un insieme di regole formalmente descritte che definiscono le modalità di comunicazione tra una o più **entità**; le regole sono definite mediante specifici protocolli, dalle tipologie più varie e ciascuno con precisi **compiti/finalità**, a seconda delle entità interessate e del mezzo di comunicazione. Se le due entità sono remote, si parla di protocollo di rete.

Diagramma di flusso del Modello Client Server



Lezione 3

Principio di base di una Rete a Commutazione di Circuito

In una rete a commutazione di circuito la capacità del canale trasmissivo è **interamente dedicata ad una specifica comunicazione**. Ciascun utilizzatore ha a disposizione **un canale trasmissivo dedicato**, con la garanzia di avere sempre disponibile tutta la capacità allocata ad ogni richiesta di servizio. La commutazione di circuito riserva un circuito dedicato tra i due host passando da diversi commutatori per l'intera durata della sessione, il tempo di trasferimento delle informazioni è costante e dipende solamente dalla distanza fra i terminali e dal numero di nodi da attraversare, in quanto la rete è trasparente al dialogo; le procedure di controllo sono limitate ad inizio e fine chiamata. **Svantaggi :** offre **minore flessibilità** come velocità di trasferimento e minore efficienza (circuito sottoutilizzato). Essa si ha quando una parte della capacità trasmissiva totale in uscita al multiplatore è stabilmente assegnata a ciascun canale tributario in ingresso. Gli elementi intermedi, o centraline di comunicazione, creano circuiti fisici Point-to-Point. Le tariffazioni applicate alla **commutazione di circuito sono tendenzialmente a tempo**.

Differenze tra Commutazione di Circuito e di Pacchetto

Nella commutazione di circuito il circuito viene dedicato ad una trasmissione e rilasciato alla fine mentre nel secondo viene utilizzato da più trasmissioni simultaneamente.

Le tecniche che si utilizzano per trasmettere più Flussi in una Rete a Commutazione di Circuito

FDM e TDM. Ci sono due tecniche : a divisione di tempo (TDM) in cui il circuito è dedicato ai diversi utenti in tempi diversi a divisione di frequenza (FDM) gli utenti utilizzano contemporaneamente il circuito ma su frequenze diverse.

FDM := Frequency Division Multiplexing — **Multiplazione a divisione di frequenza**

TDM := Time Division Multiplexing — **Multiplazione a divisione di Tempo**

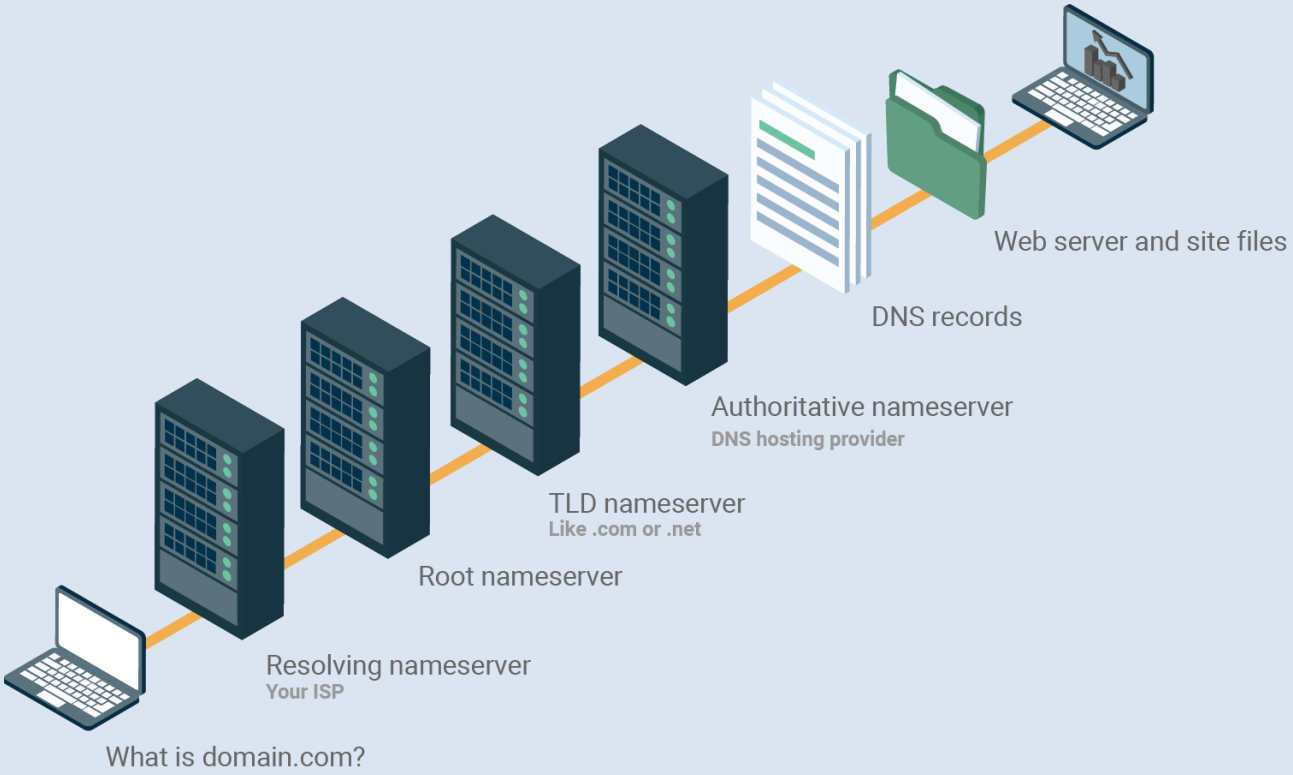
Trovare quale tipologia di traffico una Rete a Commutazione di Pacchetto risulta più efficiente di una a Commutazione di Circuito

Per le reti con **dati "a raffica"**, in cui ci sono molti utenti che condividono le risorse nello stesso momento. La commutazione di pacchetto si rivela molto più efficiente nonostante la maggior quantità di dati inviata, in quanto i canali fisici sono utilizzati solo per il tempo strettamente necessario. Inoltre, poiché ogni pacchetto porta con sé la sua identificazione, una rete può trasportare nello stesso tempo pacchetti provenienti da sorgenti differenti.

Essa permette quindi a più utenti di inviare informazioni attraverso la rete in modo efficiente e simultaneo, risparmiando tempo e costi mediante la condivisione di uno stesso canale trasmissivo (cavo elettrico, ethernet, fibra ottica ecc.). La commutazione di pacchetto (**packet switching**) è una tecnica che si basa sulla suddivisione del messaggio da trasmettere in più unità autonome, i pacchetti, ciascuna corredata delle opportune informazioni di controllo, ad esempio gli identificativi del mittente e del destinatario e del numero d'ordine del pacchetto all'interno dell'intero messaggio.

Ogni pacchetto inviato da una stazione segue un proprio percorso di rete per raggiungere la stazione finale, la quale provvederà, a riordinare i pacchetti e assemblare di nuovo il messaggio di partenza. Questo risulta essere più efficiente per le reti con dati "a raffica", in cui ci sono molti utenti che condividono le risorse nello stesso momento.

Name Server Record | CNAME Record risorse NS



Principali Differenze tra Commutazione di Circuito e Pacchetto

La commutazione di pacchetto ottimizza l'impiego della rete, perché permette a più stazioni la trasmissione di diversi messaggi sullo stesso canale è meno adatta per tutti quei servizi che richiedono la consegna dei dati nel rispetto di precisi vincoli temporali, quali la comunicazione voce e video. - Diversamente, con la tecnica a commutazione di circuito, il canale viene assegnato esclusivamente alle sole due stazioni, fino al termine della comunicazione quindi in sostanza la commutazione di circuito occupa la banda per tutta la durata della comunicazione invece quella di pacchetto solo quando serve. In una rete a commutazione di circuito la capacità del canale trasmissivo è interamente dedicata ad una specifica comunicazione. Ciascun utilizzatore ha a disposizione un canale trasmissivo dedicato, con la garanzia di avere sempre disponibile tutta la capacità allocata ad ogni richiesta di servizio. La commutazione di pacchetto si rivela molto più efficiente nonostante la maggiore quantità di dati inviata perché i canali fisici sono utilizzati solo per il tempo strettamente necessario. Inoltre, poiché ogni pacchetto porta con sé la sua identificazione, una rete può trasportare nello stesso tempo pacchetti provenienti da sorgenti differenti. Essa permette quindi a più utenti di inviare informazioni attraverso la rete in modo efficiente e simultaneo, risparmiando tempo e costi mediante la condivisione di uno stesso canale trasmissivo (cavo elettrico, ethernet, fibra ottica ecc.). Nella commutazione di pacchetto gli utenti accedono alle risorse su richiesta con la possibilità di congestione invece su quelle a circuito sono risorse dedicate.

Lezione 4

Perché si possono verificare perdite in una Rete

Perché il **buffer interno al router** (**nodo**) è una memoria finita e quindi non è illimitata. Le perdite in un nodo avvengono quando questo non è dimensionato per il lavoro che deve svolgere cioè quando il tasso di arrivo dei pacchetti sul collegamento eccede la capacità del collegamento di evaderli e il buffer in uscita è pieno ed è per questo che il pacchetto va eliminato o scartato.

Perché si possono verificare ritardi in una Rete

Perché vi è un traffico superiore, rispetto a quanto la rete stessa è dimensionata. I ritardi nella rete avvengono quando il tasso di arrivo dei pacchetti sul collegamento eccede la capacità del collegamento di evaderli. Il pacchetto è inserito nel buffer e rimarrà in coda finché non saranno processati i pacchetti già in coda.

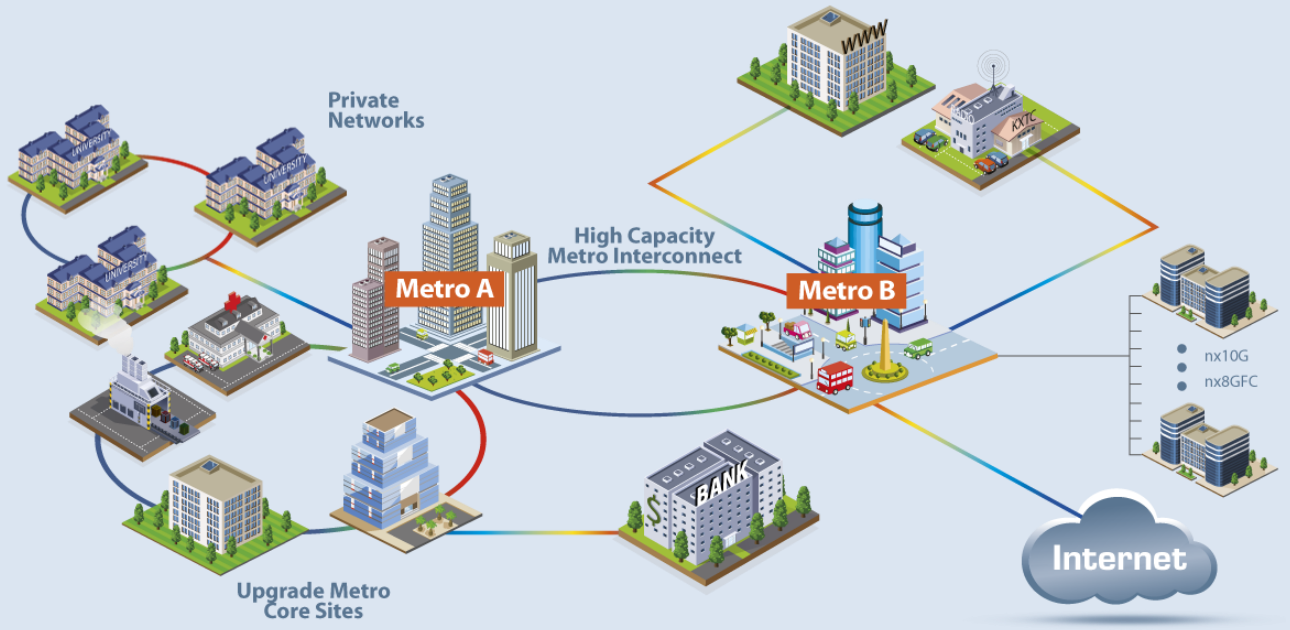
Cosa si intende per Ritardo di Elaborazione

Il ritardo di elaborazione è il tempo necessario al nodo di elaborare e smistare il pacchetto cioè di esaminare il pacchetto e a determinarne l'instradamento In questo tempo è compreso anche il controllo degli errori e il successivo invio alla corretta coda di trasmissione. Il suo ordine di grandezza è qualche microsecondi (o inferiore).

Quali sono le Componenti del Ritardo di un Nodo

Elaborazione, Trasmissione e Accodamento sono le componenti di ritardo del nodo. Invece la propagazione riguarda il mezzo trasmissivo di cui è fatto il link (livello 2 della pila protocollare).

Rete di Computer | Rete di Telecomunicazione | Rete di Trasporto



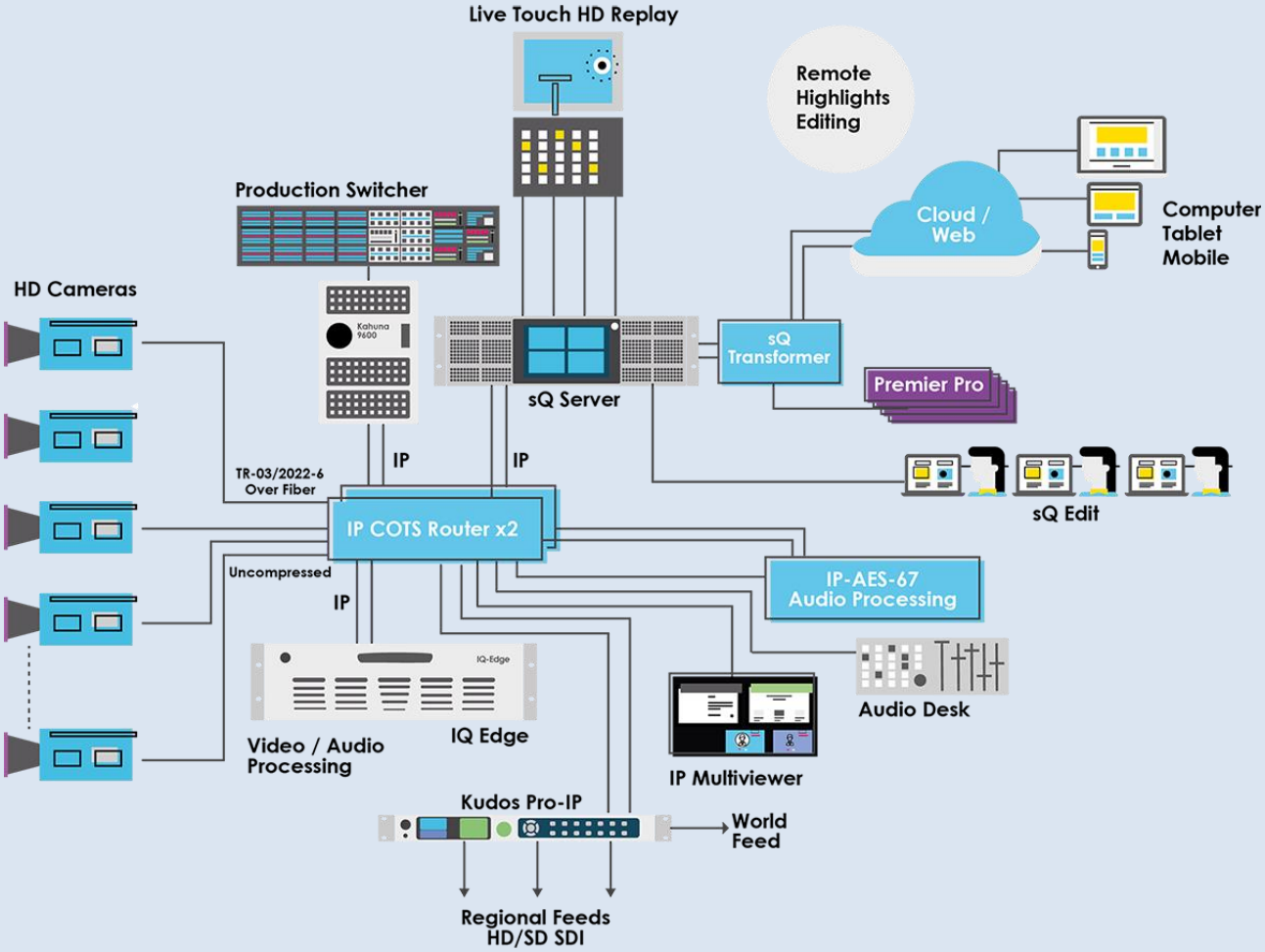
Cosa si Intende per Ritardo di Propagazione

Il ritardo di propagazione è il tempo necessario al pacchetto per transitare lungo l'intera lunghezza del link fisico Questo ritardo dipende dalla lunghezza (d) del link e dalla velocità di propagazione (s) sul mezzo (circa 2×10^8 m/s) e si calcola come **d/s**. È una componete che determina il ritardo totale del nodo.

Quali sono le Funzionalità del Livello di Trasporto

Il livello di trasporto fornisce la comunicazione tra i processi applicativi di host differenti. I protocolli di trasporto, vengono eseguiti nei sistemi terminali: lato invio il protocollo scinde i messaggi in segmenti e li passa al livello di rete invece lato ricezione i segmenti vengono riassemblati in messaggi e li passa al livello di applicazione

Indirizzo IP di Routing Broadcasting | System Internet Protocol



Lezione 5

Architetture del Livello Applicazione

Le architetture del livello applicazione sono

- **Peer to Peer (P2P) :** In questa architettura non c'è un server sempre attivo e coppie arbitrarie di host (peer) comunicano direttamente tra loro. Inoltre è un'architettura facilmente scalabile ma non facile da gestire.
- **Client/Server :** In questa architettura c'è un server che è host sempre attivo con IP fisso in attesa di essere contattato e che fornisce un servizio e un client che richiede un servizio al server, esso ha un IP dinamico e non può comunicare direttamente con altri client
- **Architetture Ibride :** (client - server e P2P)

Livelli della pila protocollare e le loro Funzionalità

I livelli protocollari sono **5 :**

- **Applicazione :** E' di supporto alle applicazioni di rete. Applicazioni Utente, Http, Mail, DNS, FTP
- **Trasporto :** Trasferimento dei messaggi a livello di applicazione tra il modulo client e server di un'applicazione. Controllo di flusso Errore TCP UDP
- **Rete :** Instradamento dei datagrammi dall'origine al destinatario. Instradamento IP
- **Link (Collegamento) :** Instradamento dei datagrammi attraverso una serie di commutatori di pacchetto. Accesso Ethernet CSMA-CD
- **Fisico :** Trasferimento dei singoli bit a mezzo rame, fibra, wireless.

Lezione 6

Differenze tra indirizzo IP e numero di Porta

Un indirizzo IP è un'etichetta numerica che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete. Le porte, sono lo strumento utilizzato per realizzare la **multiplazione** delle connessioni a livello di trasporto, ovvero per permettere ad un calcolatore di effettuare più connessioni contemporanee verso altri calcolatori, facendo in modo che i dati contenuti nei pacchetti in arrivo vengano indirizzati al processo che li sta aspettando. L'indirizzo IPv4 è un indirizzo di 32 bit univoco all'interno della rete che identifica l'host, il numero di porta è un numero che è associato ad un determinato **socket** in esecuzione in quel momento sull'host con quell'indirizzo IP.

Cosa è il Socket

Un socket è l'interfaccia standard tra i programmi applicativi e i protocolli TCP. Il socket è come una porta di comunicazione che permette di utilizzare il protocollo TCP/IP. È un metodo per la comunicazione tra un programma client e un programma server su una rete, può essere definito come un punto terminale di una connessione a doppio senso tra due programmi che comunicano e scambiano dati sulla rete. I protocolli coinvolti nell'implementazione dei Socket sono : TCP (Transfer Control Protocol) e UDP (User Datagram Protocol)

Cosa definisce un Protocollo a livello di Applicazione

Un protocollo a livello applicazione definisce **:**

Regole : necessarie per determinare quando e come un processo invia e risponde ai messaggi
Semantica dei Campi : Ovvero significato delle informazioni nei campi
Sintassi dei tipi di messaggio : quali sono i campi nel messaggio e come sono descritti
Tipi di messaggi scambiati : ad esempio messaggi di richiesta e di risposta

Errore HTTP 403 Cookie | Accesso Negato

Lezione 7

Come funziona una Connessione Persistente

Il Server invia più oggetti possono su una singola connessione TCP tra Client e Server. In questo modo non occorre instaurare diverse connessioni per diversi oggetti risparmiando il tempo di invio di pacchetti.

Come funziona una Connessione non Persistente

Un **Server** deve inviare **10 oggetti** al **Client** questo vuol dire che il server-client devono instaurare **10 diverse connessioni** perdendo tempo per lo scambio di messaggi per instaurare la connessione. Ogni oggetto viene trasmesso su una connessione **TCP** distinta.

Cosa è HTTP

Http è l'acronimo per **Hypertext Transfer Protocol** ovvero protocollo di trasferimento di un ipertesto. L'HTTP è usato come principale sistema per la trasmissione d'informazioni sul web. Http è un protocollo di livello applicazione del Web identificato con la porta 80 e che utilizza il protocollo TCP, utilizza un Modello Client/Server in cui **-server :** il server web invia oggetti in risposta a una richiesta **-client :** il browser che richiede, riceve, "visualizza" gli oggetti del Web

Lezione 8

Le differenze tra HTTP/1.0 e HTTP/1.1

La differenza sostanziale che http/1.0 non ha la comunicazione persistente ed ha solo tre metodi (GET richiede un oggetto, POST invia un oggetto e HEAD chiede al server di escludere l'oggetto richiesto dalla risposta) invece **http/1.1** ne ha 2 in più (PUT include il file nel corpo dell'entità e lo invia al percorso specificato nel campo URL e DELETE cancella il file specificato nel campo URL)

Illustrare il formato generale di un messaggio di risposta HTTP

Una risposta HTTP comprende **:**

- l'identificativo della versione del protocollo HTTP
- il codice di stato e l'informazione di stato in forma testuale
- un insieme di possibili altre informazioni riguardanti la risposta
- l'eventuale contenuto della risorsa richiesta

Riga di stato (protocollo codice di stato espressione di stato)
http/1.1 200 OK
Righe di intestazione-Connection close

- **Date** : Thu, 06 Aug 1998 12:00:15 GMT
- **Server** : Apache/1.3.0 (Unix)
- **Last-modified** : Mon, 22 Jun 1998
- **Content-Type** : text/html
- **Dati :** ad esempio il file HTML richiesto

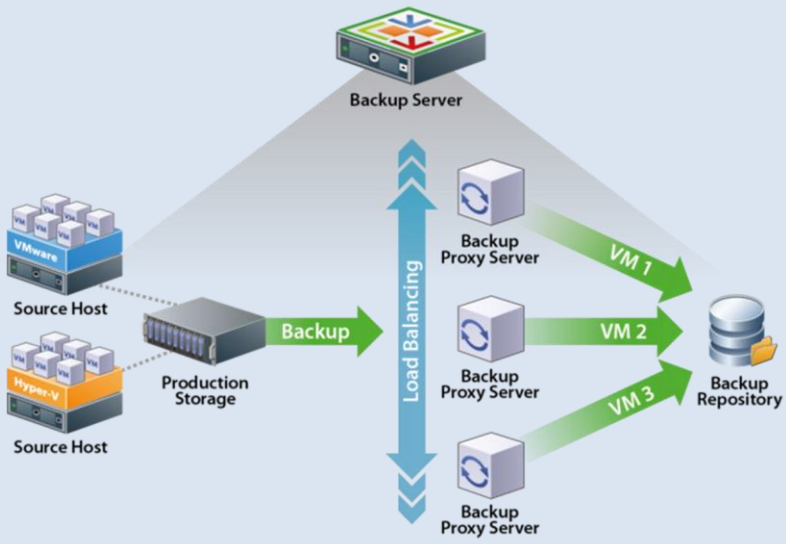
Cosa servono i Codici di stato di una Risposta HTTP

Sono codici di risposta inviati dal server al client e servono per identificare lo stato della richiesta e comunicarla all'utente. La comunicazione tra client e server deve però seguire un protocollo che nella maggior parte dei casi è il protocollo HTTP(HyperText Transfer Protocol) che è quindi il principale sistema usato per la trasmissione di dati sul web. Quando noi richiediamo una pagina web il browser fa delle richieste al server il quale le decodifica e manda al client delle risposte che lo informano circa lo stato della richiesta. Queste risposte sono chiamate codici di stato http e sono rappresentate con tre cifre a loro volta raggruppate in classi le quali sono rappresentate dalla prima cifra del codice.

Cosa si intende per pipelining in una Connessione HTTP

Quando è attivo il pipeling in una connessione HHTP si hanno diverse trasmissioni di più richieste senza attendere l'arrivo della risposta alle richieste precedenti. L'HTTP pipelining è una tecnica in cui vengono inviate più richieste HTTP su una singola connessione TCP senza aspettare le risposte corrispondenti. L'adozione del pipelining delle richieste HTTP comporta un significativo miglioramento nella velocità di caricamento delle pagine HTML, in particolare nel caso di connessioni ad alta latenza come nel caso delle connessioni satellitari. Poiché è generalmente possibile inserire più richieste HTTP nello stesso segmento TCP, il pipelining HTTP consente di inviare e ricevere sulla rete meno pacchetti, riducendone quindi il carico.

Server ProXY Veeam Backup & Replication Server Server



Lezione 9

Per quali motivi si utilizza un ProXY Web

Il Pro**XY** web è il **Server/Host** che implementa il caching in questo modo si riducono i tempi di risposta alle richieste dei client e il traffico sul collegamento di accesso a Internet. un server proxy è un server che funge da intermediario per le richieste da parte dei client alla ricerca di risorse su altri server, disaccoppiando l'accesso al web dal browser. Un client si connette al server proxy, richiedendo qualche servizio (ad esempio un file, una pagina web o qualsiasi altra risorsa disponibile su un altro server), quest'ultimo valuta ed esegue la richiesta in modo da semplificare e gestire la sua complessità.

Cosa servono i Cookie Web
Vengono memorizzati sulla macchina Client e facendo parte dello Stato della sessione di utente permette di ottenere più velocemente la richiesta già fatta dal Client.

Cosa è il metodo HTTP GET condizionale e per cosa viene utilizzato?
È un metodo introdotto per il protocollo http per diminuire il traffico nella rete e di utilizzare le cache, il get condizionale richiede al server se l'oggetto richiesto è stato modificato, se è stato modificato invia il nuovo oggetto altrimenti risponde che non è stato modificato e utilizza la copia nella cache.

A cosa serve una cache Web?
Serve per diminuire il traffico in rete e la latenza de pacchetti infatti in essa è conservata una copia di tutti gli oggetti per le future richieste. Il client ottiene l'oggetto senza utilizzare il server d'origine. La web cache è una parte di memoria (parte di hard-disk o magari interna al browser di internet) che si occupa di memorizzare le pagine dei siti web che visitiamo. In questa maniera per noi sarà più veloce caricare la pagina web dei siti che visitiamo maggiormente, e per i server ci sarà meno lavoro visto che in genere le pagine web pesano molto.

Lezione 10

Come funziona e a cosa serve la Cache DNS
La **cache DNS è un piccolo database locale** sul server in cui c'è la corrispondenza tra gli indirizzi IP e nomi memonici dei siti in precedenza visitati, questa è interrogata ogni qual volta si richiede l'indirizzo IP di un sito web, se l'indirizzo IP di questo sito è presente nella cache viene comunicato all'utente per poter caricare il sito web, altrimenti invia una richiesta al server DNS principale per ottenere l'IP.

Cosa si intende per query DNS ricorsiva
La query ricorsiva richiede che al cliente venga fornita la risposta esatta chiedendo anche ad altri utenti senza passare dall'utente o si segnali errore. In questo caso si prevede una catena di server **request/reply**. In questo caso il server rimane impegnato finche non risolve la query che sta processando.

Illustrare le principali funzionalità e caratteristiche del DNS
Il server DNS occorre per effettuare la traduzione degli host name in indirizzi IP, in questo modo l'URL del sito web ricercato è tradotto nel indirizzo IP del server web a cui si può fare la richiesta, inoltre effettua la funzione di host aliasing, in quanto un host può avere diversi nomi. Il DNS è un DB distribuito implementato in una gerarchia di server DNS (server TLD, authoritative server e local server) ed è un Protocollo a livello di applicazione che consente agli host, ai router e ai server DNS di comunicare per risolvere i nomi .

Perché l'ARP deve precedere la richiesta DNS
Per spedire un frame al gateway il DNS ha bisogno dell'indirizzo MAC che viene fornito da ARP. ARP è un protocollo ausiliario di livello rete il cui scopo è ottenere l'indirizzo MAC di una stazione di cui è noto l'indirizzo IP

Quali del Servizio DNS sono i vantaggi per avere e poter disporre di una struttura distribuita

Avere una struttura distribuita permette di avere diversi punti di accesso dagli utenti nel mondo quindi più velocemente raggiungibile un traffico più distribuito, una manutenzione del server semplificata senza avere problemi di ridondanza, scalabilità o un unico punto di guasto.

Lezione 11

Come funziona il file sharing in una rete P2P

In una rete P2P degli host "arbitrari" (peer) comunicano direttamente tra loro e non ci devono essere server sempre attivi inoltre i peer sono connessi in maniera "intermittente" e possono avere indirizzi IP dinamici. In questo modo i peer che richiedono un determinato file non scaricano direttamente il file dal server principale ma anche dai peer che hanno già scaricato il file, in questo modo ci sono diverse sorgenti da cui poter scaricare le diverse parti. Questo permette di diminuire il tempo di scaricamento di un file.

Come funziona e a cosa serve la cache DNS

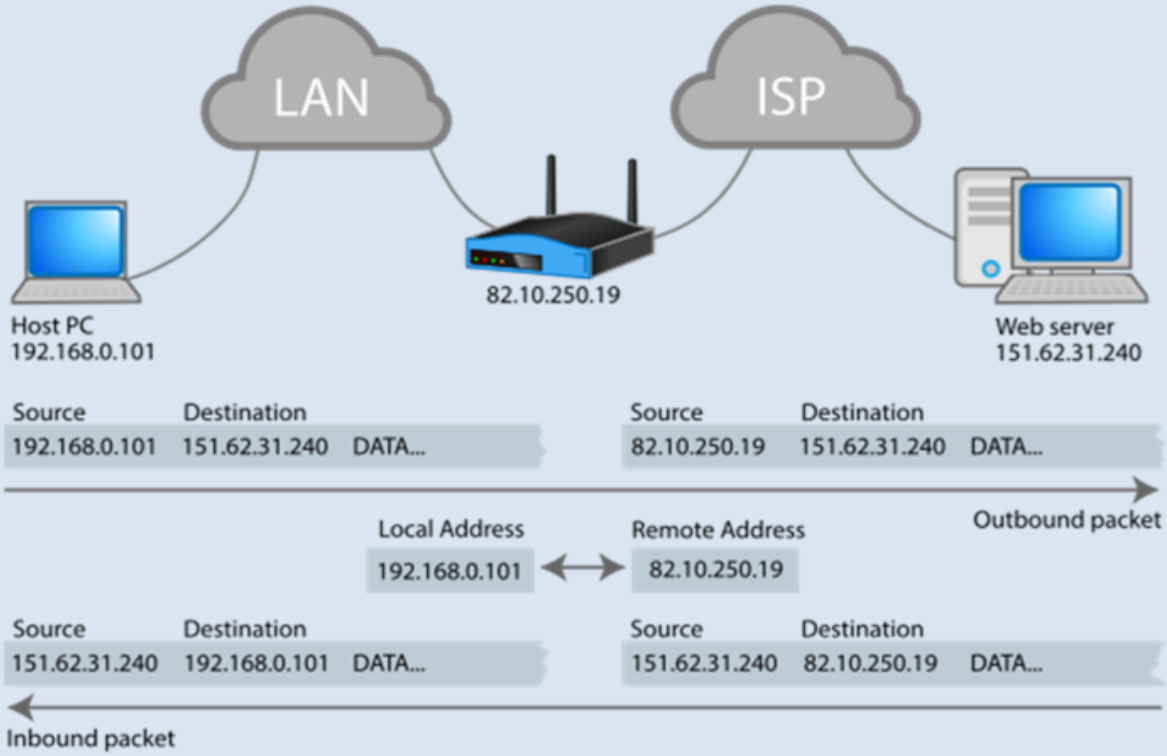
La cache DNS è un piccolo database locale sul server in cui c'è la corrispondenza tra gli indirizzi IP e nomi memonici dei siti in precedenza visitati, questa è interrogata ogni qual volta si richiede l'indirizzo IP di un sito web, se l'indirizzo IP di questo sito è presente nella cache viene comunicato all'utente per poter caricare il sito web, altrimenti invia una richiesta al server DNS principale per ottenere l'IP.

Differenza tra DNS, DHCP e WINS

La rete è composta da Computer e da Server, che hanno la necessità di comunicare tra di loro sulla rete **LAN**, per fare questo ogni dispositivo deve disporre di un'identità che può essere il nome del dispositivo logico che identifica in modo univoco il dispositivo e la sua posizione nella rete. La distribuzione dei nomi e degli indirizzi non può essere gestita manualmente, per questo la rete dispone di **DNS** (**Domain Name System**), **DHCP** (**Dynamic Host Configuration Protocol**) e **WINS** (**Windows Internet Naming**) che sono tre meccanismi essenziali per la fornitura di servizi di gestione e assegnazione di indirizzi **IP** dei **PC** dell'azienda. Lo **scopo principale di DNS, è quello di convertire nomi host facili da leggere e da ricordare in indirizzi IP numerici**. Tra le tante funzionalità, **DNS risolve anche indirizzi di posta elettronica** per individuare lo specifico server di scambio di posta elettronica del destinatario. **DHCP invece è un protocollo che consente a un computer, un router o un altro dispositivo di rete di richiedere e ottenere un indirizzo IP univoco e altri parametri come una subnet mask da un server che contiene un elenco di indirizzi IP disponibili per una rete.**

WINS è un servizio di risoluzione dei nomi **NetBIOS** che consente ai computer client di registrare i nomi NetBIOS e gli indirizzi IP in un database dinamico e distribuito e di risolvere i nomi NetBIOS delle risorse di rete nei relativi indirizzi IP. WINS e DNS sono entrambi servizi di risoluzione dei nomi per reti TCP/IP. Mentre WINS risolve i nomi nello spazio dei nomi NetBIOS, DNS risolve i nomi nello spazio dei nomi del dominio di DNS. WINS principalmente supporta i client su cui sono in esecuzione le precedenti versioni di Windows e le applicazioni che utilizzano NetBIOS. All'interno della rete i servizi e gli host di rete vengono configurati con i nomi DNS affinché possano essere individuati nella rete. Vengono anche configurati con i server DNS che risolvono i nomi dei controller di dominio di Active Directory. Stabilire i server DNS interni consente di avere massima flessibilità e controllo sulla risoluzione dei nomi dei domini interni ed esterni. Ciò riduce il traffico di rete Internet e Intranet.

Traduzione Indirizzo Rete | Indirizzo IP Pacchetto di Rete



Lezione 12

Illustrare l'interazione Client/Server dei socket con TCP

Il client contatta il server per instaurare la comunicazione, in questo caso il server deve avere il processo in esecuzione e creare il socket che deve accogliere il tentativo comunicazione. Nel frattempo il cliente crea il socket locale specificando l'indirizzo IP e il numero della porta del processo server e stabilisce la connessione con il server. Il server una volta contattato dal client il server TCP crea un nuovo socket per il processo server per comunicare con il client. In questo modo c'è una connessione uno a uno e ordinate tra le due entità

Differenza tra il tempo di distribuzione di un file in una rete Client/Server e in una rete P2P

Il tempo di distribuzione di un file in una rete client/server dipende linearmente solo dal numero di utenti che richiedono quel file in vece una rete P2P oltre a dipendere linearmente dal numero di utenti dipende anche inversamente dalla capacità di ogni peer di condividere la risorsa. Quindi al crescere del numero di utenti il tempo di distribuzione di una rete P2P è molto inferiore.

Differenze tra Socket UDP e Socket TCP

Nel socket UDP non c'è handshaking quindi non c'è un setup della connessione prima della comunicazione tra client/server, il client invia semplicemente la richiesta con indirizzo IP e il numero di porta del server. Il server una volta ricevuta la richiesta la elabora e la invia al client. In questo caso le richieste del client possono arrivare al server in maniera non ordinata o perdersi, mentre nel socket TCP c'è una fase di instaurazione della connessione e per questo motivo fornisce un trasferimento di byte affidabile e ordinato.

Lezioni 13

Come funzione il Demultiplexing orientato alla Connessione

L'host che effettua il demultiplexing orientato alla connessione, utilizzando il protocollo TCP, utilizza 4 parametri per inviare il segmento al socket appropriato. I parametri utilizzati sono: indirizzi IP e numero di porta della sorgente e l'indirizzo IP e numero di porta

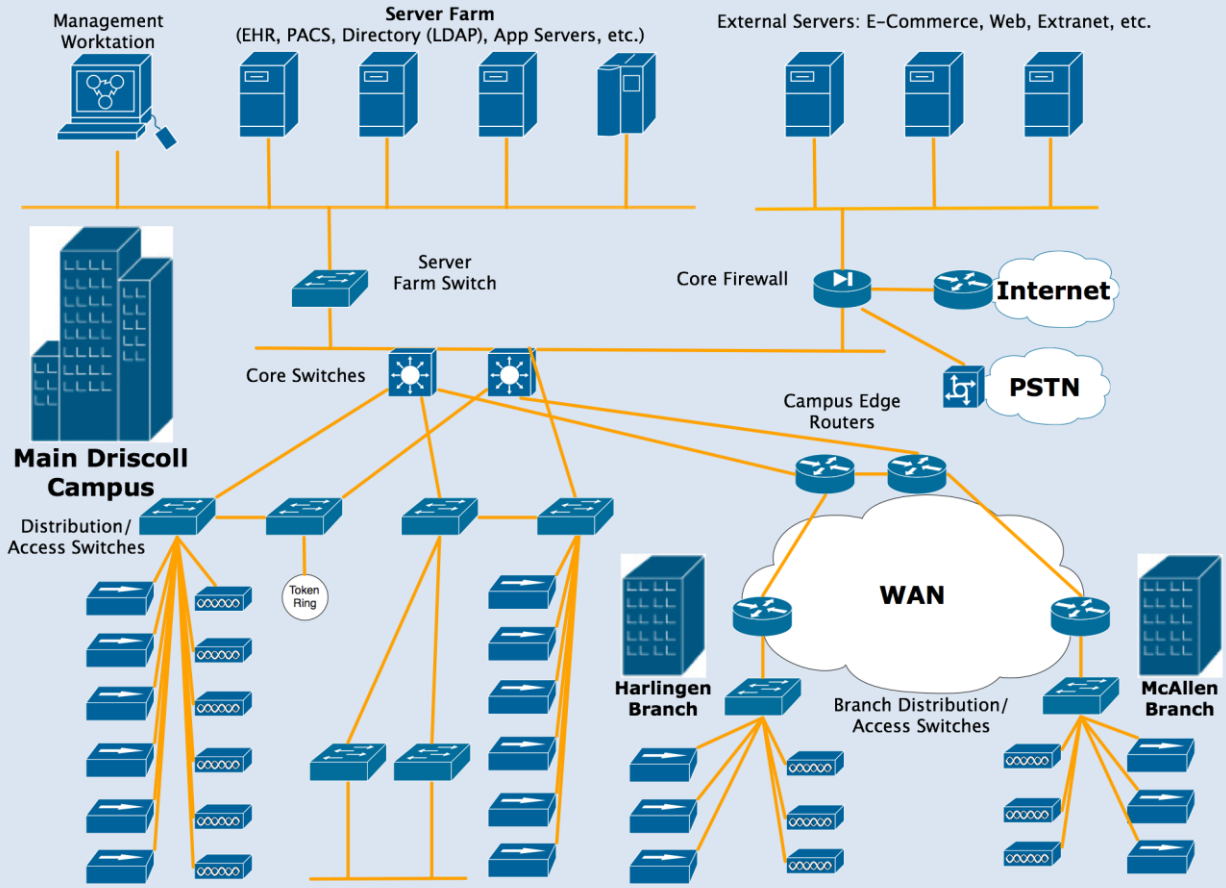
Cosa si intende per Trasporto dati Affidabile

Per trasporto di dati affidabile vuol dire trasportare i pacchetti dalla sorgente alla destinazione senza perdita di pacchetti e la consegna in ordine.

Cosa si intende per Demultiplexing a livello di Trasporto

L'host riceve i datagrammi IP contenenti indirizzo IP di origine e di destinazione, ogni datagramma ha un numero di porta di origine e un numero di porta di destinazione. L'host usa gli indirizzi IP e i numeri di porta per inviare il segmento alla socket appropriata.

Schema di Rete di Computer | Topologia di Rete | Grafico a strati



La rete PSTN (Public Switched Telephone Network), ovvero **Rete Telefonica Pubblica Commutata**, non è altro che la normale Rete Telefonica. Presenta il limite di essere alquanto lenta nella trasmissione di dati per un computer. Commutazione di Circuito.

Differenza tra reti PSDN, PSTN, ISDN

PSDN è l'acronimo di Packed Switched Data Network. Identifica un modello di trasmissione, basato sulla commutazione a pacchetto, che permette a più utenti di condividere i medesimi circuiti. I dati sono divisi in diversi pacchetti ed instradati per essere trasmessi al destinatario. Se una linea è troppo affollata i pacchetti sono indirizzati su una linea diversa. La rete è composta da più nodi di commutazione, ognuno dei quali possiede apposite tabelle per effettuare l'instradamento (routing). Giunti al nodo finale, i pacchetti sono riassemblati nell'ordine originale.

La rete PSTN (Public Switched Telephone Network), ovvero Rete telefonica pubblica commutata, non è altro che la normale rete telefonica. Presenta il limite di essere alquanto lenta nella trasmissione di dati per un computer. Ciò vuol dire che i dati sono inviati in formato analogico, cioè sotto forma di segnali elettronici di frequenza e di estensione variabile. Public Switched Telephone Network (rete telefonica pubblica commutata). La tradizionale rete telefonica commutata pubblica. Il sistema impiega linee telefoniche costituite da cavi in rame per trasmettere segnali vocali analogici o digitali impostando un percorso (un canale o circuito dedicato) che viene creato tra due punti per la durata della chiamata.

Rete ISDN (Integrated Services Digital Network | Rete Integrata di Servizi Digitali) consente la trasmissione di dati in forma digitale: il segnale non viene modulato secondo una determinata onda, ma codificato e inviato lungo la linea come una lunga sequenza di zero e uno. Questa rete è caratterizzata da una elevata velocità di trasmissione, pari a 64 Kbit al secondo per canale: una linea ISDN è due volte più veloce di una semplice linea telefonica analogica.

Lezione 14

A cosa serve la stima del RTT nel TCP

La stima del RTT serve al trasmettitore di stimare il tempo dopo il quale un pacchetto può essere considerato perso perché non ha ricevuto l'ACK. Questo tempo non può essere troppo piccolo per evitare ritrasmissioni non necessarie ma neanche troppo grande perché varia. La stima è effettuata facendo una media mobile esponenziale ponderata partendo dal tempo misurato dalla trasmissione del segmento fino alla ricezione di ACK.

Come si chiude una connessione TCP

Il client chiude la socket : clientSocket.close();
Passo 1 : il client invia un segmento di controllo FIN al server.
Passo 2 : il server riceve il segmento FIN e risponde con un ACK. Chiude la connessione e invia un FIN.
Passo 3: il client riceve FIN e risponde con un ACK. - inizia l'attesa temporizzata - risponde con un ACK ai FIN che riceve.
Passo 4 : il server riceve un ACK. La connessione viene chiusa. Con una piccola modifica può gestire segmenti FIN simultanei.

Il livello dello stack IP/TCP che prevede nuovi protocolli/tecnologie

Il livello applicazione fornisce servizi al utente. La comunicazione è fornita per mezzo di una connessione logica. Il livello applicazione è l'unico che fornisce servizi agli utenti di Internet, la sua flessibilità consente di aggiungere nuovi protocolli/tecnologie con estrema facilità.

Illustrazione del formato del Header UDP

L'header del protocollo UDP è formato da :

- **Source port [16 bit] |** Identifica il numero di porta sull'host del mittente del datagramma;
- **Destination port [16 bit] |** Identifica il numero di porta sull'host del destinatario del datagramma.
- **Length [16 bit] |** Contiene la lunghezza totale in bytes del datagramma UDP (header+dati);
- **Checksum [16 bit] |** Contiene il codice di controllo del datagramma (header+dati+pseudo-header, quest'ultimo comprendente gli indirizzi IP di sorgente e destinazione). L'algoritmo di calcolo è definito nell'RFC del protocollo.

Illustrare il formato del Header TCP

L'header del protocollo TCP è formato da **:**

- Source port [16 bit] | Identifica il numero di porta sull'host mittente associato alla connessione TCP.

- Destination port [16 bit] | Identifica il numero di porta sull'host destinatario associato alla connessione TCP

- Sequence number [32 bit] | Numero di sequenza, indica lo scostamento (espresso in byte) dell'inizio del segmento TCP all'interno del flusso completo, a partire dall'Initial Sequence Number (ISN), negoziato all'apertura della connessione.

- Acknowledgment number [32 bit] | Numero di riscontro, ha significato solo se il flag ACK è impostato a 1, e conferma la ricezione di una parte del flusso di dati nella direzione opposta, indicando il valore del prossimo Sequence number che l'host mittente del segmento TCP si aspetta di ricevere.

- Data offset [4 bit] | Indica la lunghezza (in dword da 32 bit) del header del segmento TCP; tale lunghezza può variare da 5 dword (20 byte) a 15 dword (60 byte) a seconda della presenza e della lunghezza del campo facoltativo Options.

- Reserved [4 bit] | Bit non utilizzati e predisposti per sviluppi futuri del protocollo; dovrebbero essere impostati a zero.

- Flags [8 bit] | Bit utilizzati per il controllo del protocollo (SYN,ACK, etc.)

- Window size [16 bit] | Indica la dimensione della finestra di ricezione del host mittente, cioè il numero di byte che il mittente è in grado di accettare a partire da quello specificato dal acknowledgment number.

- Checksum [16 bit] | Campo di controllo utilizzato per la verifica della validità del segmento. È ottenuto facendo il complemento a 1 della somma complemento a uno a 16 bit dell'intero header TCP (con il campo checksum messo a zero),dell'intero payload, con l'aggiunta di uno pseudo header composto da : indirizzo IP sorgente(32bit), indirizzo IP destinazione(32bit), un byte di zeri, un byte che indica il protocollo e due byte che indicano la lunghezza del pacchetto TCP (header + dati).

- Urgent pointer [16 bit] | Puntatore a dato urgente, ha significato solo se il flag URG è impostato a 1 ed indica lo scostamento in byte a partire dal Sequence number del byte di dati urgenti all'interno del flusso.

- Options | Opzioni (facoltative) per usi del protocollo avanzati.

Tutte le funzionalità del Protocollo UDP

Il protocollo UDP non affidabile perché è un protocollo senza connessione in quanto non c'è handshaking tra mittente e destinatario UDP e ogni segmento UDP è gestito indipendentemente dagli altri. Il protocollo effettua un servizio di consegna "**best effort**" e i segmenti UDP possono essere perduti o consegnati fuori sequenza. Il protocollo è utilizzato spesso nelle applicazioni multimediali perché tollera piccole perdite ed è sensibile alla frequenza. L'unico controllo che effettua il protocollo UPD è un checksum sui bit che compongono l'intero il pacchetto.

Lezione 15

Cosa si intende per Trasporto dati affidabile

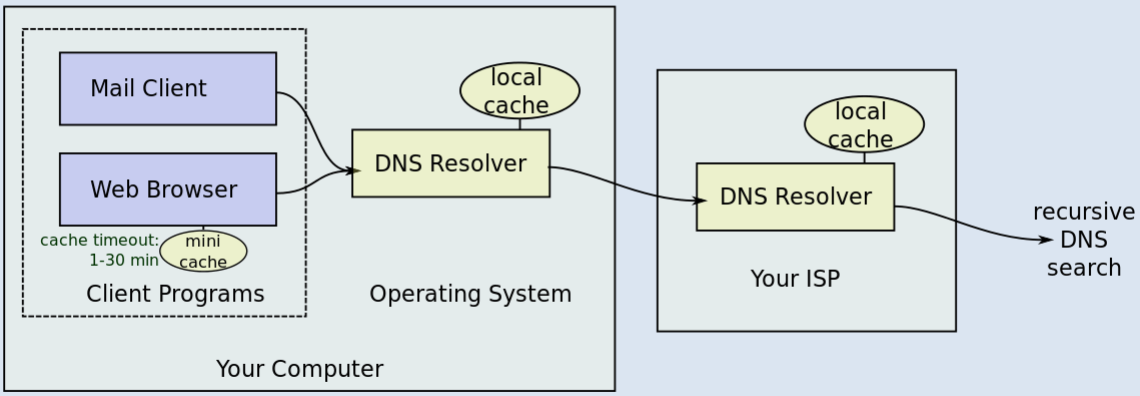
Per trasporto di dati affidabile vuol dire trasportare i pacchetti dalla sorgente alla destinazione senza perdita di pacchetti e la consegna in ordine.

Cosa servono i pacchetti di ACK e come funziona la ritrasmissione dei segmenti persi

I pacchetti ACK servono per informare la sorgente che il pacchetto è stato ricevuto correttamente o controllando i numeri di sequenza che un pacchetto non è stato ricevuto. Un pacchetto è ritrasmesso se un ack non è ricevuto prima della scadenza del time out o se si ricevano tre ACK identici. ACK, in ambito di telecomunicazioni e informatico, è il simbolo che identifica un segnale di riconoscimento (Acknowledgment in inglese) emesso in risposta alla ricezione di un'informazione completa. Tipico esempio è il pacchetto di controllo previsto dal protocollo TCP trasmesso dal ricevente al mittente per segnalare la corretta ricezione di un pacchetto dati.

L'ACK può anche essere di tipo cumulativo (quello usato dal TCP), indicando cioè l'avvenuta corretta ricezione di più pacchetti di dati. Per esempio un ACK4 indica che il pacchetto 4 che la stazione trasmittente ha inviato è stato ricevuto correttamente; implicitamente però l'ACK4 cumulativo sta ad indicare che anche i pacchetti 3, 2, 1, 0 sono stati ricevuti e non sono andati persi. Similmente un NACK (Negative-Acknowledgment) indica la mancata ricezione di un pacchetto (nel caso di NACK selettivo), o la corretta ricezione di n-1 pacchetti, ma la mancata ricezione di 1 (NACK4= il pacchetto 4 non è arrivato, ma il 3, 2, 1 e 0 si). L'ACK può essere trasmesso in un messaggio a sé stante, o essere inviato in un campo di un pacchetto utente in direzione opposta, ossia in piggyback.

DNS Domain Name Server



Cosa si intende e come funziona il controllo di flusso del TCP

Nella comunicazione TCP il destinatario ha un buffer di ricezione, il controllo di flusso permette al mittente di non sovraccaricare il buffer del destinatario trasmettendo troppi dati, troppo velocemente. Per fare questo il destinatario comunica lo spazio disponibile includendo lo spazio disponibile nel buffer nei segmenti e il mittente limita il numero di segmenti per i quali non ha ricevuto ACK inferiore all’ultimo.

Lezione 16

Cosa cambia tra controllo della congestione punto-punto e assistito dalla Rete

Controllo di congestione punto-punto **:**

• **N**essun supporto esplicito dalla rete
• **L**a congestione è dedotta osservando le perdite e i ritardi nei sistemi terminali
• **M**etodo adottato da TCP.
Controllo di congestione assistito dalla rete i router forniscono un feedback ai sistemi terminali -un singolo bit per indicare la congestione (SNA, DECbit, TCP/IP ECN, ATM) -comunicare in modo esplicito al mittente la frequenza trasmissiva.

Descrivere il three-way handshake, a livello di pacchetti scambiati, e a livello di macchina a stati

Passo 1 :
- il client invia un segmento SYN al server
- specifica il numero di sequenza iniziale
- nessun dato.

Passo 2 :
- il server riceve SYN e risponde con un segmento SYNACK
- il server alloca i buffer -specifica il numero di sequenza iniziale del server

Passo 3 : il client riceve SYNACK e risponde con un segmento ACK, che può contenere dati.
MACCHINA a STATI :
- **Closed** (stato iniziale, per uscire da questo stato si deve effettuare operazione di open)
- **Listen** (in questo stato il protocollo è attivo ed è in ascolto su una porta, quando riceve un SYN risponde con un **SYN+ACK** e passa allo stato Syn Received)
- **Syn Sent** (stato in cui si è mandato un SYN e si attende l'ACK corrispondente per un certo tempo)
- **Syn Received** (stato in cui si è ricevuto un SYN)
- **Established** (stato in cui è stata stabilita la connessione ed è possibile iniziare il trasferimento dei dati)
- **Close_Wait** (stato in cui si è ricevuto un messaggio FIN e si attende che l'applicazione chiuda la connessione)
- **Last_ACK** (stato in cui si è ricevuto il FIN dall'altro end point e si è risposto con un FIN)
- **Fin_Wait_1** (stato in cui si è inviato un messaggio FIN e si attende che l'altro end point chiuda la connessione)
- **Closing** (stato in cui si entrambi gli end point hanno mandato un FIN contemporaneamente)
- **Fin_Wait_2** (stato in cui si è inviato un messaggio FIN per il quale è stato ricevuto l'ACK e si attende il FIN dell'altro end point)
- **Time_Wait** (attende un tempo pari a **2*MSL** (Maximum Segment Lifetime) prima di chiudere la connessione per attendere eventuali richieste di ritrasmissione dell'ultimo ACK)

Come si chiude una connessione TCP

Il client chiude la socket: clientSocket.close(); Passo 1: il client invia un segmento di controllo FIN al server. Passo 2: il server riceve il segmento FIN e risponde con un ACK. Chiude la connessione e invia un FIN. Passo 3: il client riceve FIN e risponde con un ACK. - inizia l'attesa temporizzata - risponde con un ACK ai FIN che riceve. Passo 4: il server riceve un ACK. La connessione viene chiusa. Con una piccola modifica può gestire segmenti FIN simultanei.

Lezione 17

Come si rivela una perdita nel TCP

La perdita di un pacchetto, generato al TCP dal lato del mittente, avviene al verificarsi di un **time out** o alla ricezione di **tre ACK** per uno stesso segmento. In presenza di un traffico elevato, i buffer di uno o più router sono pieni e quei router scartano i pacchetti (contenenti segmenti del TCP). Il pacchetto scartato provoca il verificarsi dell'evento perdita di un pacchetto al mittente (time out o tre ACK ripetuti), che viene usato come indicatore di presenza di un canale congestionato tra mittente e destinatario.

Cosa si intende per Congestion Window e cosa indica

CongWin è una funzione dinamica della congestione percepita. A livello pratico l'idea è di aumentare il rate trasmissivo per sfruttare al meglio la banda disponibile e diminuirlo quando viene riscontrata una perdita.

Descrivere lo Slow Start del TCP

Quando si inizia a trasmettere su una connessione TCP, si usa un valore iniziale di cwnd molto piccolo, ad esempio 1 MSS (Maximum Segment Size), che corrisponde ad una velocità di trasmissione, approssimativa, di MSS/RTT. Siccome la banda disponibile al mittente potrebbe essere un po' di più di MSS/RTT, il TCP mittente prova a calcolare anche il margine a disposizione, in tempi rapidi. Quando inizia la connessione, il rate di trasmissione aumenta in modo esponenziale, fino a quando non si verifica un evento di perdita :

- Raddoppia CongWin a ogni RTT
- Ciò avviene incrementando CongWin per ogni ACK ricevuto

Cosa si intende per Additive Increase Multiplicative Decrease AIMD?

Nel controllo di congestione AIDM il Decremento moltiplicativo riduce a metà la CongWin dopo un evento di perdita mentre l'incremento additivo : aumenta CongWin di 1 MSS a ogni RTT in assenza di eventi di perdita: sondaggio.

Lezione 18

Andamento della congestion window durante una connessione TCP

CongWin è una funzione dinamica della congestione percepita. A livello pratico l'idea è di aumentare il rate trasmissivo per sfruttare al meglio la banda disponibile e diminuirlo quando viene riscontrata una perdita. Quando CongWin è sotto la soglia (Threshold), il mittente è nella fase di partenza lenta e la finestra cresce in modo esponenziale, se è sopra la soglia, il mittente è nella fase di congestion avoidance e la finestra cresce in modo lineare. Quando si verificano tre ACK duplicati, il valore di Threshold viene impostato a CongWin/2 e CongWin viene impostata al valore di Threshold. Quando si verifica un timeout, il valore di Threshold viene impostato a CongWin/2 e CongWin è impostata a 1 MSS.

Cosa cambia se una perdita di pacchetto viene riscontrata per la scadenza di un time out e per la ricezione di 3 ACK duplicati

Quando si rileva un evento di perdita = time out o ricezione di 3 ACK duplicati il mittente TCP riduce la frequenza d'invio (CongWin), il valore di Threshold viene impostato a CongWin/2 e CongWin viene impostata al valore di Threshold.

Perché il TCP è un protocollo di trasporto fair

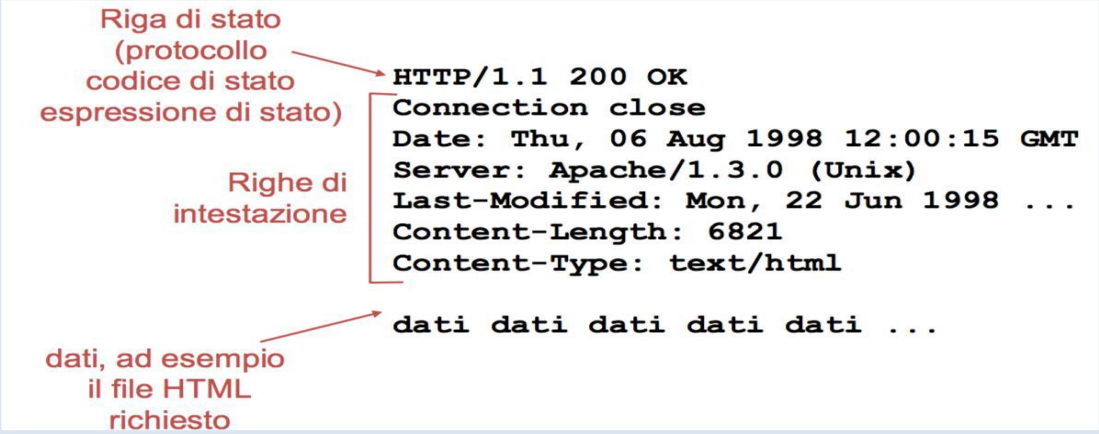
Il meccanismo di controllo della congestione visto con l'algoritmo Tahoe è detto AIDM e fa si che TCP sia fair(equo) più connessioni sono attive contemporaneamente su uno stesso canale, dopo una fase iniziale a regime ogni connessione userà la stessa percentuale della banda disponibile. Se K sessioni TCP condividono lo stesso collegamento con ampiezza di banda R, che è un collo di bottiglia per il sistema, ogni sessione dovrà avere una frequenza trasmissiva media pari a R/K.

Quali sono i limiti per cui il TCP necessita di nuove varianti per essere utilizzato nelle "Long, Fat Networks"

Un limite per cui sono necessarie nuove varianti del protocollo TCP è perché la crescita della larghezza di banda sta superando la capacità di TCP di gestire il throughput.

UDP è fair nei confronti di TCP

Le applicazioni multimediali spesso non usano TCP(non vogliono che il loro rate trasmissivo venga ridotto dal controllo di congestione), utilizzano UDP(immettono audio/video a frequenza costante, tollerano la perdita di pacchetti), questo vuol dire che in caso di congestione le applicazioni che usano UDP "rallentano" quelle che usano UDP no, quindi possiamo dire che UDP non è equo nei confronti di UDP.



Lezione 19

Quali sono i vantaggi di una rete a datagramma?

Vantaggi offerti dalle reti a datagramma :

- **a.** Non è necessario stabilire un collegamento iniziale
- **b.** Consente di effettuare collegamento senza connessioni.
- **c.** L'impostazione della chiamata non avviene a livello di rete
- **d.** I router della rete a datagramma non conservano informazioni sullo stato dei circuiti virtuali (perché non ce ne sono).
- **e.** I pacchetti vengono inoltrati utilizzando l'indirizzo del host destinatario(passano attraverso una serie di router che utilizzano gli indirizzi di destinazione per inviarli).

Qual è la differenza tra forwarding e routing?

Inoltro (forwarding) : trasferisce i pacchetti dall'input di un router all'output del router appropriato.
Instradamento (routing) :

- determina il percorso seguito dai pacchetti dall'origine alla destinazione
- Algoritmi d'instradamento

Principali differenze tra le reti a circuito virtuale e a datagramma

Nelle reti a datagramma :

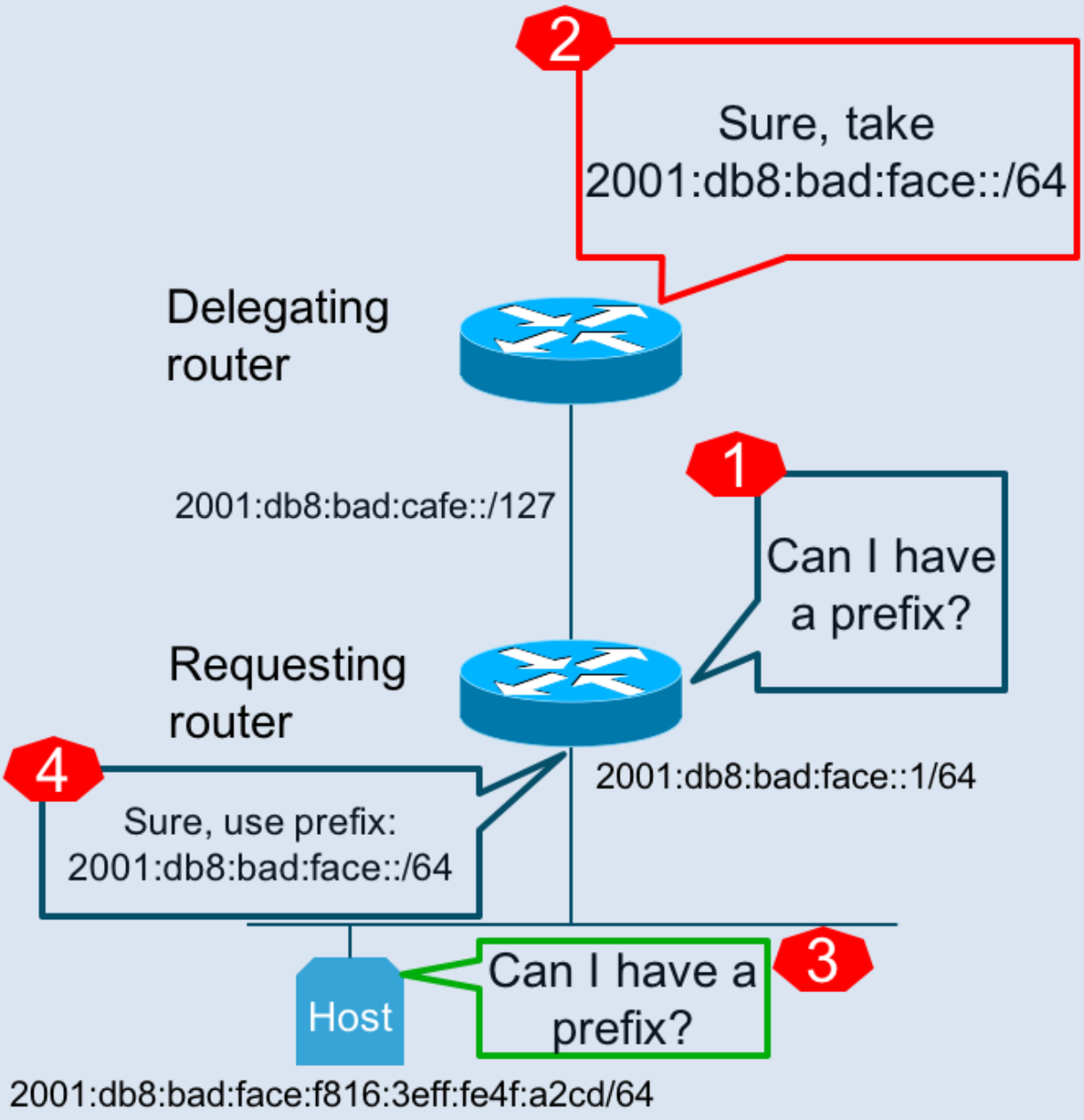
• Non è necessario stabilire un collegamento iniziale ;
• Consente di effettuare collegamento senza connessioni.

Nelle reti a circuiti virtuali :

• Il processo di individuazione del percorso viene effettuato soltanto all'inizio del collegamento ;
• I pacchetti sono ricevuti sempre nello stesso ordine in cui sono stati generati ;
• Fornisce un servizio orientato alla connessione

Lezione 20

Prefisso indirizzo IPv6 DHCPv6 Radvd



Funzionamento della Frammentazione in IPv4

L'unità massima di trasmissione (MTU) è la massima quantità di dati che un frame a livello di collegamento può trasportare. Se il datagramma IP eccede l'MTU deve essere frammentato in datagrammi IP più piccoli. Quando un datagramma viene frammentato i frammenti saranno riassemblati solo una volta raggiunta la destinazione, i bit dell'intestazione IP sono usati per identificare e ordinare i frammenti. I campi Identification, Flags, Fragment offset: controllano le operazioni di frammentazione e riassemblaggio. La frammentazione di un datagramma avviene a livello dei router, cioè alla transizione da una rete con un MTU importante ad un'altra con un MTU più debole.

Come possono coesistere IPv4 e IPv6

Si gestisce con dei tunne IP in IP. La tecnica del tunneling utilizza il principio del tunneling per cui si stabilisce un collegamento point to point tra due host. I pacchetti IPv6 vengono, così, incapsulati dall'host sorgente in pacchetto IPv4, inviati nel tunnel e, una volta giunti a destinazione, l'host li decapsula e li tratta come se fossero comunissimi pacchetti IP.Il tunneling IPv6 su IPv4 ha una difficile realizzabilità per le reti globali e quindi il suo utilizzo è limitato ad applicazioni e comunicazioni in reti locali più o meno grosse.

Quali sono le principali novità introdotte da IPv6

L'IPv6 introduce alcuni nuovi servizi e semplifica molto la configurazione e la gestione delle reti IP. La sua caratteristica più importante è il più ampio spazio di indirizzamento è lungo 128 bit, cioè 32 cifre esadecimali: 8 gruppi di 4 cifre esadecimali (ovvero 8 word di 16 bit ciascuna) in cui le lettere vengono scritte in forma minuscola. Formato dell'intestazione estremamente "snello" rende più veloci i processi di elaborazione e inoltro. **Agevola la QoS.**

Illustrare i vari campi del datagramma IP

Un datagramma è lungo 32 bit ed è composto da :

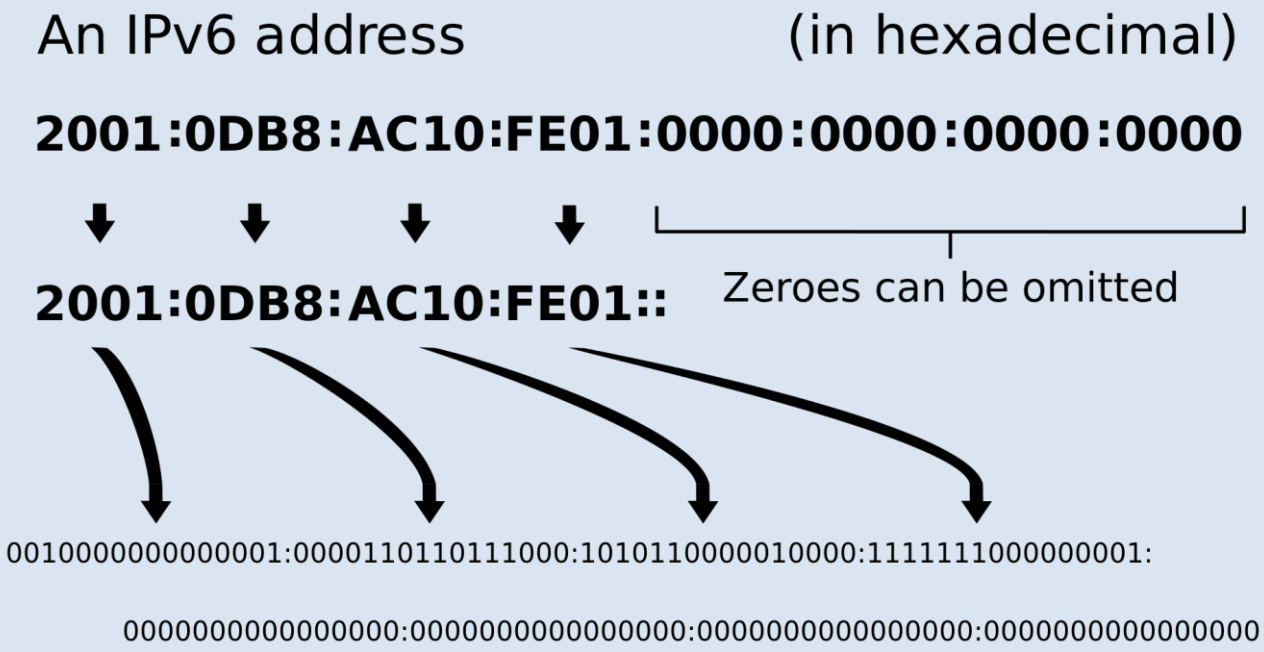
- **Versione** (4 bit), indica la versione del protocollo IP utilizzata per verificare la validità del datagramma
- **Lunghezza Intestazione** (4 bit), è il numero di parole di 32 bit costituenti l'intestazione
- **Tipo di servizio** (8 bit), indica il modo in cui il datagramma deve essere trattato.
- **Lunghezza totale** (16 bit), indica la dimensione totale del datagramma in byte.|
- **Identificazione** (16 bit), flags (3 bit) e spostamento sezione (13 bit) sono dei campi che permettono la frammentazione dei datagrammi|
- **Tempo di vita**, detta anche TTL (8bit) si decrementa ad ogni passaggio in un router
- **Protocollo** di livello superiore o upper layer (8 bit)
- **Header checksum** (16 bit) controlla l'integrità dell'intestazione per assicurarsi che non sia stata alterata durante la trasmissione| Indirizzo IP sorgente (32 bit) |Indirizzo IP destinazione (32 bit)

Lezione 21

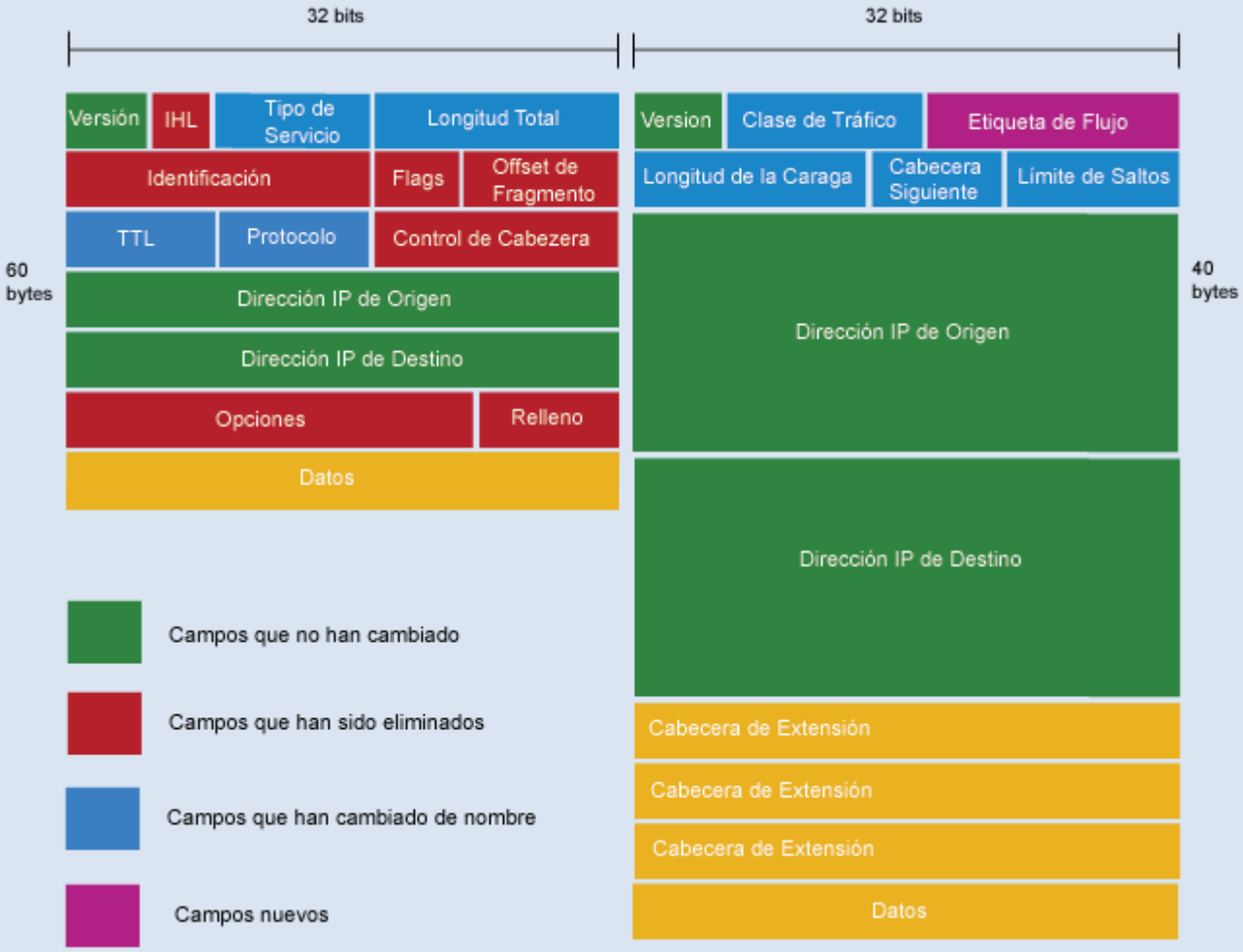
Le funzionalità del NAT

Il NAT serve principalmente a mappare gli indirizzi privati della rete locale sull'indirizzo pubblico esterno del NAT "nascondendo" dietro un unico indirizzo pubblico decine e decine di indirizzi privati (e quindi altrettanti dispositivi connessi alla rete); è un meccanismo che permette di modificare l'indirizzo IP dei pacchetti di informazioni in transito attraverso il router (o altri apparati di rete) all'interno di una comunicazione in corso tra due/più dispositivi connessi alla rete.

Indirizzo IPv6 e IPv4 | Meccanismo di transizione IPv6



IPv6 e IPv4 Header Pacchetto di Rete



Quale è la struttura di un indirizzo IPv4

Gli indirizzi IPv4 sono stringhe di 32 bit lette nella notazione decimale puntata a.b.c.d (con a,b,c,d valori compresi tra 0 e 255) è composto da **:**

- **Versione (4 bit)**, si tratta della versione del protocollo IP che si utilizza per verificare la validità del datagramma
- **Lunghezza dell'intestazione (4 bit)**, numero di parole di 32 bit costituenti l'intestazione
- **Tipo di servizio (8 bit)**, indica il modo in cui il datagramma deve essere trattato;
- **Lunghezza totale (16 bit)**, indica la dimensione totale del datagramma in byte.|
- **Identificazione (16 bit), flags(3 bit) e spostamento sezione (13 bit)** sono dei campi che permettono la frammentazione dei datagrammi|
- **Tempo di vita, detta anche TTL(8bit)** si decrementa ad ogni passaggio in un router
- **Protocollo di livello superiore o upper layer(8 bit)**
- **Header Checksum (16 bit)** controlla l'integrità dell'intestazione per assicurarsi non sia stata alterata durante la trasmissione| Indirizzo IP sorgente (32 bit) |Indirizzo IP destinazione (32 bit)

Lezione 22

A cosa serve e come funziona il Traceroute

Con il comando traceruote si può conoscere il percorso seguito dai pacchetti inviati da un host mittente ad un host destinazione infatti, esso visualizza tutti i router utilizzati per il recapito di pacchetti dal mittente al destinatario e il tempo impiegato per ciascun passaggio (hop). Se i pacchetti non arrivano al host di destinazione, il comando traceroute visualizza l'ultimo router che ha inoltrato correttamente i pacchetti.

A quale livello dello stack protocollare IP/TCP prevede nuovi protocolli e tecnologie

Il livello applicazione fornisce servizi al utente. La comunicazione è fornita per mezzo di una connessione logica. Il livello applicazione è l'unico che fornisce servizi agli utenti di Internet, la sua flessibilità consente di aggiungere nuovi protocolli/tecnologie con estrema facilità.

Che protocollo è ICMP

Internet Control Message Protocol. **ICMP** è un protocollo di servizio per reti a pacchetto che si occupa di trasmettere informazioni riguardanti malfunzionamenti (causati dai primi 8 byte del datagramma IP), informazioni di controllo o messaggi tra i vari componenti di una rete di calcolatori. ICMP è incapsulato direttamente in IP (è un protocollo di livello 3 dello stack TCP/IP) e non è quindi garantita la consegna a destinazione dei pacchetti. Viene utilizzato da molti applicativi di rete, tra cui **ping** e **traceroute**.

Quali informazioni può restituire un server DHCP

- Indirizzo del primo hop (indirizzo del router da attraversare per raggiungere Internet)
- Nome e indirizzo di un server DNS
- Network Mask
- Indirizzo IP del gateway(router LAN)

Illustrare lo scambio di messaggi client/server in DHCP

- Host invia in broadcast un messaggio "DHCP discover" [opzionale]
- Il server DHCP risponde con un messaggio "DHCP offer"[opzionale]
- Host richiede un indirizzo IP : messaggio "DHCP request"
- Il server DHCP invia l'indirizzo: messaggio "DHCP ack"

Per individuare un processo su un host è sufficiente l'indirizzo IP

No, perché su un host possono esserci diversi processi in esecuzione nello stesso momento

Quali sono le principali funzionalità del DHCP

Il DHCP permetter ad un host di ottenere automaticamente un indirizzo IP da un server, nel momento in cui si connette alla rete :

- Può rinnovare l'associazione dell'indirizzo
- Permette il riuso degli indirizzi (l'indirizzo è assegnato solo fino a quando l'host è connesso)

Lezione 23

A cosa serve un Algoritmo di instradamento

… determinare il percorso (sequenza di router) che un pacchetto deve seguire per andare dal mittente al destinatario considerando il cammino a costo minimo. Il costo può assumere diversi significati **:**

- Numero di hop (shortest path)
- Costo economico/amministrativo dei collegamenti. Sono classificati come: globale o centralizzato, statico o dinamico.

Cosa rappresenta un grafo di Rete

un grafo è un tipo di dato astratto formato da un insieme di elementi detti nodi N che possono essere collegati fra loro da linee chiamate archi E. I grafi possono essere classificati come orientati, non orientati, pesati. Una struttura dati grafo può inoltre associare ad ogni arco un valore o peso Il grafo è un'astrazione utile anche in altri contesti di rete.

Quali sono le principali novità introdotte da IPv6

IPv6 è la versione dell'Internet Protocol designata come successore dell'IPv4. Tale protocollo introduce alcuni nuovi servizi e semplifica molto la configurazione e la gestione delle reti IP. La sua caratteristica più importante è il più ampio spazio di indirizzamento è lungo 128 bit, cioè 32 cifre esadecimali: 8 gruppi di 4 cifre esadecimali (ovvero 8 word di 16 bit ciascuna) in cui le lettere vengono scritte in forma minuscola. Formato dell'intestazione estremamente "snello" rende più veloci i processi di elaborazione e inoltro. Agevola la QoS.

Come è possibile la coesistenza di IPv4 e IPv6

Si gestisce con dei tunne IP in IP. La tecnica del tunneling utilizza il principio del tunneling per cui si stabilisce un collegamento point to point tra due host. I pacchetti IPv6 vengono, così, incapsulati dall'host sorgente in pacchetto IPv4, inviati nel tunnel e, una volta giunti a destinazione, l'host li de capsula e li tratta come se fossero comunissimi pacchetti IP.Il tunneling IPv6 su IPv4 ha una difficile realizzabilità per le reti globali e quindi il suo utilizzo è limitato ad applicazioni e comunicazioni in reti locali più o meno grosse.

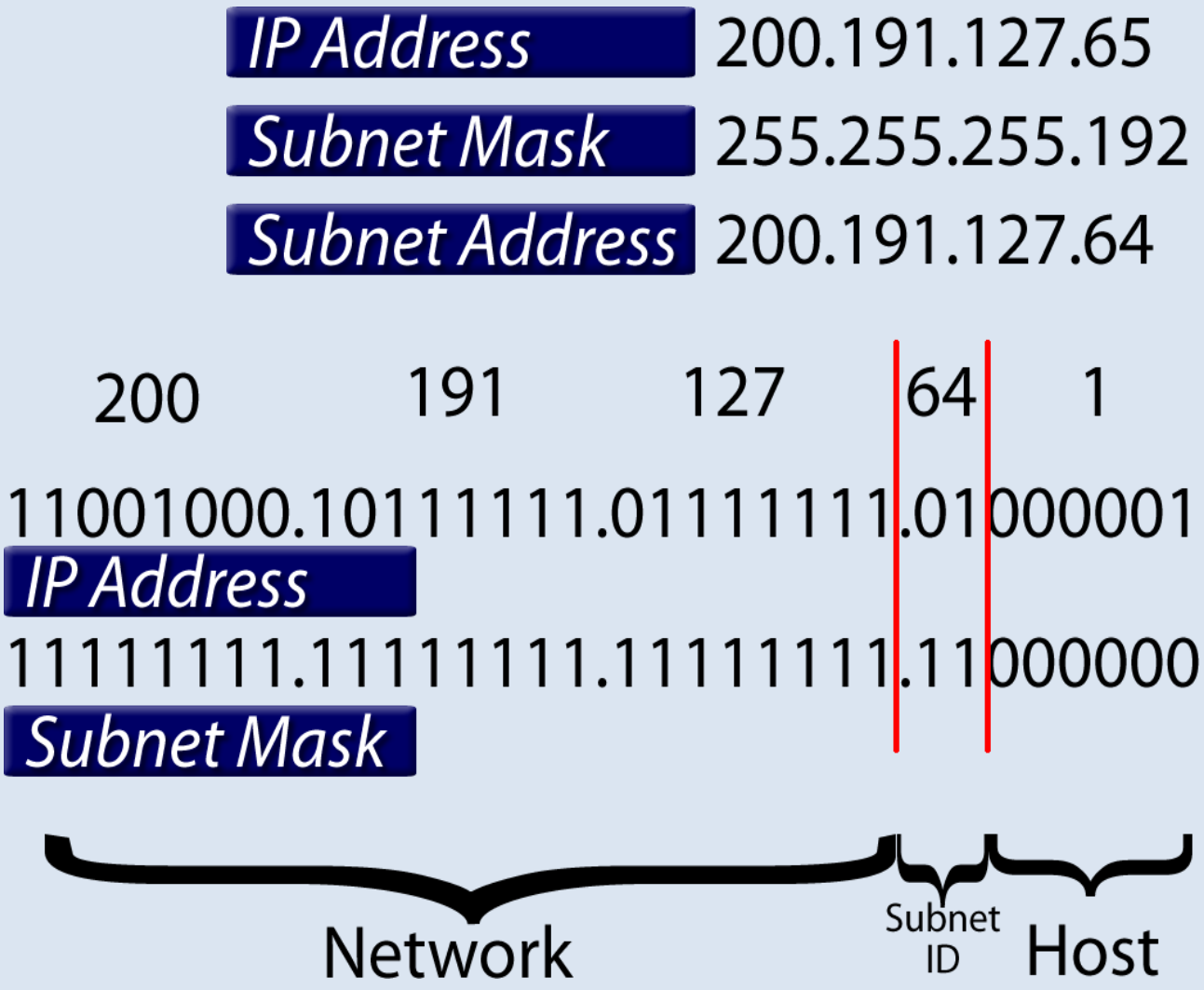
Come funziona la frammentazione in IPv4

MTU := Maximum Transmission Unit è la massima quantità di dati che un frame a livello di collegamento può trasportare. Se il datagramma IP eccede l'MTU deve essere frammentato in datagrammi IP più piccoli. Quando un datagramma viene frammentato i frammenti saranno riassemblati solo una volta raggiunta la destinazione, i bit dell'intestazione IP sono usati per identificare e ordinare i frammenti. I campi Identification, Flags, Fragment offset: controllano le operazioni di frammentazione e riassemblaggio. La frammentazione di un datagramma avviene a livello dei router, cioè alla transizione da una rete con un MTU importante ad un'altra con un MTU più debole.

Come è possibile la coesistenza di IPv4 e IPv6

Si gestisce con dei tunne IP in IP. La tecnica del tunneling utilizza il principio del tunneling per cui si stabilisce un collegamento point to point tra due host. I pacchetti IPv6 vengono, così, incapsulati dall'host sorgente in pacchetto IPv4, inviati nel tunnel e, una volta giunti a destinazione, l'host li decapsula e li tratta come se fossero comunissimi pacchetti IP.Il tunneling IPv6 su IPv4 ha una difficile realizzabilità per le reti globali e quindi il suo utilizzo è limitato ad applicazioni e comunicazioni in reti locali più o meno grosse.

Indirizzo IP della Sottorete Subnet Mask



Quali sono le principali novità introdotte da IPv6

IPv6 è la versione dell'Internet Protocol designata come successore dell'IPv4. Tale protocollo introduce alcuni nuovi servizi e semplifica molto la configurazione e la gestione delle reti IP. La sua caratteristica più importante è il più ampio spazio di indirizzamento è lungo 128 bit, cioè 32 cifre esadecimali: 8 gruppi di 4 cifre esadecimali (ovvero 8 word di 16 bit ciascuna) in cui le lettere vengono scritte in forma minuscola. Formato dell'intestazione estremamente "snello" rende più veloci i processi di elaborazione e inoltro. Agevola la ***QoS* = Quality of Service.**

Illustriamo i vari campi del datagramma IP

Un datagramma è lungo 32 bit ed è composto da **:**

- **Versione** (4 bit), indica la versione di IP utilizzata per verificare la validità del datagramma
- **Lunghezza Intestazione** (4 bit), si tratta del numero di parole di 32 bit di intestazione
- **Tipo di servizio** (8 bit), indica il modo in cui il datagramma deve essere trattato.
- **Lunghezza totale** (16 bit), indica la dimensione totale del datagramma in byte.|
- **Identificazione** (16 bit), flags (3 bit) e spostamento sezione (13 bit) sono dei campi che permettono la frammentazione dei datagrammi|
- **Tempo di vita**, detta anche TTL (8bit) si decrementa ad ogni passaggio in un router
- **Protocollo** di livello superiore o upper layer (8 bit)
- **Header checksum** (16 bit) controlla l'integrità dell'intestazione per assicurarsi non sia stata alterata nella trasmissione| Indirizzo IP sorgente (32 bit) |Indirizzo IP destinazione (32 bit)

Quale è la struttura di un indirizzo IPv4

Gli indirizzi IPv4 sono stringhe di 32 bit lette nella notazione decimale puntata a.b.c.d (con a,b,c,d compresi tra 0 e 255) è composto da :

- **Versione (4 bit)**, si tratta della versione IP che si utilizza per verificare la validità del datagramma
- **Lunghezza dell'intestazione (4 bit)**, numero di parole di 32 bit costituenti l'intestazione
- **Tipo di servizio (8 bit)**, indica il modo in cui il datagramma deve essere trattato;
- **Lunghezza totale (16 bit)**, indica la dimensione totale del datagramma in byte.|
- **Identificazione (16 bit), flags(3 bit) e spostamento sezione (13 bit)** sono dei campi che permettono la frammentazione dei datagrammi|
- **Tempo di vita, detta anche TTL(8bit)** si decrementa ad ogni passaggio in un router
- **Protocollo di livello superiore o upper layer(8 bit)**
- **Header Checksum (16 bit)** controlla l'integrità dell'intestazione per assicurarsi non sia stata alterata durante la trasmissione| Indirizzo IP sorgente (32 bit) |Indirizzo IP destinazione (32 bit)

Lezione 24

Illustrare il funzionamento dell'algoritmo DV

L'algoritmo distance vector è anche noto come algoritmo di Bellman-Ford. Per realizzare tale algoritmo ogni router mantiene, oltre alla tabella di instradamento, una struttura dati, detta distance vector per ogni linea. Il distance vector associato a ciascuna linea contiene informazioni ricavate dalla tabella di instradamento del router collegato all'altro estremo della linea. Ogni nodo invia una copia del proprio vettore distanza a ciascuno dei suoi vicini. Quando un nodo x riceve un nuovo vettore distanza, DV, da qualcuno dei sui vicini, lo salva e usa la formula B-F per aggiornare in proprio vettore distanza come segue: $D_x(y) \leftarrow \min_v\{c(x,v) + D_v(y)\}$ per ciascun nodo y in N. In condizioni “normali” Dx(y) converge a $d_x(y)$.

Illustrare il funzionamento dell'algoritmo di Dijkstra

Calcola il cammino a costo minimo da un nodo (origine) a tutti gli altri nodi della rete. -Crea una tabella d’inoltro per quel nodo. È iterativo: dopo la k-esima iterazione i cammini a costo minimo sono noti a k nodi di destinazione. Per ogni nodo z, l’algoritmo tiene traccia di un valore d_z, inizialmente posto uguale a ∞, e di un nodo u_z, inizialmente indefinito. L’algoritmo consiste semplicemente nel ripetere il seguente passo: si prende dall’insieme F un qualunque nodo z con d_z minimo, si sposta z da F in V, si spostano tutti i successori di z sconosciuti in F, e per ogni successore w di z si aggiornano i valori d_w e u_w. L’aggiornamento viene effettuato con la regola $d_w \leftarrow \min\{d_w, d_z + p_a\}$,dove a è l’arco che collega z a w. Se il valore di d_w è stato effettivamente modificato, allora u_w viene posto uguale z.

Lezione 25

Quale tra (LS o DV) in caso di guasti della Rete risulta migliore

Cosa può succedere se un router si guasta o funziona male? Vediamo le differenze in termini di "robustezza" degli algoritmi. In LS un router può comunicare via broadcast un costo sbagliato per uno dei suoi collegamenti connessi (ma non per altri). I nodi si occupano di calcolare soltanto le proprie tabelle infatti ogni nodo calcola un nuovo percorso.

In DV un nodo può comunicare cammini a costo minimo errati a tutte le destinazioni, la tabella di ciascun nodo può essere usata dagli altri per cui un calcolo sbagliato si può diffondere per l'intera rete, le decisioni di instradamento potrebbero essere incorrette fino a che l'algoritmo non converge nuovamente e può essere un percorso lento o addirittura presentare il problema del conteggio all'infinito.

Problema dell'instradamento ciclico in un algoritmo DV

Un algoritmo dinamico può essere eseguito sia periodicamente o come conseguenza diretta di un cambiamento nella topologia o nel costo di un collegamento. Gli algoritmi dinamici rispondono meglio ai cambiamenti della rete, ma sono anche maggiormente soggetti a problemi quali l'instradamento ciclico e l'oscillazione dei percorsi. Con l'algoritmo DV, distance vector ogni router mantiene, oltre alla tabella di instradamento, una struttura dati, detta distance vector per ogni linea. Con l'algoritmo DV un nodo rileva un cambiamento nel costo dei collegamenti, aggiorna il proprio vettore distanza e se si verifica un cambiamento nel costo, trasmette ai suoi vicini il nuovo DV.

I percorsi a costo minimo sono scritti e sviluppati rapidamente ma se accade un errore si verifica il fenomeno dell'instradamento ciclico (routing loop) cioè un percorso ciclico dell'instradamento che avviene quando un router invia un pacchetto su un collegamento (link) ma, a causa di errori nelle tabelle di routing, il router all'altra estremità del link non può risolverlo e lo rimanda indietro. Questo farà rimbalzare i pacchetti avanti e indietro saturando la banda (il link).

Illustrare le principali differenze tra algoritmi LS e DV

Le principali differenze tra algoritmo LS e DV sono : Complessità del messaggio : L'algoritmo LS impone che ciascun nodo conosca il costo di ciascun link nella rete. Questo richiede la spedizione di tanti messaggi per numero di nodi nella rete e numero di link. Ogni volta che il costo di un link cambia, il nuovo costo del link deve essere inviato a tutti i nodi. L'algoritmo DV richiede scambi tra i nodi adiacenti se vi si presenta una variazione e il tempo di convergenza può variare. Velocità di convergenza : LS è un algoritmo 0(n2) che richiede O(nE) messaggi, e che potenzialmente soffre di oscillazioni. DV può convergere lentamente (in funzione dei costi relativi dei percorsi e può avere percorsi ciclici durante la convergenza.

DV soffre anche del problema di conteggio all'infinito. Robustezza : Cosa può succedere se un router si guasta o funziona male? Per LS, un router può trasmettere un costo incoerente per uno dei link a esso attaccati, i nodi si occupano di calcolare soltanto le proprie tabelle, un router può comunicare via broadcast un costo sbagliato per uno dei suoi collegamenti connessi (ma non per altri). Per DV, un nodo può comunicare cammini a costo minimo errati a tutte le destinazioni, la tabella di ciascun nodo può essere usata degli altri. Un calcolo errato si può diffondere per l'intera rete, spesso creando non pochi problemi.

Lezione 26

Cosa si intende per Gateway Router

Per **Gateway Router** si intende il router appartenente a un **Sistema Autonomo AS** di router ma oltre ad eseguire lo stesso protocollo di instradamento del suo gruppo ha il compito di inoltrare pacchetti destinazioni esterne dal suo sistema autonomo.

Il Routing Gerarchico

La rete può essere vista semplicemente come una collezione di router interconnessi, ciascun router indistinguibile dagli altri nel senso che tutti eseguono lo stesso algoritmo per calcolare l'instradamento attraverso la rete ma non è effettivamente cosi, al crescere del numero di router, il tempo richiesto per archiviare le informazioni d'instradamento su ciascun host richiederebbe un'enorme quantità di memoria. Attualmente, Internet è costituita da milioni di host e dal punto di vista ideale, ciascuno dovrebbe essere in grado di amministrare la propria rete nel modo desiderato, pur mantenendo la possibilità di connetterla alle reti esterne. Per implementare la scalabilità si sono organizzati gerarchicamente i router in sistemi autonomi (AS, Autonomous System), i router di un AS eseguono lo stesso algoritmo di instradamento. L' algoritmo di instradamento in esecuzione in un AS è detto protocollo di instradamento interno al sistema autonomo (intra-AS routing protocol). Ovviamente, è necessario connettere gli AS tra loro, e pertanto uno o più router (i cosiddetti router gateway) avranno il compito aggiuntivo di inoltrare pacchetti a destinazioni esterne realizzando un instradamento gerarchico.

Gli annunci RIP

RIP (ROUTING INFORMATION PROTOCOL) è uno dei protocolli più noti di routing interno **intra-AS (protocolli gateway interni - IGP)** insieme a **OSPF** e **IGRP**. **RIP** è un protocollo a vettore distanza (tipicamente incluso in UNIX BSD dal 1982). Conta gli hop, come metrica di costo (**max = 15 hop**). **Annunci RIP :** in RIP, i router adiacenti si scambiano gli aggiornamenti d'instradamento ogni 30 secondi circa utilizzando un messaggio di risposta RIP, noto anche come annuncio **RIP** (**RIP advertisement**).Ogni messaggio contiene un elenco comprendente fino a 25 sotto reti di destinazione all'interno del sistema autonomo nonché la distanza del mittente rispetto a ciascuna di tali sotto reti.

Cosa si intende per protocollo di routing IGP

I protocolli d'instradamento (o di routing) intra-AS sono noti come protocolli gateway interni (IGP) .I protocolli intra-AS più comuni sono **:**

- **RIP :** routing information protocol
- **OSPF :** open shortest path first
- **IGRP :** Interior Gateway Routing Protocol (di proprietà Cisco)

Lezione 27

A cosa serve il Link State Advertisement in OSPF

OSPF (**Open Shortest Path First**). Il Link State Advertisement da l'informazione necessaria per ricostruire la struttura dei collegamenti all'interno dell'AS. Gli LSA vengono generati da ciascun router dell'AS secondo le competenze assegnategli, esistono quattro tipi di LSA e sono: Router LSA, Network LSA, Summary LSA, AS External LSA.

Descrizione della procedura di neighbor discovery e scambio dei database in OSPF

Il protocollo Open Shortest Path First o OSPF è uno dei protocolli di routing di tipo link state più diffusi, su reti IP. Utilizza il flooding di informazioni riguardo allo stato dei collegamenti, e l'algoritmo di Dijkstra per la determinazione del percorso a costo minimo INTRA-AS. Neighbor Discovery serve per aggiornare la lista di nodi adiacenti scambiandosi un messaggio di Hello nell'ultimo intervallo. Alla scoperta di un adiacente (neighbor) tramite OSPF Hello, il router risponde dichiarandosi in ascolto. Il vicino invia un DB vuoto mentre il router invia DB con gli header LSA. Il vicino risponde di aver ricevuto ed il router riscontra l'avvenuta ricezione. Questo è lo scambio di DataBase.

Il link state database in OSPF

Ogni router mantiene in memoria un link state database per ciascun'area sulla quale è operativo. Ogni router ha un database che contiene gli LSA di tutti gli altri router, ogni router ha lo stesso database. I database in OSPF vengono scambiati tramite neighbor discovery.

Lezione 28

Cosa sono le politiche di instradamento in BGP

Le politiche di instradamento in BGP sono Inter_As dove le politiche possono prevalere sulle prestazioni. Il controllo amministrativo desidera avere il controllo su come il traffico viene instradato e su chi instrada attraverso le sue reti.

Come si distribuiscono le informazioni di raggiungibilità in BGP

Il BGP mette a disposizione di ciascun AS un modo per: ottenere informazioni sulla raggiungibilità delle sottoreti da parte di AS confinanti, propagare le informazioni di raggiungibilità a tutti i router interni di un AS ,determinare percorsi "buoni" verso le sottoreti sulla base delle informazioni di raggiungibilità e delle politiche dell'AS. I router ai capi di una connessione TCP sono chiamati peer BGP, e la connessione TCP con tutti i messaggi BGP che vi vengono inviati è detta sessione BGP. In una sessione eBGP tra i gateway si scambiano informazioni, un sistema autonomo invia ad un altro sistema autonomo la lista di prefissi raggiungibili. Il gateway di un sistema autonomo utilizza le proprie sessioni iBGP per distribuire i prefissi agli altri router del sistema autonomo, anche due sistemi autonomi differenti si scambiano informazioni sulla raggiungibilità dei prefissi attraverso i propri gateway. Quando un router viene a conoscenza di un nuovo prefisso, lo memorizza in una nuova riga della propria tabella d'inoltro.

Che tipo di protocollo è BGP

Il Border Gateway Protocol (BGP) è uno standard "de facto" BGP mette a disposizione di ciascun AS un modo per **:**

- Ottenere informazioni sulla raggiungibilità delle sotto reti da parte di AS confinanti
- Propagare le informazioni di raggiungibilità a tutti i router interni di un AS
- Determinare percorsi "buoni" verso le sotto reti sulla base delle informazioni di raggiungibilità e delle politiche dell'AS

BGP consente a ciascuna sottorete di comunicare la propria esistenza al resto di Internet.

Lezione 29

Dove vengono duplicati i pacchetti di instradamento broadcast

I pacchetti in caso di instradamento broadcast ossia un pacchetto spedito da un nodo origine viene consegnato a tutti i nodi della rete, ciò può avvenire in tre modi **:**

- **Flooding (inondazione) :** quando un nodo riceve un pacchetto broadcast, lo duplica e lo inoltra a tutti i propri vicini. Problema : se nel grafo c'è un ciclo, più copie di un pacchetto broadcast continueranno a percorrere quel ciclo.
- **Flooding controllato :** un nodo origine pone il proprio indirizzo e un numero di sequenza broadcast nei pacchetti, prima di inviarli ai suoi vicini. Ogni nodo mantiene una lista di indirizzi d'origine e numeri di sequenza per ogni pacchetto ricevuto.
- **Broadcast su percorso inverso (RPB) :** un router riceve un pacchetto broadcast, lo trasmette su tutti i propri collegamenti in uscita solo se è pervenuto attraverso il percorso unicast più breve tra il router e l'origine. Albero di copertura Elimina i pacchetti broadcast ridondanti.

Cosa si intende per albero di copertura

In un grafo (N, A) non orientato e connesso, un albero di copertura è un albero che connette tutti i nodi del grafo nel quale sommando i pesi degli archi si ottiene un valore minimo. Ogni nodo, ossia router, invia un pacchetto broadcast solo sui collegamenti che appartengono all'albero di copertura. Per determinare l'albero di copertura si definisce un nodo centrale, i nodi inoltrano al nodo centrale il messaggio di adesione. Il messaggio prosegue fino a quando raggiunge un router che già appartiene all'albero di copertura o arriva al nodo centrale.

Definire il Multicast

Con il termine multicast, si indica la distribuzione simultanea di informazione verso un gruppo di destinatari, cioè la possibilità di trasmettere la medesima informazione a più dispositivi finali, senza dover indirizzare questi ultimi singolarmente e senza avere, quindi, la necessità di duplicare per ciascuno di essi l'informazione da diffondere. L'instradamento multicast ha come obiettivo di trovare un albero che colleghi tutti i router connessi ad host che appartengono al gruppo multicast, abbiamo due approcci, un albero basato sull'origine: viene creato un albero per ciascuna origine nel gruppo multicast e un albero condiviso dal gruppo: viene costruito un singolo albero d'instradamento condiviso per il multicast originato da tutti i mittenti.

Funzionamento dello Shortest Path Tree (Albero del percorso)

Lo shortest path tree è un approccio per determinare l'albero di instradamento multicast ed è basato sull'origine. **Albero basato sull'origine :** viene creato un albero per ciascuna origine nel gruppo multicast**.** Questo approccio utilizza l'algoritmo di Dijkstra e costruisce l'albero con il percorso più breve dall'origine a tutti i destinatari.

Lezione 30

Cosa è il controllo a ridondanza ciclica e come funziona

Il controllo a ridondanza ciclica è una tecnica di rilevazione degli errori a livello link, esamina i dati, D, come numeri binari. L' origine e la destinazione si accordano su una stringa di **r+1 bit**, conosciuta come generatore, G. L'obiettivo è scegliere r bit addizionali, R, in modo che :

a. <D,R> siano esattamente divisibili per G (modulo 2)

b. Il destinatario conosce G, e divide <D,R> per G.

Se il resto è diverso da 0 si è verificato un errore !

Quali sono i servizi offerti dal livello Link

I servizi offerti dal livello link sono : **Framing.** I protocolli incapsulano i datagrammi del livello di rete all'interno di un **frame := pacchetto di bit che costituisce un'unità strutturata di informazioni** a livello di link. Il protocollo MAC controlla l'accesso al mezzo e per identificare origine e destinatario vengono utilizzati indirizzi "MAC" Diversi rispetto agli indirizzi IP! Consegna affidabile: anche se è considerata non necessaria nei collegamenti che presentano un basso numero di errori sui bit (fibra ottica, cavo coassiale e doppino intrecciato) è spesso utilizzata nei collegamenti soggetti a elevati tassi di errori (es.: collegamenti wireless). Controllo di flusso: Evita che il nodo trasmittente saturi quello ricevente. Rilevazione degli errori: Gli errori sono causati dall'attenuazione del segnale e da rumore elettromagnetico. Il nodo ricevente individua la presenza di errori è possibile grazie all'inserimento, da parte del nodo trasmittente, di un bit di controllo di errore all'interno del frame. Correzione degli errori: Il nodo ricevente determina anche il punto in cui si è verificato l'errore, e lo corregge. Half-duplex e full-duplex Nella trasmissione full-duplex gli estremi di un collegamento possono trasmettere contemporaneamente: non in quella half-duplex.

Lezione 31

Come funziona la trasmissione con lo slotted Aloha

Slotted Aloha è un protocollo di rete che garantisce le funzionalità di accesso casuale e definisce come rilevare un'eventuale collisione e come ritrasmettere se si è verificata una collisione. Consente a un singolo nodo di trasmettere continuamente pacchetti alla massima velocità del canale e fortemente decentralizzato, ciascun nodo rileva le collisioni e decide indipendentemente quando ritrasmettere. Assumiamo che Tutti i pacchetti hanno la stessa dimensione. Il tempo è suddiviso in slot; ogni slot equivale al tempo di trasmissione di un pacchetto. I nodi iniziano la trasmissione dei pacchetti solo all'inizio degli slot. Se in uno slot due o più pacchetti collidono, i nodi coinvolti rilevano l'evento prima del termine dello slot. Quando a un nodo arriva un nuovo pacchetto da spedire, il nodo attende fino all'inizio dello slot successivo. **Se non si verifica una collisione :** il nodo può trasmettere un nuovo pacchetto nello slot successivo. **Se si verifica una collisione :** il nodo la rileva prima della fine dello slot e ritrasmette con probabilità *p* il suo pacchetto durante gli slot successivi. L'efficienza è definita come la frazione di slot vincenti nel caso di un elevato numero di nodi attivi, che hanno sempre un elevato numero di pacchetti da spedire. E un protocollo di rete atto a garantire le funzionalità di accesso multiplo al mezzo di trasmissione dati condiviso tra più utenti. Funziona come ALOHA ma la trasmissione avviene solo a intervalli equispaziati e sincroni(SLOT), la collisione o è totale o non c'è, il tempo sprecato nella collisione è minore e l'intervallo "critico" è più corto

Cosa si intende per protocollo di Accesso Multiplo

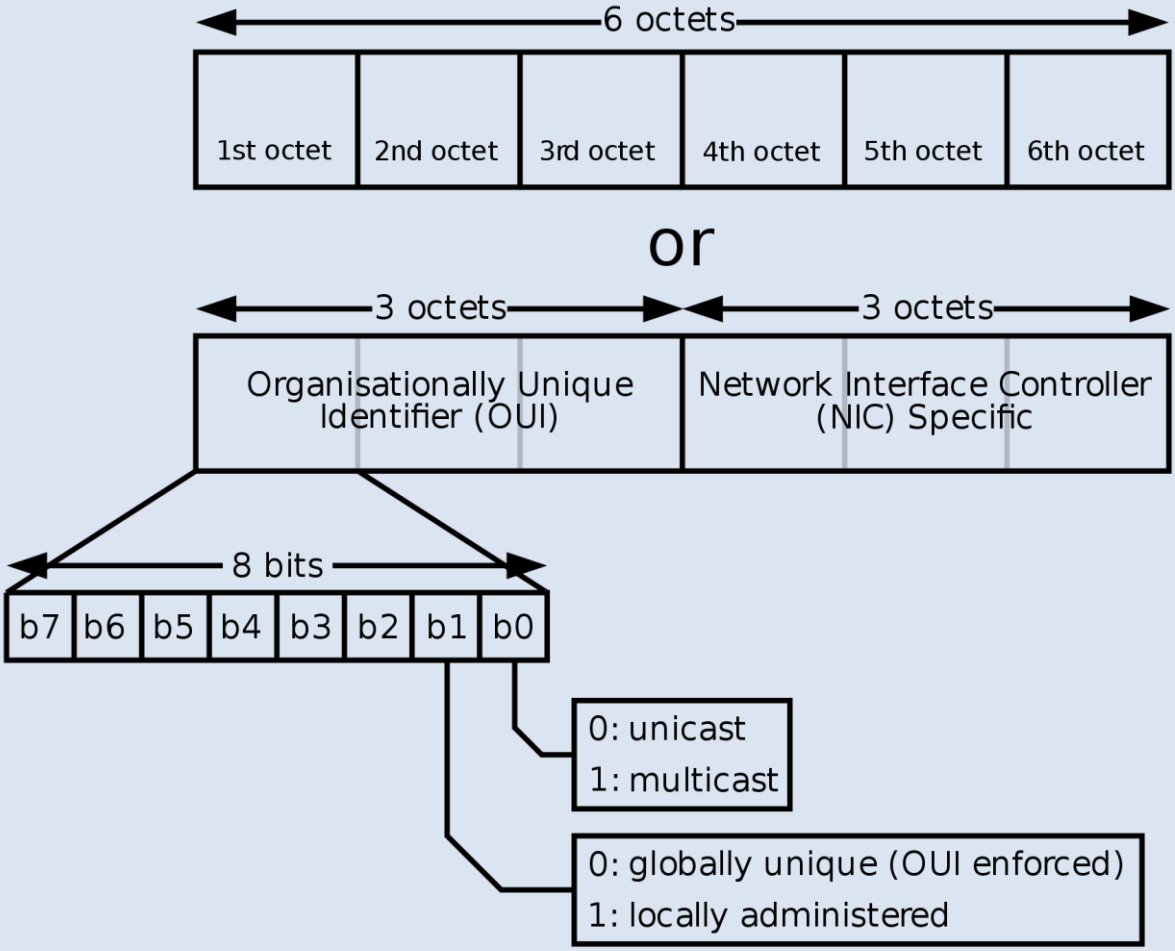
Quando tanti nodi comunicano su un canale broadcast condiviso si genera una collisione quando i nodi ricevono due o più frame contemporaneamente, per questo si adottano i Protocolli di accesso multiplo, questi protocolli fissano le modalità con cui i nodi regolano le loro trasmissioni sul canale condiviso. Si possono classificare tre categorie: Protocolli a suddivisione del canale (***channel partitioning***) Suddivide un canale in "parti più piccole" (slot di tempo, frequenza, codice), tipo TDMA: accesso multiplo a divisione di tempo e FDMA: accesso multiplo a divisione di frequenza. Protocolli ad accesso casuale (***random access***) I canali non vengono divisi e si può verificare una collisione. I nodi coinvolti ritrasmettono ripetutamente i pacchetti. Protocolli a rotazione ("*taking-turn*") Ciascun nodo ha il suo turno di trasmissione, ma i nodi che hanno molto da trasmettere possono avere turni più lunghi.

Lezione 32

Cosa si intende per CSMA/CD

Il CSMA/CD è un protocollo ad accesso multiplo rileva le collisioni e nel caso interrompe la trasmissione, CSMA/CD è rilevamento della portante differito, come in CSMA, rileva la collisione in poco tempo. Annulla la trasmissione non appena si accorge che c'è un'altra trasmissione in corso. Rilevazione della collisione: facile nelle LAN cablate e difficile nelle LAN wireless.

Indirizzo MAC | Controllo Accesso Medio | Codice di Autenticazione



Cosa si intende per CSMA/CD

CSMA/CD (acronimo inglese di Carrier Sense Multiple Access with Collision Detection, ovvero accesso multiplo tramite rilevamento della portante con rilevamento delle collisioni) è un protocollo di accesso multiplo, evoluzione del protocollo di livello MAC CSMA, nato per la risoluzione dei conflitti di trasmissione, ovvero collisioni, dovuti al CSMA puro, presenti in un certo dominio di collisione su reti locali cablate di tipo broadcast.

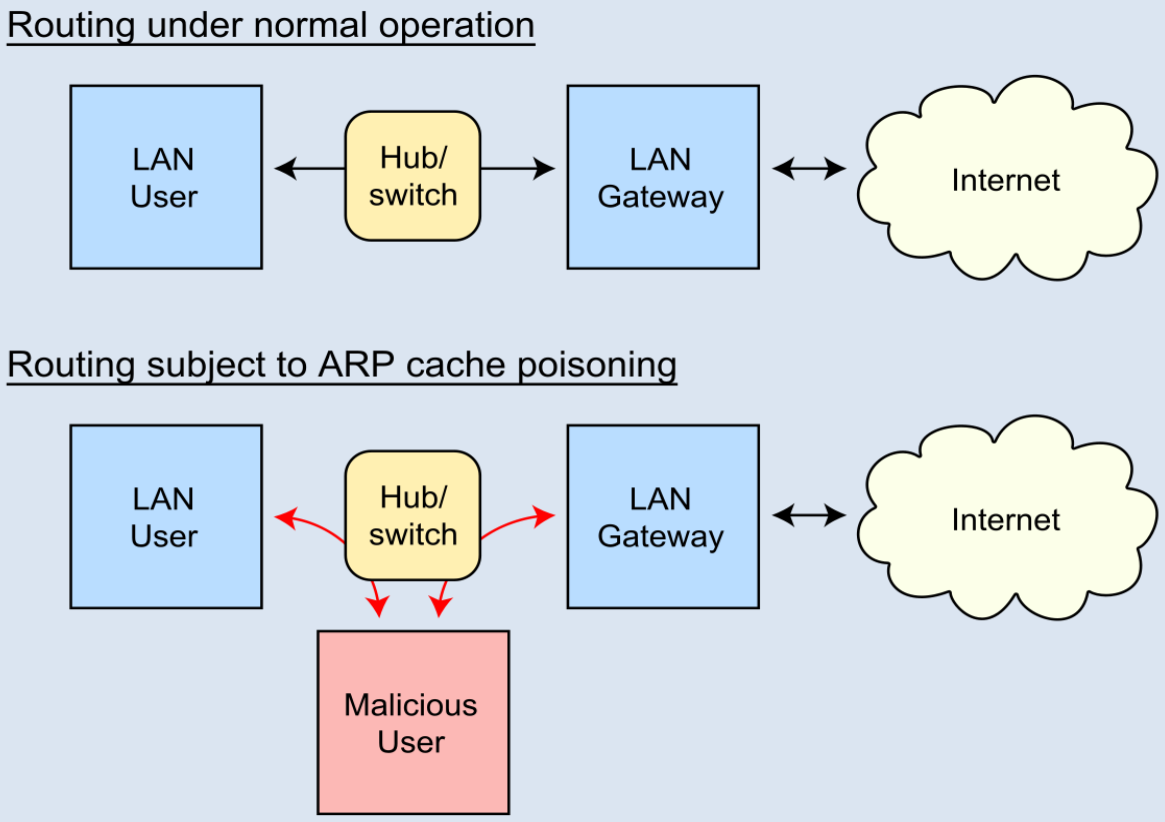
Cosa si intende per CSMA

CSMA, è protocollo indica una tecnica di trasmissione dati che si basa sull'accesso multiplo tramite rilevamento della portante. È un protocollo MAC. CSMA: si pone in ascolto prima di trasmettere: se rileva che il canale è libero, trasmette l'intero pacchetto, se invece il canale sta già trasmettendo, il nodo aspetta un altro intervallo di tempo. Il ritardo di propagazione fa sì che due nodi non rilevino la reciproca trasmissione Quando un nodo rileva una collisione, cessa immediatamente la trasmissione. La distanza e il ritardo di propagazione giocano un ruolo importante nel determinare la probabilità di collisione.

Cosa si intende per CSMA

CSMA, (acronimo inglese di Carrier Sense Multiple Access traducibile come: protocollo ad accesso multiplo con rilevamento della portante) indica una tecnica di trasmissione dati che si basa sull'accesso multiplo tramite rilevamento della portante. È un protocollo MAC posto al secondo livello del modello ISO/OSI, nelle reti a bus per condividere tra più host la capacità della rete evitando che due dispositivi trasmettano contemporaneamente generando una collisione,

Indirizzo Risoluzione Protocollo ARP



A cosa serve e come funziona il protocollo ARP

Il protocollo ARP (Address Resolution Protocol) serve per conoscere il MAC address, una volta noto l'indirizzo IP di destinazione. Ogni nodo IP (host, router) nella LAN ha una tabella ARP che contiene la corrispondenza tra indirizzi IP e MAC. A vuole inviare un datagramma a B, e l'indirizzo MAC di B non è nella tabella ARP di A. **A** trasmette in un pacchetto broadcast il messaggio di richiesta ARP, contenente l'indirizzo IP di B. Tutte le macchine della LAN ricevono una richiesta ARP. **B** riceve il pacchetto ARP, e risponde ad A comunicando il proprio indirizzo MAC.

Quali sono le categorie di protocolli di accesso multiplo

Quando elevati nodi comunicano su un canale broadcast condiviso si genera una collisione quando i nodi ricevono due o più frame contemporaneamente. Per questo si adottano i Protocolli di accesso multiplo Si possono classificare tre categorie: Protocolli a suddivisione del canale (*channel partitioning*) Suddivide un canale in "parti più piccole" (slot di tempo, frequenza, codice), tipo. TDMA: accesso multiplo a divisione di tempo e FDMA: accesso multiplo a divisione di frequenza. Protocolli ad accesso casuale (*random access*) I canali non vengono divisi e si può verificare una collisione. I nodi coinvolti ritrasmettono ripetutamente i pacchetti. Protocolli a rotazione ("*taking-turn*") Ciascun nodo ha il suo turno di trasmissione, ma i nodi che hanno molto da trasmettere possono avere turni più lunghi.

Lezione 33

Cosa è un hub e come funziona

L'hub è un dispositivo che opera sui singoli bit, all'arrivo di un bit, l'hub lo riproduce incrementandone l'energia e lo trasmette attraverso tutte le sue altre interfacce anche se su qualcuna di queste c'è un segnale.

- non implementa la rilevazione della portante né CSMA/CD
- trasmette in broadcast, e quindi ciascun adattatore può sondare il canale per verificare se è libero e rilevare una collisione mentre trasmette.
- può fornire aspetti di gestione della rete.

Come funziona l'attesa esponenziale nel CSMA/CD di Ethernet

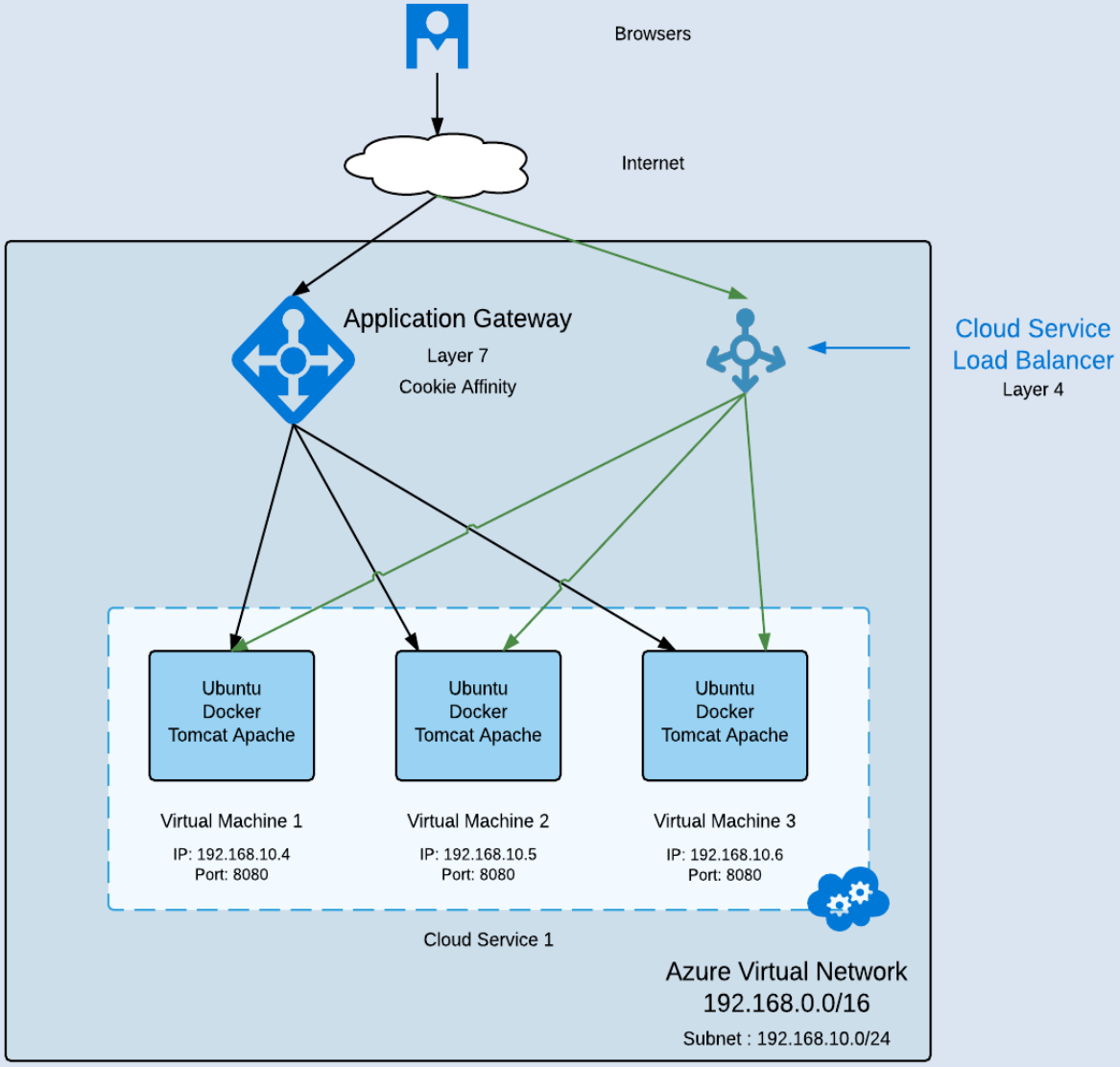
Obiettivo: l'adattatore prova a stimare quanti siano gli adattatori coinvolti. - Se sono numerosi il tempo di attesa potrebbe essere lungo. Prima collisione: sceglie K tra {0,1}; il tempo di attesa è pari a K volte 512 bit. Dopo la seconda collisione: sceglie K tra {0,1,2,3}… Dopo dieci collisioni, sceglie K tra {0,1,2,3,4,…,1023}.

Quale protocollo di accesso multiplo utilizza ethernet

Ethernet utilizza il protocollo **CSMA/CD** questo non utilizza slot ma utilizza il protocollo di accesso multiplo **CSMA/CD** con rilevamento della portante e delle collisioni. Non può trasmettere un pacchetto quando rileva che altri adattatori stanno trasmettendo: rilevazione della portante. Annulla la propria trasmissione non appena rileva che un altro adattatore sta trasmettendo: rilevazione di collisione. Prima di ritrasmettere, l'adattatore resta in attesa per un lasso di tempo stabilito arbitrariamente. Nelle fasi operative del protocollo **CSMA/CD** su Ethernet :

1. L'adattatore riceve un datagramma di rete dal nodo cui è collegato e prepara un pacchetto Ethernet
2. Se il canale è inattivo, inizia la trasmissione. Se il canale risulta occupato, resta in attesa fino a quando non rileva più il segnale.
3. Verifica, durante la trasmissione, la presenza di eventuali segnali provenienti da altri adattatori. Se non ne rileva, considera il pacchetto spedito.
4. Se rileva segnali da altri adattatori, interrompe immediatamente la trasmissione del pacchetto e invia un segnale di disturbo (*jam*), Segnale di disturbo (*jam*): la finalità è di avvisare della collisione tutti gli altri adattatori che sono in fase trasmissiva; 48 bit.
5. L'adattore rimane in attesa. Quando riscontra l'*n*-esima collisione consecutiva, stabilisce un valore *k* tra {0,1,2,…,2**m**-1}. L'adattatore aspetta un tempo pari a *K* volte 512 bit e ritorna al Passo 2.

Gateway a livello di applicazione Rete | Microsoft Azure



Lezione 34

Quali sono le differenze tra Hub e Switch

Gli Hub e gli Switch sono componenti di rete che permettono l'interconnessione tra nodi (host). Svolgono più o meno la stessa funzione, ma con significative differenze nell' indirizzamento dei pacchetti. Utilizzare un Hub è il modo più semplice per interconnettere le Lan e permette di incrementare la distanza tra i nodi. Quando un hub dipartimentale manifesta un funzionamento non conforme, l'hub della dorsale rileva il problema e lo disconnette dalla LAN.

Lo Switch filtra e inoltra i pacchetti Ethernet, esamina l'indirizzo di destinazione e lo invia all'interfaccia corrispondente alla sua destinazione, quando un pacchetto è stato inoltrato nel segmento, usa CSMA/CD per accedere al segmento. esclusivamente alla porta del destinatario mappata, permettendo un dialogo più veloce minimizzando il traffico inutile che ritarderebbe la consegna dei pacchetti, l'uso degli switch è trasparente, gli host sono inconsapevoli della presenza. Gli switch non hanno bisogno di essere configurati. Rispetto a un hub, uno switch isola il traffico.

Come funziona il processo di autoapprendimento degli Switch

Le operazioni sono eseguite mediante una tabella di commutazione. Lo switch archivia nelle proprie tabelle l'indirizzo MAC, l'interfaccia e il momento dell'arrivo. Se lo switch non riceve pacchetti per un determinato lasso di tempo, da un determinato indirizzo sorgente, lo cancella. Lo switch apprende quali nodi possono essere raggiunti attraverso determinate interfacce quando riceve un pacchetto, lo switch "impara" l'indirizzo del mittente e registra la coppia mittente/indirizzo nella sua tabella di commutazione, se lo switch non conosce dove si trova un determinato nodo lo invia a tutte le interfacce. Le operazioni sono eseguite mediante una tabella di commutazione.

Lo switch archivia nelle proprie tabelle :

- L'indirizzo MAC, l'interfaccia e il momento dell'arrivo.
- Se lo switch non riceve pacchetti da un determinato indirizzo sorgente, lo cancella.
- Lo switch apprende quali nodi possono essere raggiunti attraverso determinate interfacce
- Quando riceve un pacchetto, lo switch "impara" l'indirizzo del mittente
- Registra la coppia mittente/indirizzo nella sua tabella di commutazione

Cosa si intende per Commutazione Cut-Through

La commutazione cut-through è un in cui lo switch inizia a inoltrare un frame prima che l'intero frame sia stato ricevuto. Quando lo switch inizia la trasmissione della parte iniziale del pacchetto anche se questo non è pervenuto integralmente (switching fast forward). Lo switch cut-through riduce il ritardo solamente di un tempo compreso tra 0,12 e 1,2 ms, ed esclusivamente con carichi leggeri del collegamento in uscita.

Quali sono le differenze tra Switch e Router

Entrambi sono dispositivi store-and-forward, i router sono dispositivi a livello di rete mentre gli switch a livello di link. I router mantengono tabelle d'inoltro e implementano algoritmi d'instradamento, gli switch mantengono tabelle di commutazione e implementano il filtraggio e algoritmi di autoapprendimento.

Lezione 35

Cosa è il protocollo 802.1 Q

Il protocollo 802.1Q (nome del protocollo di incapsulamento definito da IEEE) è uno standard che permette a più reti virtuali VLAN di condividere lo stesso collegamento fisico senza perdita di informazioni tra un apparato e un altro.802.1Q non incapsula il frame originale, ma aggiunge 4 byte all'header. In pratica 802.1Q serve agli switch sotto VLAN in cascata, per sapere che un frame che arriva a una porta di trunking appartiene a una VLAN piuttosto che ad un'altra.

Cosa è una Trunk Port

Una porta in Trunk è una connessione punto-punto tra due switch (ad esempio porta 16 del trasmittente e porta 1 del ricevente) e/o un altro apparato di networking (es. Router) interconnessi in cascata per realizzare una VLAN su switch multipli. I Trunk possono "far passare" più VLAN su un singolo link e permettono alle VLAN di essere raggiunte attraverso l'intera rete. In grandi aziende con numerosi host, si può ricorrere alle VLAN su switch multipli collegati in cascata, con la modalità "trunk port" che con il protocollo 802.1q aggiunge campi addizionali all'headerd el frame dei pacchetti Ethernet.

Come si realizza una VLAN

Una Virtual Local Area Network (VLAN) è un piccolo segmento logico all'interno di un'ampia rete fisica collegata tramite cavi. Il raggruppamento delle diverse stazioni in un'unica rete avviene indipendentemente dalla loro localizzazione: infatti, finché esse sono collegate ad una stessa LAN, possono essere raggruppate in un'unica VLAN. Non è un problema se la LAN si estende su più switch: la cosa importante è che lo switch sia adatto per la VLAN. **Ci sono in genere due modi per realizzare una VLAN :**

- Port Based (Private VLAN), lo switch assegna una VLAN a delle porte; Tramite "Traffic isolation" le porte dello switch vengono raggruppate e assegnate (con il software di gestione dello switch) in maniera di realizzare un secondo switch indipendente dal primo, una sorta di switch nello switch.

- Tagged (802.1Q), lo switch associa un indirizzo IP/MAC ad una VLAN. In grandi aziende con numerosi host, si può ricorrere alle VLAN su switch multipli collegati in cascata, con la modalità "trunk port" che grazie al protocollo 802.1q aggiunge campi addizionali all'headerd el frame dei pacchetti Ethernet.

Lezione 36

Perché l'ARP deve precedere la richiesta DNS

Per spedire un frame al **Gateway il DNS** ha bisogno dell'indirizzo MC che viene fornito da ARP. ARP è un protocollo ausiliario di livello rete il cui scopo è ottenere l'indirizzo MAC di una stazione di cui è noto l'indirizzo IP. Prima di spedire una richiesta HTTP, un host client ha bisogno della risoluzione del nome del web server che desidera, tramite DNS.Crea quindi la richiesta DNS e la incapsula in UDP e IP e poi in Ethernet. Subito dopo deve spedirla al Router Gateway per instradarla, perciò chiede, tramite Broadcast, ad ARP il MAC Address del Router. Una volta che il Router l'ha ricevuta, risponde con un ARP Replay contenente il suo MAC Address. A questo Punto l'host client conosce il MAC Address del Router Gateway e gli spedisce il frame contenente la query DNS.

Elencare in ordine i protocolli coinvolti nella richiesta di una web page

Per spedire la richiesta http, il client instaura una connessione TCP con il server TCP/IP. Per "navigare" in internet un host client ha bisogno di essere connesso alla rete Lan tramite Ethernet. Necessita di avere assegnato un indirizzo IP manualmente o con DHCP. In DHCP la richiesta viene incapsulata in UDP e con DHCPACK il server trasporta al client l'IP Address assegnato, l'IP Address del Gateway e l'IP Address del DNS. Tramite 802.3 Ethernet il client ora ha il suo IP e conosce gli IP del Gateway e del DNS. Prima di spedire una richiesta HTTP, un host ha bisogno della risoluzione del nome del web server da contattare, tramite DNS. Crea quindi la richiesta DNS e la incapsula in UDP e IP e poi in Ethernet. Subito dopo deve spedirla al Router Gateway per instradarla, perciò chiede, tramite Broadcast, ad ARP il MAC Address del Router. Una volta che il Router l'ha ricevuta, risponde con un ARP Replay contenente il suo MAC Address. A questo Punto l'host client conosce il MAC Address del Router Gateway e gli spedisce il frame contenente la query DNS. A questo punto il Datagramma della query DNS viene inoltrato tramite lo switch al Gateway. Tramite Rip, OSPF, IS-IS e/o BGP e viene ricevuto dal Server DNS che restituisce l'IP Address del Server WEB. Ora il client deve stabilire una connessione TCP con il Server WEB. Tramite TCP SYN (1° passo del treeway handshake) la richiesta arriva al Server WEB che risponde con TCP SYNACK (2° passo del 3-way handshake) e manda l'ACK al client per "stabilire" la connessione. Ora è il momento del HTTP Request e Replay, il Datagramma arriva al Server WEB che risponde con HTTP Replay che arriva al client. Ora tramite protocollo HTTP, la pagina richiesta scende ed è visualizzata nel browser tramite le funzioni di parsing.

Perché per contattare il DHCP non è necessario effettuare l'ARP

Per potersi connettere alla rete ad un device mobile deve essere assegnato un indirizzo IP e conoscere l'indirizzo IP del gateway e del server DNS e per far ciò basta il DHCP. ARP è un protocollo ausiliario di livello rete il cui scopo è ottenere l'indirizzo MAC di una stazione di cui è noto l'indirizzo IP per cui se prima non viene attivato il DHCP, non si può attivare ARP.

Quali informazioni è necessario ottenere appena ci si connette ad una nuova rete per poter navigare in Internet

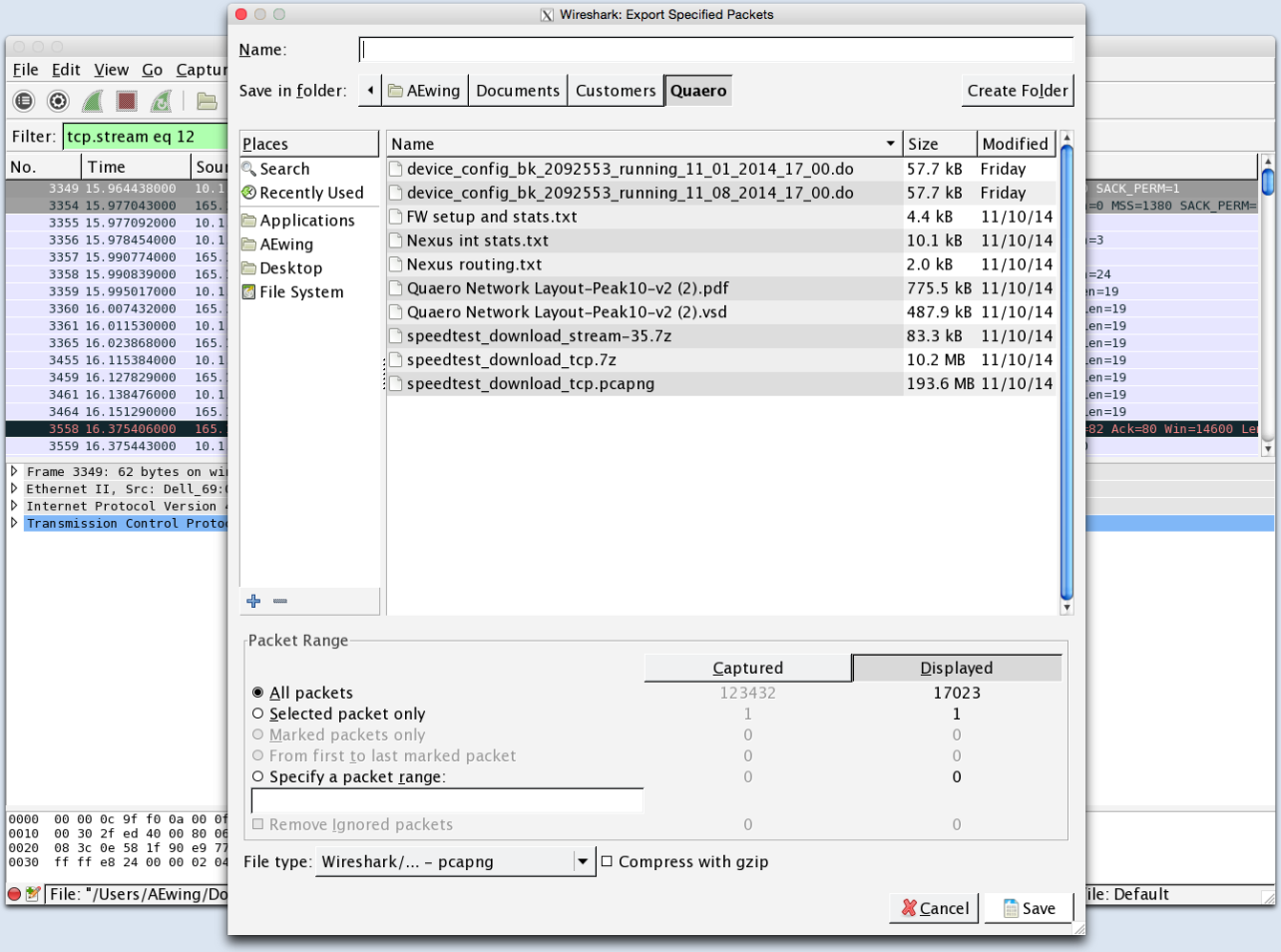
Nella navigazione internet, per un host appena connesso ad una rete, il primo protocollo utilizzato è DHCP. Per "navigare" in internet un host client ha bisogno di essere connesso alla rete Lan tramite Ethernet. Necessita di avere assegnato un indirizzo IP manualmente o con DHCP.

Lezione 37

Cos'è Wireshark

Wireshark è un software

Software Wireshark | Protocollo di controllo della Trasmissione



Lezione 38

Come funziona il CDMA

Code Division Multiple Access (CDMA) permette ai diversi trasmettitori di inviare informazioni contemporaneamente su un singolo canale di comunicazione. Il "codice" unico assegnato ad ogni utente: "code set partitioning" "partizionamento del set di codici" - Tutti gli utenti condividono la stessa frequenza, ma ognuno ha il proprio codice per codificare i dati - Permette a più utenti di "coesistere" e trasmettere simultaneamente con interferenza minima. Ciò assicura che la larghezza di banda disponibile è utilizzato in modo ottimizzato. La comunicazione radio si avvale di due risorse: la frequenza e il tempo.

Cosa si intende per problema del nodo nascosto

Il problema del terminale nascosto, nelle reti wireless, si verifica quando un nodo è visibile da un Access Point (AP) wireless, ma non da altri nodi che possono vedere lo stesso AP. Questo comporta una serie di difficoltà nel controllo di accesso al mezzo. Nelle reti wireless, il problema del terminale nascosto si verifica quando un nodo è visibile da un Access Point (AP) wireless, ma non da altri nodi che possono vedere lo stesso AP. Questo comporta una serie di difficoltà nel controllo di accesso al mezzo. Ad esempio i nodi A e B sono in copertura, i nodi B e C sono in copertura ma i nodi A e C non sono in copertura, non saranno consapevoli di poter creare collisioni e interferenza su B (se entrambi trasmettono a B). In questo caso A è un nodo nascosto per C e viceversa.

A cosa serve la base station in una Rete Wireless

Normalmente connessa a una rete cablata, (relay) è responsabile dell'inoltro dei pacchetti tra la rete cablata e gli host wireless nella sua "area". I terminali mobili non comunicano mai direttamente ma sempre tramite un stazione fissa (Base station, BS) di riferimento. La struttura delle reti cellulari prevede un punto di accesso fisso BS per ogni cella ed ogni cellulare utilizza la BS della cella in cui al momento risiede.

Lezione 39

Come funziona il meccanismo per evitare le collisioni in 802.11

Per evitare le collisioni si deve permettere al mittente di "prenotare" il canale piuttosto che accedere in maniera random durante trasmissioni "lunghe", Il mittente prima invia un pacchetto request-to-send (RTS) alla BS usando CSMA, anche RTS possono comunque collidere con altri RTS • BS invia in broadcast un clear-to-send CTS in risposta a RTS, il CTS viene ricevuto da tutti i nodi - Il mittente invia i dati - Gli altri nodi aspettano.

Quali sono le differenze tra passive e active scanning durante la fase di associazione in 802.11

Quando un host vuole associarsi ad un AP ha bisogno di acquisire la sincronizzazione relativa alle informazioni dall'Access Point. Effettua una scansione dei canali, in attesa di ***beacon frames*** che contengono il nome dell'AP (SSID) e il suo MAC address seleziona l'AP a cui associarsi, può effettuare l'autenticazione. Questo può avvenire in due modi **passive scanning** Frame beacon inviati dagli AP, Invio di un frame di richiesta associazione dal host all'AP selezionato, Invio di un frame di risposta di associazione dall'AP selezionato a Host. **active scanning** Frame sonda di richiesta inviato in broadcast da Host, Frame sonda di risposta inviato dagli AP ,Invio di un frame di richiesta di associazione da Host all'AP selezionato, Invio di un frame di risposta di associazione dall'AP selezionato a Host.

Come funziona il power management in 802.11

Il nodo può comunicare all'AP che va in modalità "sleep" fino al prossimo beacon frame". L'AP capisce di non inviare frame a quel nodo, si "sveglia" prima del prossimo beacon frame. Il beacon frame: contiene la lista dei nodi i cui frame sono stati memorizzati dall'AP. Il nodo rimarrà "sveglio" se ci sono frame da ricevere (li deve richiedere in maniera esplicita), altrimenti torna in modalità "sleep".

Lezione 40

Quali sono gli elementi di una rete 4G

Gli elementi di una rete 4G sono : **eNodeB** : discendente logico della **Base Station** 2G e del 3G radio network Controller (Node B) Nel piano dati trasmette I datagrammi tra utente e gateway tramite un tunnel (analogo a quanto visto per I Tunnel **IPv6-IPv4**). Nel piano di controllo gestisce registrazione e mobilità per conto dell' utente **Packet Data Network Gateway** (P-GW) : assegna indirizzi IP a utente e si occupa della **Quality of Service - QoS** (ad esempio garantire un certo ritardo massimo e una certa percentuale di perdite) Serving Gateway (S-GW): nodo di appoggi della mobilità del piano Mobility Management Entity (MME): gestisce la mobilità per l'UE residente nella cella che controlla Home Subscriber Server (HSS): contiene le informazioni dell'utente tipo Capacità di roaming, profilo di QoS, informazioni di autenticazione.

Quale è la differenza principale tra reti cellulari 2/3G e 4G

Le reti cellulare 2G è la vecchia generazione e si poteva usare solo la voce, il 3G è una rete che lavora in parallelo con quella 2G e abbiamo l'utilizzo della rete voce e della rete dati. Con il **4G l'architettura di rete viene unificata e completamente basata su IP**: a differenza delle precedenti reti cellulari, sia dati che voce vengono trasportati in datagrammi IP.

Cosa è OFDM

LTE Radio Access Network utilizza OFDM (Multiplexing a divisione di frequenza ortogonale: una combinazione di multiplexing a divisione di frequenza e di tempo). L'idea base consiste nello scomporre il flusso dei dati da trasmettere in N flussi più lenti che si trasmettono in parallelo mediante un insieme di portanti tali da non avere interferenza mutua tra i flussi in ricezione, grazie alla proprietà di ortogonalità tra le portanti.

Cosa si intende per rete cellulare e cos'è una cella

Una rete cellulare è una rete che permette in tutti i punti di un territorio la comunicazione, invece una cella identifica un aria geografica. Una rete cellulare è una rete che permette la telecomunicazione in tutti i punti di un territorio suddiviso in aree di non grandi dimensioni, chiamate "celle", un device mobile si può muovere attraverso la rete passando da una cella, che copre una determinata regione geografica, all'altra senza interrompere la comunicazione (**handoff**)

Lezione 41

Cosa si intende per care-of-address

Il care-of address è utilizzato nel **indirect routing**, è un indirizzo IP temporaneo per un dispositivo mobile. Ciò consente a un home agent di inoltrare messaggi al dispositivo mobile. Il care-of address è l'indirizzo dinamico che viene assegnato al host quando si connette ad una "visited network". Usato dall'home agent per inoltrare i pacchetti al device mobile (dispositivo Mobile). Molto spesso, realizzato come normale indirizzo IP ma utilizzato SOLO da Mobile IP per forwarding e per la e le funzionalità di gestione.

Cosa è problema del routing triangolare

Il problema del routing triangolare si ha quando il correspondent si trova nella stessa rete del device mobile. Come soluzione si utilizza l'Optimal Routing che permette al correspondent node di non instradare i pacchetti incapsulati verso la Home network ma direttamente al care-of-address, in questo modo il corrispondente nodo gestisce la corrispondenza tra home agent e care-of -address.

Lezione 42

Descrivere l'handoff nella rete cellulare con MSC diversi

Per non interrompere una chiamata, quando un device mobile si sposta da una cella all'altra in MSC diversi collegati tra loro, il BSS al quale si è collegati invia una richiesta di handoff al proprio MSC la quale viene "girata" all'MSC successivo che controlla la cella di destinazione. ESEMPIO: primo MSC visitato dalla stazione mobile quando vengono inizializzate le chiamate e non può cambiare durante la chiamata. Per tutta la sua durata, indipendentemente dal numero di trasferimenti inter-MSC effettuati dalla stazione mobile, la chiamata è instradata da MSC home a MSC anchor e, in seguito, da questo a quello visitato.

Descrivere l'handoff nella rete cellulare con lo stesso MSC

L'handoff è la procedura che permette di garantire continuità del servizio quando una dispositivo (stazione) stazione mobile passa da una AP all'altra.

I passi dell'Handoff (passaggio di mano) nello stesso MSC sono :

a. La vecchia BSS comunica all'MSC che sta per essere eseguito un handoff, e fornisce la lista della/e nuova/e BSS cui l'utente mobile sarà associato.
b. MSC inizializza un percorso (alloca risorse) per la nuova BSS.
c. La nuova BSS alloca e attiva un canale radio per la stazione mobile.
d. La nuova BSS trasmette a MSC; vecchia BSS pronta.
e. La vecchia BSS dice al device di eseguire l'handoff verso la nuova BSS.
f. Il device segnala alla nuova BSS di attivare il nuovo canale.
g. Il device segnala il completamento dell'handoff alla nuova BSS, MSC inoltra chiamata.
h. Le risorse allocate vengono rilasciate.

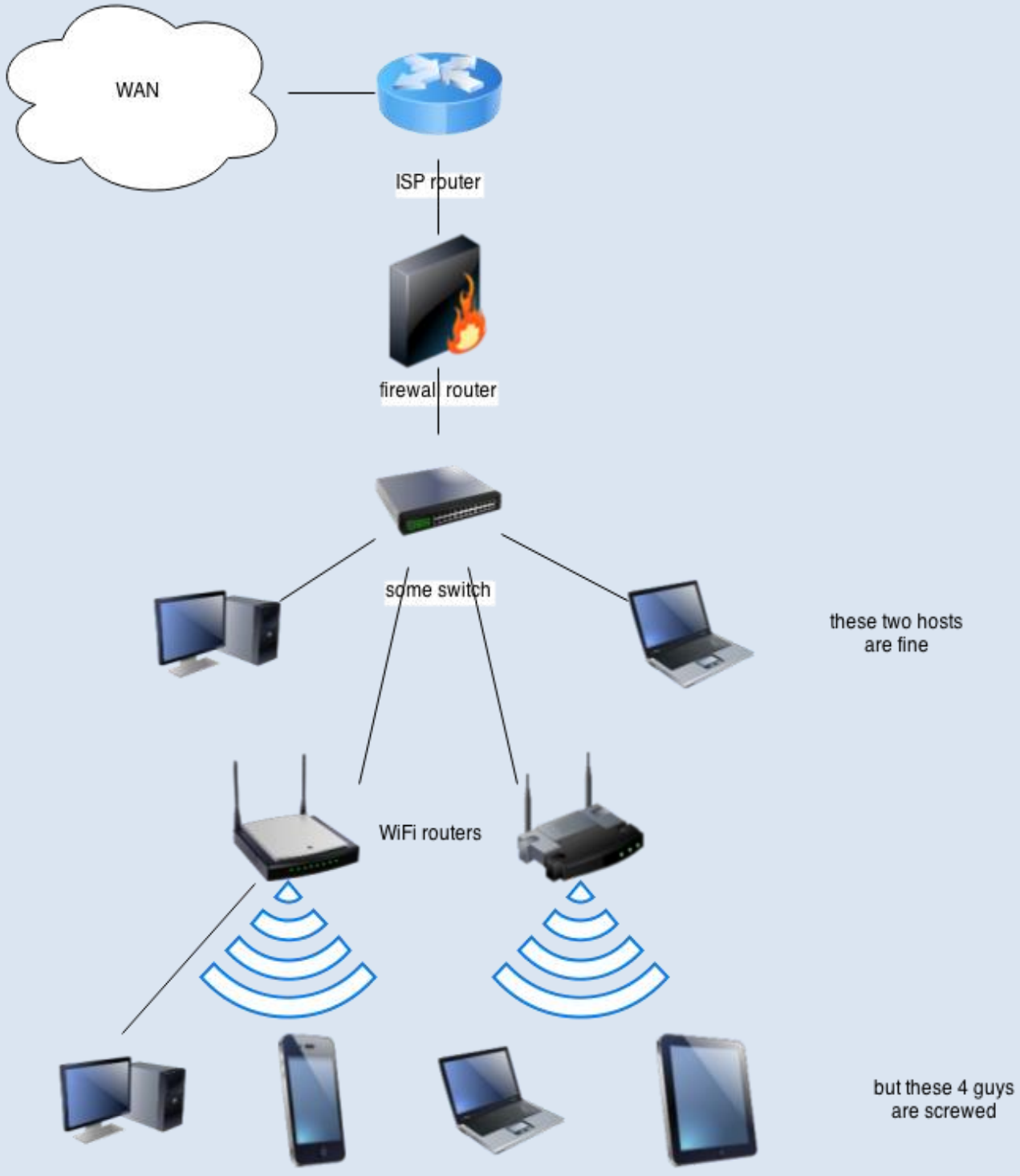
Come funziona l'indirect routing di mobile IP

Nell'IR mittente e destinatario appartengono a reti fisiche diverse. La comunicazione dal correspondent node al nodo mobile passa attraverso l'home agent, che la inoltra al foreign address(tunnel IP in IP) del nodo remoto. Il correspondent invia i pacchetti utilizzando l'home address del device mobile; home agent intercetta i pacchetti e li inoltra al foreign agent che una volta ricevuti li inoltra al device mobile; il device mobile risponde direttamente al correspondent. Utilizza due indirizzi: permanent adress e care of adress. Nell'IR mittente e destinatario appartengono a reti fisiche diverse. La comunicazione dal correspondent node al nodo mobile passa attraverso l'homeagent, che la inoltra al foreign address (tunnel IP in IP) del nodo remoto Il correspondent invia i pacchetti utilizzando l'home address del device mobile; home agent intercetta i pacchetti e li inoltra al foreign agent che una volta ricevuti li inoltra al device mobile; il device mobile risponde direttamente al correspondent. Utilizza due indirizzi: permanent adress e care of adress. MPLS è una tecnologia per reti IP che permette di instradare flussi di traffico multiprotocollo tra nodo di origine e nodo di destinazione tramite l'utilizzo di identificativi (label) tra coppie di router adiacenti e semplici operazioni sulle etichette stesse.

A cosa serve la fase di registrazione nella mobilità

La fase di registrazione nella mobilità serve a rendere visibile il device mobile al foreign agent e a segnalare la sua posizione all'home agent. Otteniamo come risultato finale che il foreing agent è a conoscenza del device mobile e l'home agent conosce la posizione del divice mobile.

Router Wireless Rete di Computer | Query di Instradamento



Lezione 43

LSP | LER | LSP | LSR | MPLS
LSP (Label Switched Path o abbreviato LSP è un cammino attraverso una rete MPLS

LER (Label Edge Router) d'ingresso applica la Label al pacchetto e lo invia sul corretto

LSP (Label Switched Path) Un Label Switched Path, o abbreviato LSP è un cammino attraverso una rete MPLS, impostata da un protocollo di segnalazione come LDP, RSVP-TE, BGP o CR-LDP. L'LSP viene anche chiamato tunnel MPLS poiché è opaco rispetto agli altri livelli.

LSR (Label Switched Router) sono Nodi che commutano il pacchetto, sostituendo la Label. Il LER d'uscita LER toglie la Label e inoltra il pacchetto con la normale procedura IP

MPLS (Multiprotocol Label Switching) è una tecnologia per reti IP che permette di instradare flussi di traffico multiprotocollo tra nodo di origine e nodo di destinazione tramite l'utilizzo di identificativi (label) tra coppie di router adiacenti e semplici operazioni sulle etichette stesse.

Operazioni che possono essere effettuate dei router MPLS sulle label

Per l'uso di MPLS nelle reti IP serve un'infrastruttura con router che supportano MPLS collegati da almeno un Interior Gateway Protocol (IGP) comune, che garantisce la visibilità a tutti i router. Poi vengono stabiliti i dati dei percorsi, denominati Label Switched Paths (LSP). Il primo router trasmette ai pacchetti, che vengono inviati in rete MPLS, un header MPLS aggiuntivo, che viene aggiunto tra le informazioni del secondo e del terzo livello con l'operazione chiamata "pushing". Sul percorso di trasmissione i singoli hop coinvolti scambiano il label con delle proprie informazioni di connessione (latenza, banda larga e hop di destinazione) tramite una variante adattata: questo procedimento è spesso chiamato "swapping". Alla fine del percorso viene eliminato di nuovo il label dall'header IP durante un'operazione "popping". Le operazioni sono denominate Pushing(aggiunge la label "in" iniziale - Ingress LSR/entrata dominio MPLS) Swapping (mappa la label "in" in "out" in ogni LSR) Popping(rimuove la lable "out" -egress LSR/uscita dominio). Un router che supporta la tecnica MPLS è denominato Label Switching Router (LSR). La LSR esamina la label associata al pacchetto sul link entrante, determina la porta d'uscita accedendo ad una Forwarding Table (FT), sostituisce la vecchia etichetta con la nuova valida sul link d'uscita(label swapping), trasferisce in uscita il pacchetto.

I principali vantaggi di MPLS, rispetto a una rete IP standard

a. Tabelle di routing molto piccole e look-up molto veloce (il router deve leggere una label, invece di fare longest prefix match degli indirizzi)
b. Virtual Private Network
c. Traffic Engineering
d. Path protection e fast reroute

Il rilancio dei pacchetti è notevolmente semplificato e quindi si ottiene un miglioramento delle prestazioni di un router IP; Tabelle di routing molto piccole e look-up molto veloce (il router deve leggere una label, invece di fare longest prefix match degli indirizzi); Virtual Private Network; un insieme di pacchetti può essere forzato a seguire in rete un cammino fissato a priori indipendentemente dalle indicazioni fornite dal tradizionale instradamento IP (Traffic engineering).

Lezione 44

Qual è il principio di base di SDN

L'idea di base è quella di disaccoppiare il piano dati e il piano di controllo della rete, spostando tutto il piano di controllo in un'entità centralizzata (detto controller), che mantiene una visione complessiva e consistente della rete e sopra il quale possono essere sviluppate applicazioni di vario tipo. Il piano dati resta invece composto da dispositivi estremamente semplici, senza alcuna intelligenza, che si limitano ad inoltrare I pacchetti secondo quanto indicato dal controller.

Quali sono gli elementi dell'architettura SDN

-Controller: nodo centralizzato responsabile del calcolo delle tabelle di forwarding degli switch (gira in S.O. di rete)

a. **Northbound interface :** interfaccia tra il controller e le varie applicazioni che possono essere implementate (routing, firewall,etc)
b. **Southbound Interface :** interfaccia tra il controller e gli switch, usata dal controller per scrivere le tabelle di forwardigng sugli switch e per richiedere informazioni dagli switch.
c. **Switch :** hardware per il forwarding dei pacchetti, "privato" di ogni intelligenza.

Lezione 45

Quali sono le principali limitazioni di Openflow

Scalabilità e affidabilità : il controller è un single-point of failure e un potenziale collo di bottiglia. partizionare o replicare il controller per scalabilità e affidabilità; uno dei problemi è mantenere la visione della rete consistente - Interoperabilità. Scalabilità e affidabilità : il controller è un single-point of failure e un potenziale bottleneck; partizionare o replicare il controller per scalabilità e affidabilità; uno dei problemi è mantenere la visione della rete consistente - Interoperabilità

Descrivere il processing di un pacchetto in uno Switch Openflow

Uno switch openflow consiste fondamentalmente di tabelle forwarding (flow table) che vengono create dal controllore e configurate tramite openflow. Quando un pacchetto arriva a uno switch, se c'è un match con una delle regole di una delle flow table, il pacchetto viene processato come indicato, contrariamente se non c'è una regola corrispondente, il pacchetto viene inviato al controller. Il controller a questo punto calcola una nuova regola per il pacchetto in esame e aggiorna le flow table degli switch.

Cosa è Openflow

OpenFlow quindi è un protocollo di comunicazione che consente, in una rete SDN, l'accesso al piano di inoltro (forwarding plane) di un dispositivo di rete (switch) attraverso la rete. Uno switch OpenFlow è costituito da una o più tabelle di flusso e una tabella di gruppo, che eseguono ricerche e inoltri di pacchetti, e un canale OpenFlow a un controller esterno. Lo switch comunica con il controller e il controller lo gestisce tramite il protocollo OpenFlow. Il controller può aggiungere, aggiornare ed eliminare voci di flusso. Openflow è un protocollo di comunicazione che permette l'approccio ad un modello standard dell'hardware di forwarding dei pacchetti e che costituisce il nucleo di diversi dispositivi di networking SDN. Lo scopo di OpenFlow è quello di presentare all'esterno un modello di nodo generale e unificato, rendendo gli strati più alti dell'architettura di rete SDN indipendenti dall'implementazione del costruttore e dalle tecnologie impiegate per il forwarding.

Il principio di funzionamento alla base di MPLS

Multiprotocol Label Switching (MPLS) è una tecnologia per reti IP che permette di instradare flussi di traffico multiprotocollo tra nodo di origine e nodo di destinazione tramite l'utilizzo di identificativi (label) tra coppie di router adiacenti e semplici operazioni sulle label stesse -Label-switched Path (LSP) al posto dell'inoltro "tradizionale" (IP) - Possibilità di decidere in maniera esplicita i percorsi, inclusi percorsi di backup - Mappaggio flessibile del traffico dato sui percorsi

Lezione 46

Quali sono le peculiarità di IoT

Le peculiarità dell'IoT è quella di avere sempre più "cose" connesse a persone o "cose" quindi avere sempre più dispositivi connessi in rete che acquisiscono e condividono dati cercando di fornire soluzioni in tempo reale**.** Elemento peculiare della tecnologia IoT, è che ogni oggetto è in grado di scambiare in modo autonomo informazioni con gli oggetti circostanti, modificando anche il proprio comportamento in funzione degli input ricevuti dagli altri oggetti (things) o dall'ambiente.

A quali livello dello stack protocollare IP/TCP prevede nuovi protocolli/tecnologie

Il livello applicazione fornisce servizi al utente. La comunicazione è fornita per mezzo di una connessione logica. Il livello applicazione è l'unico che fornisce servizi agli utenti di Internet, la sua flessibilità consente di aggiungere nuovi protocolli/tecnologie con estrema facilità.

A cosa serve l'Object Abstraction Layer della pila protocollare IoT

IL livello l'Object Abstraction Layer della pila protocollare IoT trasferisce i dati prodotti dall'Objects layer al Service Management layer tramite un canale sicuro, dati possono essere trasferiti con varie tecnologie, quali RFID, 3G, GSM, UMTS, WiFi, Bluetooth Low Energy, infrared, ZigBee, etc . Inoltre, altre funzioni come il cloud computing e I processi di gestione dei dati sono gestiti a questo livello.

Cosa si intende per Wireless Sensor Network

Con il termine WSN si indica una determinata tipologia di rete informatica che, caratterizzata da una architettura distribuita, è realizzata da un insieme di dispositivi elettronici autonomi in grado di prelevare dati dall'ambiente circostante e di comunicare tra loro**.** Reti tipicamente basate su device con risorse e potenza limitate. Consistono di uno o più sensori eterogenei o attuatori.

Cosa sono object ID e indirizzo di un oggetto IoT e in cosa differiscono

Nell'indirizzamento dei device IoT risulta critico differenziare l'object ID e l'indirizzo. L'object ID è riferito al nome del device e può essere non univoco, ad esempio "T1" per un sensore di temperatura, mentre l'indirizzo si riferisce all'indirizzo del device che lo identifica in modo univoco nella rete di comunicazione.

Quali sono I livelli della pila protocollare IoT Five-Layer

Object (sensori fisici che raccolgono e processano le informazioni),
Object Abstraction Layer(trasferiscei dati dall'Object layer al Service Management layer su canale sicuro), ServiceManagement Layer(accoppia un servizio con chi lo richiede sulla base di indirizzi e nome), Application Layer(fornisce i servizi richiesti dagli utenti), Business Layer(gestisce le attività e iservizi dell'IoT).

Cosa serve il Service Management Layer o Middleware della pila protocollare IoT

Il Service Management Layer o Middleware della pila protocollare IoT accoppia un servizio con chi lo richiede sulla base di indirizzi e nome, abilita i programmatori di applicazioni IoT a lavorare con oggetti eterogenei senza dover considerare la specifica piattaforma hardware. I processi ricevono I dati, prendono decisioni e consegnano il servizio richiesto usando I protocolli standard della rete cablata.

Lezione 47

Elencare e descrivere almeno tre delle principali sfide del mondo IoT

Mobilità - La mobilità è una sfida chiave nell'IoT dato che la maggior parte dei servizi devono essere forniti a utenti mobili Connettere gli utenti mobili con I servizi richiesti senza interruzioni L'interruzione del servizio può avvenire quando l'utente passa da un gateway a un altro (handoff).
Prestazioni - La prestazioni dell'IoT risultano particolarmente critiche essendo legate alle prestazioni di un numero elevato di componenti eterogenei e delle tecnologie sottostanti Esistono diverse metriche per le prestazioni nell'IoT, quali velocità di processing, velocità delle comunicazioni, costi, etc.
Gestione - La connessioni di milioni (addirittura miliardi) di device pone seri problemi in termini di gestione dei guasti, configurazione, fatturazione, prestazioni e sicurezza (Fault, Configuration, Accounting, Performance and Security - FCAPS). Necessità di sviluppare nuovi protocolli di gestione "snelli"per gestire in maniera efficiente potenziali problemi legati al deployment su larga scala dell'IoT.

Cosa sono object ID e indirizzo di un oggetto IoT e in cosa differiscono

Nell'indirizzamento dei device IoT risulta critico differenziare l'object ID e l'indirizzo. L'object ID è riferito al nome del device e può essere non univoco, ad esempio "T1" per un sensore di temperatura, mentre l'indirizzo si riferisce all'indirizzo del device che lo identifica in modo univoco nella rete di comunicazione.

A cosa serve l'elemento "communication" in IoT
Facciamo Esempi delle possibili Tecnologie

L'elemento Comunication interconnette device eterogeni. Tipicamente, i nodi loT operano utilizzando poca potenza e in presenza di canali rumorosi e con perdite. Esempi di protocolli di comunicazione per l'IoT sonoWiFi, Bluetooth, IEEE 802.15.4, Z-wave, eLTE-Advanced.

- **a.** WiFi usa le onde radio per scambiare dati tra device nel raggio di 100m e permette agli smart device di comunicare in modalità ad-hoc
- **b.** Bluetooth usato per scambiare dati con onde corte su basse distanze, per risparmiare energia
- **c.** LTE (Long-Term Evolution) è originariamente uno standard wireless per le comunicazioni ad alta velocità tra telefoni cellulari bacato sulla rete GSM/UMTS

Communication. Esistono anche tecnologie specifiche, quali RFID, Near Field Communication (NFC) e ultra-wide bandwidth (UWB)

A cosa serve l' Object Abstraction Layer della pila protocollare IoT

OAL serve a trasferire i dati dall'Object layer al Service Management layer su canale sicuro. I dati possono essere trasferiti con varie tecnologie, quali RFID, 3G, WIFI, Bluetooh Low Energy ecc. A questo livello sono gestiti il Cloud computing e i processi di gestione dati.

Quali sono I principali elementi dell'architettura IoT

- **Identification :** si occupa del naming e di far corrispondere i servizi alle richieste;
- **Sensing :** raccoglie dati dagli oggetti nella rete e li invia ad un database nel cloud
- **Communication :** interconnette device eterogenei in presenza anche di canali rumorosi e con perdite.
- **Computation :** Processing units, applicazioni sw e Cloud rappresentano il cervello e la capacità computazionale dell'IoT
- **Services :**

- Servizi di Identify-related sono i servizi di base e più importanti,
- Servizi Information Aggregation raccolgono i dati dai sensori che devono essere processati ed inviati alle applicazioni IoT
- Servizi Collaborative-Aware usano i dati rilevati per prendere decisioni e reagire di conseguenza,
- Servizi Ubiquitous Services forniscono i servizi Colaborative-Aware in ogni momento e siano necessari

- **Semantics :**

Abilità di estrarre informazioni da diversi device e fornire servizi richiesti - rappresenta il cervello della IoT che smista le richieste alla risorsa corretta - requisito supportato da tecnologie di Semantic Web come RDF (resource description Framework) e OWL Ontology Web Language - il W3C ha adottato il formato EXI (Efficient XML Interchange)

A cosa serve il Service Management Layer o Middleware della pila protocollare IoT

Il SML accoppia un servizio con chi lo richiede sulla base di indirizzi e nome. Abilita i programmatori di applicazioni di IoT a lavorare con oggetti eterogenei senza dover considerare la specifica piattaforma hw. I processi ricevono i dati, prendono decisioni e consegnano il servizio richiesto usando i protocolli standard di rete.

A cosa serve la Base Station in una Rete Wireless

Normalmente connessa a una rete cablata, (relay) è responsabile dell'inoltro dei pacchetti tra la rete cablata e gli host wireless nella sua "area". I terminali mobili non comunicano mai direttamente ma sempre tramite un stazione fissa (Base station, BS) di riferimento. La struttura delle reti cellulari prevede un punto di accesso fisso BS per ogni cella ed ogni cellulare utilizza la BS della cella in cui al momento risiede

A cosa serve la stima del RTT nel TCP e come viene effettuata

La stima del RTT serve al trasmettitore di stimare il tempo dopo il quale un pacchetto può essere considerato perso perché non ha ricevuto l'ACK.

Questo tempo non può essere troppo piccolo per evitare ritrasmissioni non necessarie ma neanche troppo grande perché varia. La stima è effettuata facendo una media mobile esponenziale ponderata partendo dal tempo misurato dalla trasmissione del segmento fino alla ricezione di ACK.

A cosa serve la fase di Registrazione nella Mobilità

A rendere visibile il device mobile al foreign agent e a segnalare la sua posizione all'home agent

Lezione 48

Cosa è l'Autenticazione

L'autenticazione si riferisce all'atto di stabilire o confermare che qualcosa (o qualcuno) sia autentico, cioè che le affermazioni fatte a proposito di qualcosa siano corrette. Per garantire l'autenticità delle informazioni esistono diversi meccanismi: firma, sigilli, impronta digitale (artefatto difficile da riprodurre), un segreto condiviso come una frase segreta nascosta all'interno di un msg, una firma digitale.

a. Diversi meccanismi possono garantire l'autenticità delle informazioni:
b. Un artefatto difficile da riprodurre, come una firma, un sigillo, un water mark o un'impronta digitale
c. Un segreto condiviso, come una frase segreta, immersa all'interno di un messaggio
d. Una firma digitale

Cosa si intende per non ripudiabilità

La non ripudiabilità si riferisce al concetto di assicurarsi che una parte in una disputa non possano ripudiare o rifiutare la validità di una affermazione o di un contratto

• Il metodo più comune per garantire la non ripudiabilità dell'origine dei dati è la firma digitale

• Per garantire la completa non ripudiabilità è però necessario ricorrere a una trusted third party (arbitro)

Cosa si intende per non ripudiabilità

La non ripudiabilità si riferisce al concetto di assicurarsi che una parte in una disputa non possano ripudiare o rifiutare la validità di una affermazione o di un contratto. Il metodo più comune per garantire la non ripudiabilità dell'origine dei dati è la firma digitale. Una trusted third party (arbitro) garantisce la completa non ripudiabilità.

Cosa si intende per problema del nodo nascosto

Il problema del terminale nascosto, nelle reti wireless, si verifica quando un nodo è visibile da un Access Point (AP) wireless, ma non da altri nodi che possono vedere lo stesso AP. Questo comporta una serie di difficoltà nel controllo di accesso al mezzo.

Come si realizza un VLAN

Una VLAN è una rete LAN realizzata logicamente, isolata quindi virtualmente ma non fisicamente, da altre LAN Virtuali. Una VLAN consente di: -Separare host appartenenti allo stesso dominio di broadcast;-Connettere host separati fisicamente, alla stessa rete logica virtuale. Ci sono due modi per realizzare una VLAN:-Port Based (Private VLAN),lo switch assegna una VLAN a delle porte; -Tagged (802.1Q), lo switch associa un indirizzo IP/MAC ad una VLAN.

Come funziona un CryptoLocker

È un eseguibile che deve essere aperto dall'utente o lanciato tramite falle di sw non aggiornati.

A. Si collega al proprio server e genera due chiavi RSA a 2048 bit(pubblica/privata).
B. Inizia a copiare e criptare con la chiave pubblica documenti, foto e video
C. Cancella file originali, definitivamente e irrecuperabilmente, incluse le copie shadow
D. Il ripristino avviene solamente con la chiave privata, memorizzata sul server e non ottenibile senza pagare il riscatto

Come funziona un CryptoLocker

È un eseguibile che deve essere aperto dall'utente o (in casi più rari) lanciato tramite falle conosciute (es. Flash Player non aggiornato)

- **a.** Si collega al proprio server e genera due chiavi RSA a 2048 bit (pubblica/privata)
- **b.** Inizia a copiare e criptare con la chiave pubblica documenti, foto e video
- **c.** Cancella file originali, definitivamente e irrecuperabilmente, incluse le copie shadow
- **d.** Il ripristino avviene solamente con la chiave privata, memorizzata sul server e non ottenibile senza pagare il riscatto

L'unica soluzione è pagare il riscatto Solitamente in BitCoin o altra cryptovaluta

- **a.** Riscatto non troppo elevato Normalmente l'equivalente di poche centinaia di €
- **b.** Ma attenzione, essere vittima di un ransomware indica che un semplice guasto del disco rigido avrebbe avuto conseguenze anche peggiori
- **c.** Necessità di Prevenire

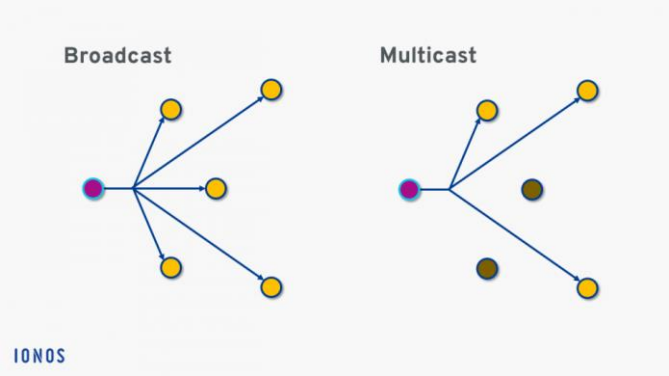
Qual è la differenza tra Virus e Worm

Simile ad un virus ma, a differenza di questo, non necessita di legarsi ad altri eseguibili per diffondersi ma si diffonde spedendosi direttamente agli altri computer, ad esempio tramite e-mail o una rete di computer. Un virus è un software che, una volta eseguito, infetta dei file in modo da fare copie di se stesso, generalmente senza farsi rilevare dall'utente. Un virus può danneggiare direttamente il sw della macchina che lo ospita, indirettamente danni anche all'hw. Un worm è una particolare categoria di malware in grado di auto replicarsi simile ad un virus con la differenza che non necessita di legarsi ad altri eseguibili per diffondersi ma si diffonde spedendosi tramite e-mail o una rete di computer.

Sicurezza Informatica Sicurezza Hacker Ransomware Cyberwarfare

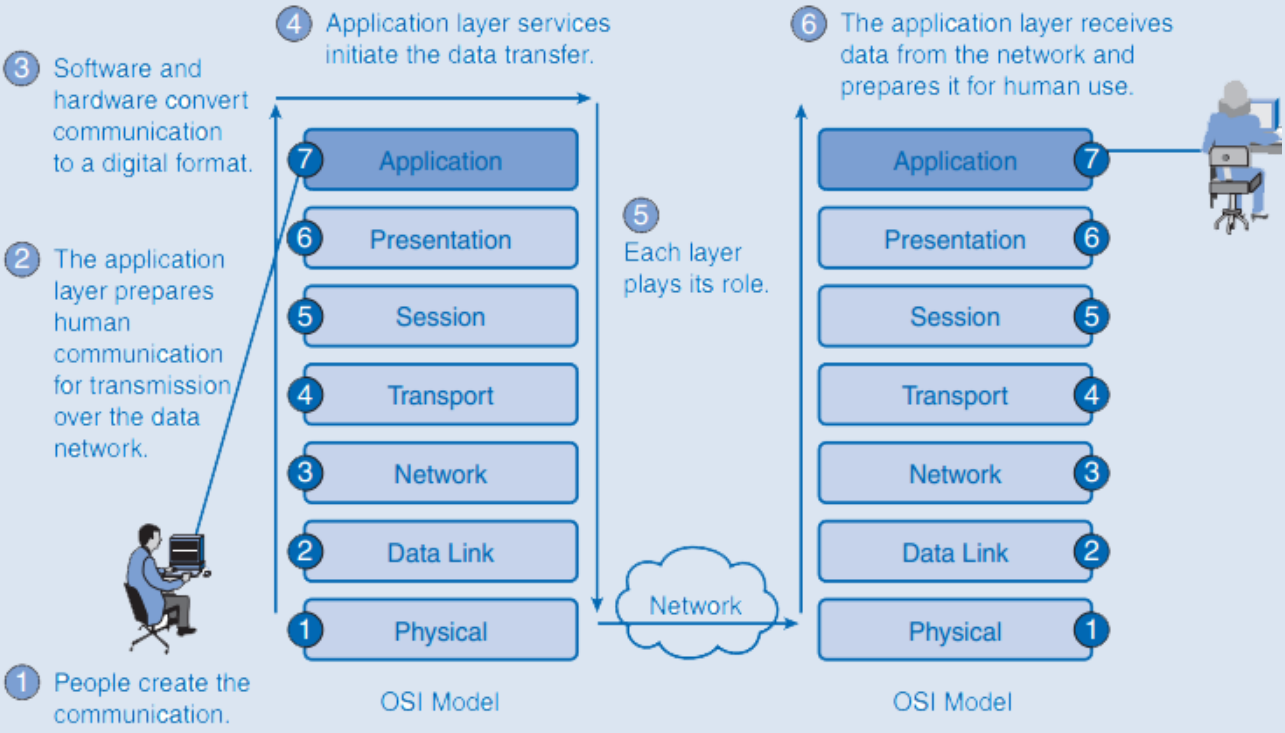
Lezione 49 | RIPASSO

Differenza tra multicast e broadcast in telecomunicazioni

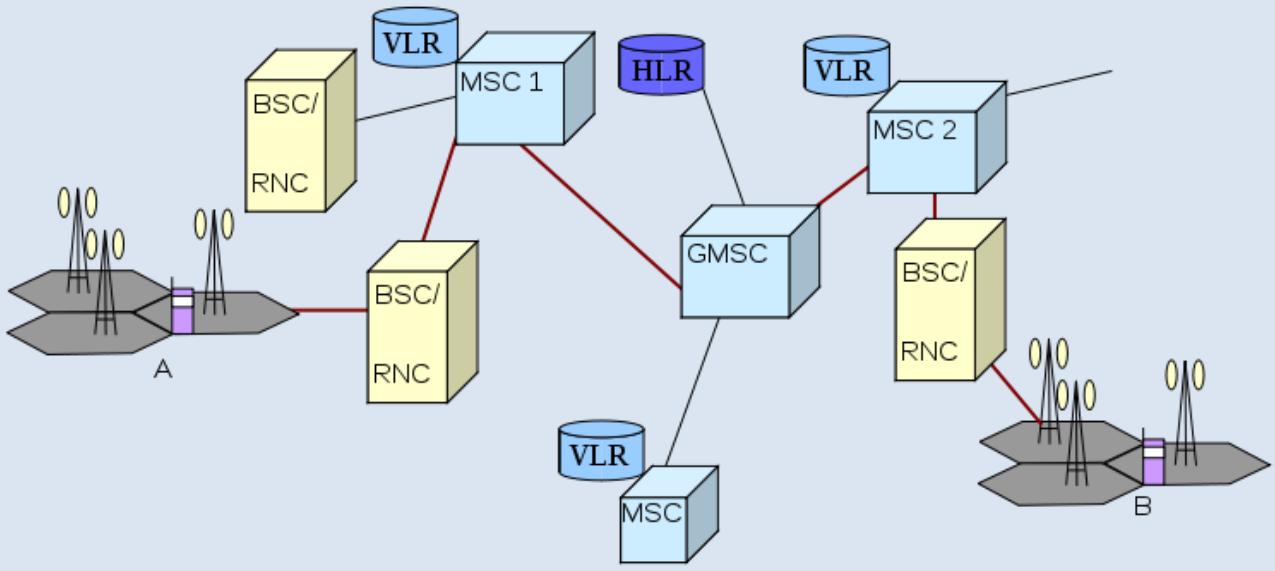


Multicast Il multicast nella rete di computer è la comunicazione tra un singolo mittente e più ricevitori su una rete. Multicast può essere una distribuzione uno-a-molti o molti-a-molti. Il multicast non deve essere confuso con la comunicazione punto-multipunto a livello fisico. In multicast, un gruppo multicast identifica un insieme di destinatari interessati a un particolare flusso di dati ed è rappresentato da un **indirizzo IP** da un intervallo ben definito. I dati inviati a questo indirizzo IP vengono inoltrati a tutti i membri del gruppo multicast. I router tra l'origine e i destinatari duplicano i pacchetti di dati e inoltrano più copie ovunque il percorso verso i destinatari diverga. Le informazioni sull'appartenenza al gruppo vengono utilizzate per calcolare i migliori router in cui duplicare i pacchetti nel flusso di dati per ottimizzare l'uso della rete. Un host sorgente invia dati a un gruppo multicast semplicemente impostando l'indirizzo di destinazione del datagramma come gruppo multicast. Le fonti non devono registrarsi in alcun modo prima di poter iniziare a inviare dati a un gruppo e non richiedono di essere membri del gruppo stesso. **Broadcast** Il broadcast in rete di computer è la comunicazione tra un singolo mittente e tutti gli host collegati alla rete. Nella comunicazione broadcast, la relazione tra origine e destinazione è uno a tutti. C'è solo una fonte, ma tutti gli altri host sono destinazioni. L'indirizzo di destinazione nel pacchetto è l'indirizzo di broadcast speciale e se il pacchetto ha un indirizzo di broadcast, tutti i dispositivi che ricevono quel messaggio lo elaboreranno. Nel broadcast, i router non inoltrano i messaggi di broadcast. Il router riceverà il traffico di broadcast, ma non lo inoltrerà attraverso il router. Flussi di traffico da un singolo punto a tutti i possibili endpoint a portata di mano sulla rete che generalmente è una LAN. Il broadcast non deve essere confusa con **unicast**, un broadcast a un destinatario specifico (come la maggior parte dei messaggi di posta elettronica) o **anycast**, un broadcast al più vicino di un gruppo di router, utilizzata nel protocollo Internet versione 6 (IPv6) come tecnica per la catena -aggiornamento di un gruppo di router con nuove informazioni di instradamento. Il broadcast non è pratica sull'Internet pubblica a causa dell'enorme quantità di dati non necessari che raggiungerebbero continuamente il dispositivo di ciascun utente, delle complicazioni e dell'impatto del rimescolamento e dei relativi problemi di privacy.

Modello OSI Livello Applicazione Rete di Computer Livello Servizio



Dominio UMTS | Applicazioni personalizzate GSM per Reti Mobili



Il protocollo 802.1 Q

Questo protocollo è uno standard che permette a più reti virtuali VLAN di condividere lo stesso collegamento fisico senza perdita di informazioni tra un apparato e un altro.802.1q è il nome del protocollo di incapsulamento utilizzato nel processo di trunking nelle reti Ethernet. 802.1Q non incapsula il frame originale, ma aggiunge 4 byte all'header.

Cosa è una trunk port

Una porta in Trunk è una connessione punto-punto tra due switch e/o un altro apparato di networking (es. Router). I Trunk possono “far passare” più VLAN su un singolo link e permettono alle VLAN di essere raggiunte attraverso l’intera rete.

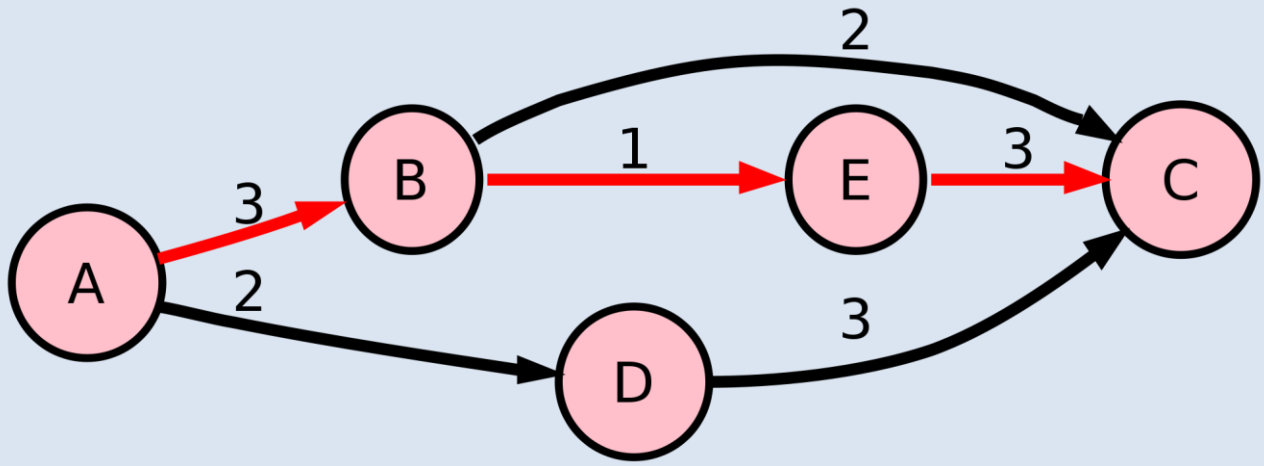
Cosa è OFDM

LTE Radio Access Network utilizza OFDM (Multiplexing a divisione di frequenza ortogonale: una combinazione di multiplexing a divisione di frequenza e di tempo) L’idea base consiste nello scomporre il flusso dei dati da trasmettere in N flussi più lenti che si trasmettono in parallelo mediante un insieme di portanti tali da non avere interferenza mutua tra i flussi in ricezione, grazie alla proprietà di ortogonalità tra le portanti.

Cosa è Openflow

L'idea di base di OpenFlow sfrutta il fatto che la maggior parte dei moderni switch e router contengono flow-table che implementano firewall, NAT, QoS, e raccolgono informazioni a velocità di linea. OpenFlow prevede un protocollo aperto per programmare le flow-table in vari tipi di switch e router. Un amministratore di rete può partizionare il traffico in produzione dai flussi di traffico sperimentali che possono essere controllati scegliendo quali percorsi devono seguire i pacchetti e quale trattamento essi debbano ricevere.

Diagramma Grafico | Metodo del percorso critico



Hub e come funziona

L’hub (ripetitore) è un dispositivo che opera sui singoli bit: -all’arrivo di un bit, l’hub lo riproduce incrementandone l‘energia e lo trasmette attraverso tutte le sue altre interfacce anche se su qualcuna di queste c’è un segnale. -non implementa la rilevazione della portante né CSMA/CD -trasmette in broadcast, e quindi ciascun adattatore può sondare il canale per verificare se è libero e rilevare una collisione mentre trasmette.

Perché per contattare il DHCP non è necessario effettuare l'ARP

Per potersi connettere alla rete ad un device mobile deve essere assegnato un indirizzo IP e conoscere l'indirizzo IP del gateway e del server DNS e per far ciò basta il DHCP. ARP è un protocollo ausiliario di livello rete il cui scopo è ottenere l'indirizzo MAC di una stazione di cui è noto l'indirizzo IP per cui se prima non viene attivato il DHCP, non si può attivare ARP.

Cosa si intende per protocollo di accesso multiplo

Quando l'accesso ad una risorsa può avvenire da parte di più utenti indipendenti, si parla di risorsa condivisa ed è necessaria l'implementazione di particolari protocolli di accesso multiplo. Il protocollo di accesso multiplo è un algoritmo distribuito che specifica come tale condivisione può avvenire, cioè le regole per l'accesso al canale. La necessità di condividere una risorsa può derivare dal costo o dalla scarsa disponibilità di quest'ultima ma anche dalla necessità di ottenere una connettività rappresentata da un mezzo di comunicazione comune.

Descrivere l'handoff nella rete cellulare con MSC diversi

Per non interrompere una chiamata, quando un device mobile si sposta da una cella all'altra in MSC diversi collegati tra loro, il BSC al quale si è collegati invia una richiesta di handoff al proprio MSC la quale viene "girata" all'MSC successivo che controlla la cella di destinazione. Il secondo MSC comanda al proprio BSC di prepararsi ad un handoff, quindi il BSC assegna un canale di traffico al nuovo BTS e risponde al proprio MSC con un HANDOFF REQUEST ACK. MSC contattato invia all'MSC mittente le informazioni relative all'handoff ed al nuovo canale di traffico assegnato dopodichè l'MSC mittente trasmette alla MS i comandi necessari affinché cambi canale

Descrizione dell'handoff nella rete cellulare con lo stesso MSC

Lo scopo di un handoff è quello di instradare la chiamata attraverso una nuova stazione base (senza interruzione). 1.La vecchia BSS comunica all'MSC che sta per essere eseguito un handoff, e fornisce la lista della/e nuova/e BSS cui l'utente mobile sarà associato. 2.MSC inizializza un percorso (alloca risorse) per la nuova BSS. 3.La nuova BSS alloca e attiva un canale radio per la stazione mobile. 4.La nuova BSS trasmette a MSC; vecchia BSS pronta. 5.La vecchia BSS dice al device di eseguire l'handoff verso la nuova BSS. 6.Il device segnala alla nuova BSS di attivare il nuovo canale. 7.Il device segnala il completamento dell'handoff alla nuova BSS, MSC inoltra chiamata. 8.Le risorse allocate vengono rilasciate.

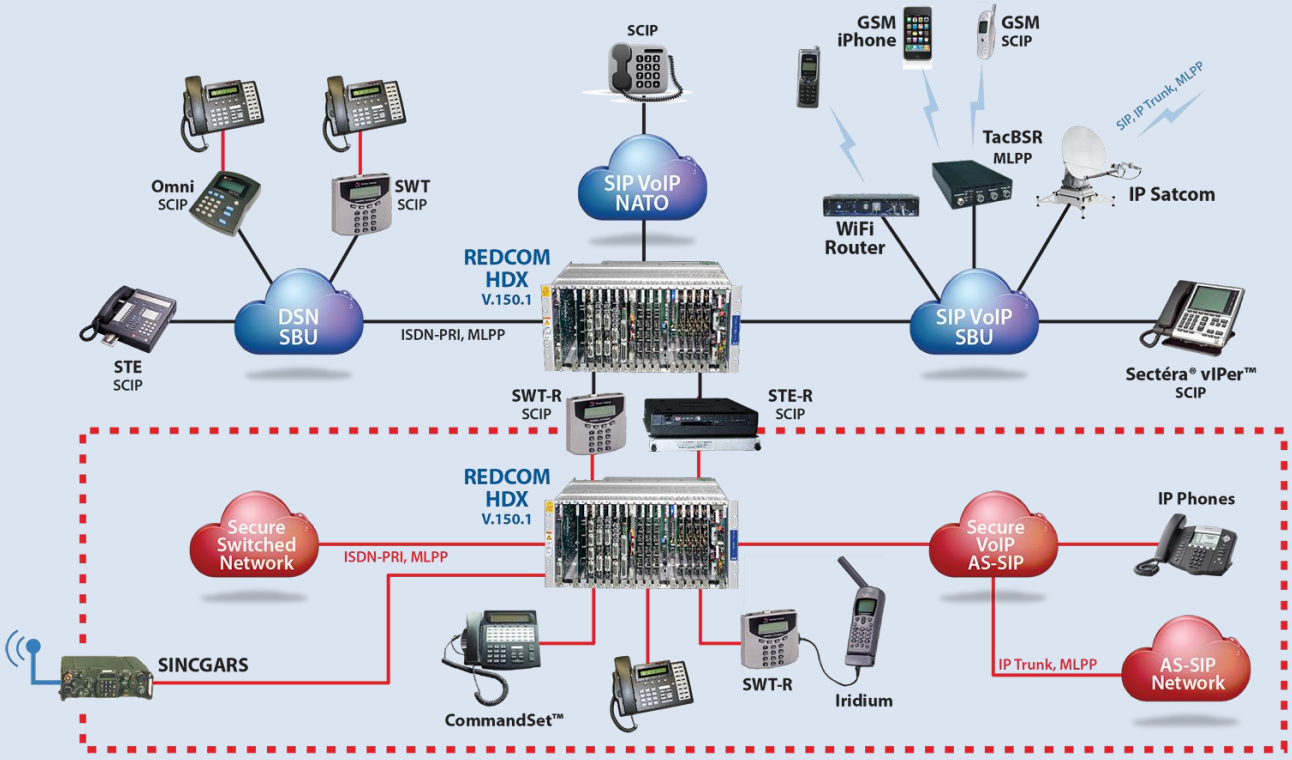
Qual è la differenza tra virus e worm

Un virus è un software che, una volta eseguito, infetta dei file in modo da fare copie di se stesso, generalmente senza farsi rilevare dall'utente. Un virus può danneggiare direttamente il sw della macchina che lo ospita, indirettamente danni anche all'hw. Un worm è una particolare categoria di malware in grado di autoreplicarsi simile ad un virus con la differenza che non necessita di legarsi ad altri eseguibili per diffondersi ma si diffonde spedendosi tramite e-mail o una rete di computer

Differenza tra Forwarding e Routing

Inoltro (forwarding) : trasferisce i pacchetti dall'input di un router all'output del router appropriato. **Instradamento (routing) :** determina il percorso seguito dai pacchetti dall'origine alla destinazione - Algoritmi d'instradamento

Architettura di Rete e Telecomunicazione



Ordinare i protocolli coinvolti nella richiesta di una pagina Web

Per spedire la richiesta http, il client instaura una connessione TCP con il server TCP/IP

Principio di base di SDN

L'idea di base è quella di disaccoppiare il piano dati e il piano di controllo della rete, spostando tutto il piano di controllo in un'entità centralizzata (detto controller), che mantiene una visione complessiva e consistente della rete e sopra il quale possono essere sviluppate applicazioni di vario tipo. Il piano dati resta invece composto da dispositivi estremamente semplici, senza alcuna intelligenza, che si limitano ad inoltrare I pacchetti secondo quanto indicato dal controller

Differenza tra Multiplexing con e senza Threading nei Server Web

La differenza consiste come vengono processati i pacchetti. Nei sistemi senza thread ogni segmento è processato da un processo diverso invece quello con thread c'è un unico processo con diversi thread

Elencare e descrivere almeno tre delle principali sfide del mondo IoT

Le sfide del mondo dell'IoT sono **:**

- **Disponibilità**
- **Affidabilità**
- **Prestazioni**
- **Mobilità**
- **Gestione**
- **Scalabilità**

La Mobilità (è una sfida chiave nel IoT poiché la maggior parte dei servizi devono essere forniti a utenti mobili che devono poter usufruire dei servizi richiesti senza interruzioni | problema interruzione del servizio quando l'utente passa da un gateway a un altro (handoff)).

- **Prestazioni** (risultano particolarmente critiche perché legate ad un numero elevato di componenti eterogenei e tecnologie sottostanti | Esistono diverse metriche per le prestazioni nell'IoT, quali velocità di processing, velocità delle comunicazioni, costi, etc.)
- **Gestione** (gestire le connessioni di milioni di device da problemi nella gestione dei guasti, configurazione, fatturazione, prestazioni e sicurezza | è necessario sviluppare nuovi protocolli di gestione "snelli" per gestire in maniera efficiente potenziali problemi legati al deployment su larga scala dell'IoT)
- **Scalabilità** (riferita alla capacità di aggiungere nuovi device, servizi e funzionalità per gli utenti, senza incidere negativamente su prestazioni e qualità dei servizi esistenti | il gran numero di piattaforme hw e di protocolli di comunicazione rende la scalabilità un aspetto molto critico) La Disponibilità (deve essere fornita sia a livello hw che sw | Servizi disponibili sempre e ovunque | La disponibilità del software nell'IoT si riferisce all'abilità di fornire i servizi a chiunque anche in posti diversi nello stesso momento | La disponibilità hardware si riferisce all'esistenza di device in ogni momento che sono compatibili con le funzionalità e i protocolli dell'IoT)
- **Affidabilità** (si riferisce al funzionamento corretto del sistema sulla base delle sue specifiche | Finalizzata ad aumentare il *rate di successo della consegna* dei servizi IoT e strettamente correlata alla disponibilità, dato che si tratta di fornire informazioni e servizi nel tempo critica quando ci si riferisce a scenari di gestione delle emergenze)

Informazioni che può restituire un server DHCP

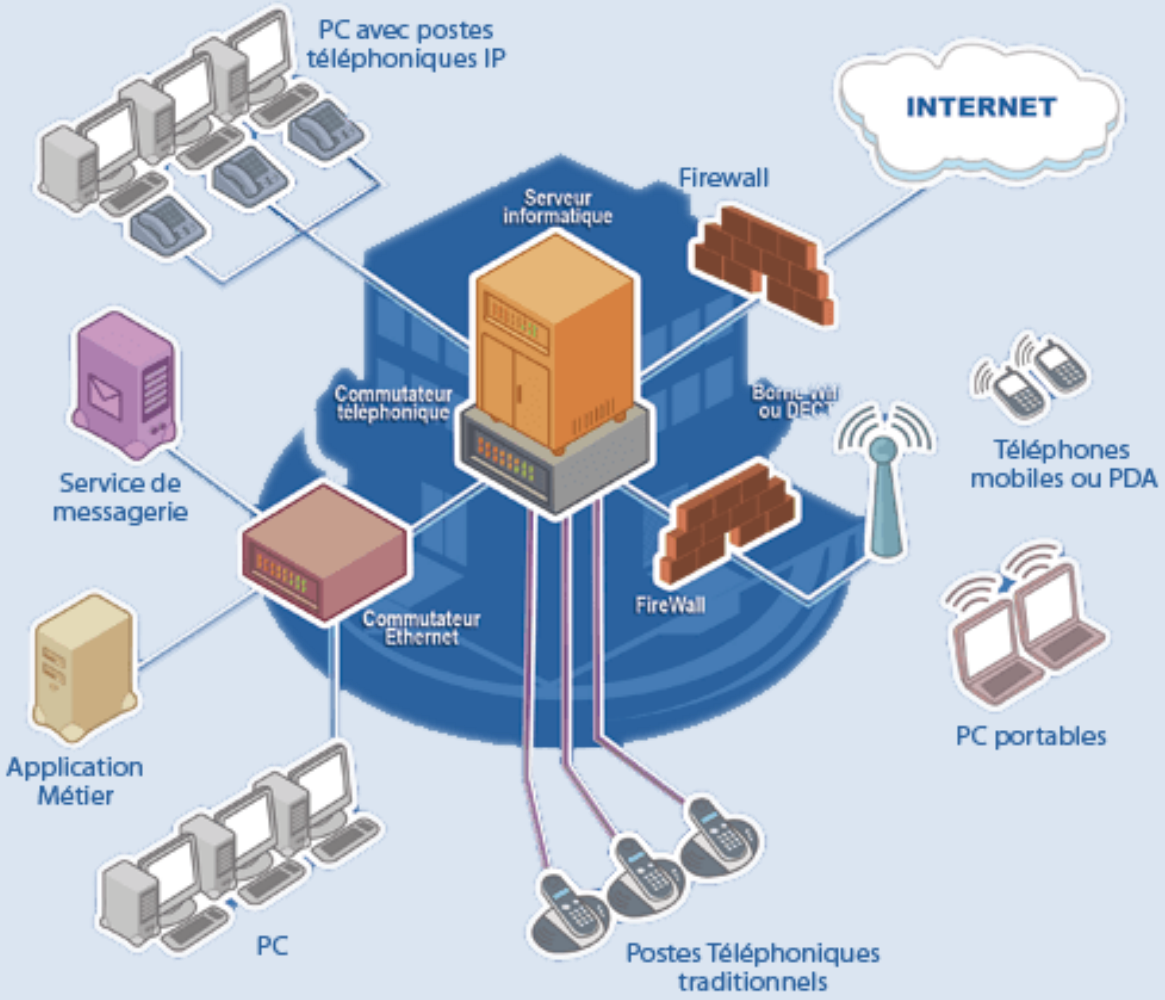
- Indirizzo del primo hop (indirizzo del router da attraversare per raggiungere Internet)
- Nome e indirizzo di un server DNS
- Network Mask
- Indirizzo IP del Gateway (Router LAN)

Principio Base del funzionamento MPLS

Multiprotocol Label Switching (MPLS) è una tecnologia per reti IP che permette di instradare flussi di traffico multiprotocollo tra nodo di origine e nodo di destinazione tramite l'utilizzo di identificativi (label) tra coppie di router adiacenti e semplici operazioni sulle label stesse

- Label-switched Path (LSP) al posto dell'inoltro "tradizionale" (IP)
- Possibilità di decidere in maniera esplicita i percorsi, inclusi percorsi di backup
- Mappaggio flessibile del traffico dato sui percorsi.

| Architettura delle Reti Informatiche |



Vantaggi della stratificazione nei Sistemi

La stratificazione permette la modularizzazione dei processi facilitando la manutenzione e l'aggiornamento di un sistema e quindi modifiche implementative al servizio di uno dei livelli risultano trasparenti al resto del sistema

Differenza principale tra reti cellulari 2/3G e 4G

2G detta anche GSM, è la rete più lenta, la più adatta per chi usa il proprio smartphone solo per chiamate e sms. Con la rete 3G iniziamo a parlare di UMTS : uso veloce della rete internet, oltre all'uso normale di una rete telefonica utile per chiamare o mandare sms. Con il **4G** si definisce lo standard **LTE**, è possibile utilizzare lo smartphone per applicazioni multimediali avanzate e utilizzare collegamenti dati con elevata banda. Nel 4G si ha: una architettura di rete unificata e completamente basata su IP, a differenza delle precedenti reti cellulari, sia dati che voce vengono trasportati in datagrammi IP; una netta separazione tra piano dati e piano di controllo e una netta separazione tra rete di accesso radio e nucleo della rete.

Struttura di un indirizzo IPv4

Gli indirizzi IPv4 sono stringhe di 32 bit lette nella notazione decimale puntata a.b.c.d (con a,b,c,d compresi tra 0 e 255) è composto da **:**

- Versione (4 bit), si tratta della versione del protocollo IP che si utilizza per verificare la validità del datagramma
- Lunghezza dell'intestazione(4 bit), numero di parole di 32 bit costituenti l'intestazione
- Tipo di servizio (8 bit), indica il modo in cui il datagramma deve essere trattato
- Lunghezza totale (16 bit), indica la dimensione totale del datagramma in byte.|
- Identificazione (16 bit), flags (3 bit) e spostamento sezione (13 bit) sono dei campi che permettono la frammentazione dei datagrammi|
- Tempo di vita, detta anche TTL (8bit) si decrementa ad ogni passaggio in un router
- Protocollo di livello superiore o upper layer (8 bit)
- Header Checksum (16 bit) controlla l'integrità dell'intestazione per assicurarsi non sia stata alterata durante la trasmissione| Indirizzo IP sorgente (32 bit) |Indirizzo IP destinazione (32 bit)

Quale protocollo di accesso multiplo utilizza ethernet

CSMA/CD ha il rilevamento della portante differito, come in CSMA **:**

- Rileva la collisione in poco tempo.
- Annulla la trasmissione non appena si accorge che c'è un'altra trasmissione in corso. La rilevazione della collisione è facile nelle LAN cablate (ethernet) e difficile nelle wireless.

I limiti per cui il TCP necessita di nuove varianti per essere utilizzato nelle "Long, Fat Networks"

Un limite per cui sono necessarie nuove varianti del protocollo TCP è perché la crescita della larghezza di banda sta superando la capacità di TCP di gestire il throughput.

Quali informazioni è necessario ottenere appena ci si connette ad una nuova rete per poter navigare in Internet

Nella navigazione internet, per un host appena connesso ad una rete, il primo protocollo utilizzato è DHCP. Il device mobile ha bisogno di ottenere un indirizzo IP e conoscere l'indirizzo del gateway e del DNS: DHCP

Operazioni effettuate dei router MPLS sulle Label

Le operazioni sono denominate Pushing (aggiunge la label "in" iniziale

- **Ingress LSR**/entrata dominio MPLS) Swapping (mappa la label "in" in "out" in ogni LSR) Popping (rimuove la lable "out"
- **Egress LSR**/uscita dominio). Un router che supporta la tecnica MPLS è denominato Label Switching Router (LSR). La LSR esamina la label associata al pacchetto sul link entrante, determina la porta d'uscita accedendo ad una Forwarding Table (FT), sostituisce la vecchia etichetta con la nuova valida sul link d'uscita(label swapping), trasferisce in uscita il pacchetto.

Gli Elementi dell'architettura SDN

- Controller: nodo centralizzato responsabile del calcolo delle tabelle di forwarding degli switch (gira in S.O. di rete)
- Northbound interface: interfaccia tra il controller e le varie applicazioni che possono essere implementate (routing, firewall, etc)
- Southbound Interface: interfaccia tra il controller e gli switch, usata dal controller per scrivere le tabelle di forwarding sugli switch e per richiedere informazioni dagli switch
- Switch: hardware per il forwarding dei pacchetti, "privato" di ogni intelligenza

Elementi di una rete 4G

-eNodeB: discendente logico della base station 2G e del 3G radio network Controller (Node B); -Packet Data Network Gateway (P-GW): assegna indirizzi IP a UE e si occupa della Quality of Service; - Serving Gateway (S-GW): nodo di appoggi della mobilità del piano dati; - Mobility Management Entity (MME): gestisce la mobilità per l'UE residente nella cella che controlla; - Home Subscriber Server (HSS): contiene le informazioni dell'UE

I livelli della pila protocollare IoT SOA based

Object (sensori fisici che raccolgono e processano le informazioni), Object Abstraction Layer (trasferiscei dati dall'Object layer al Service Management layer su canale sicuro), Service Management Layer(accoppia un servizio con chi lo richiede sulla base di indirizzi e nome), Application Layer(fornisce i servizi richiesti dagli utenti), Business Layer(gestisce le attività e i servizi dell'IoT).

I livelli della pila protocollare IoT SOA based

Object (sensori fisici che raccolgono e processano le informazioni), Object Abstraction Layer (trasferiscei dati dall'Object layer al Service Management layer su canale sicuro), Service Management Layer(accoppia un servizio con chi lo richiede sulla base di indirizzi e nome), Application Layer(fornisce i servizi richiesti dagli utenti), Business Layer(gestisce le attività e i servizi dell'IoT).

I principali elementi dell'architettura IoT

- **Identification :** si occupa del naming e di far corrispondere i servizi alle richieste;
- **Sensing :** raccoglie dati dagli oggetti nella rete e li invia ad un database nel cloud
- **Communication :** interconnette device eterogenei in presenza anche di canali rumorosi e con perdite.
- **Computation :** Processing units, applicazioni sw e Cloud rappresentano il cervello e la capacità computazionale dell'IoT
- **Services :** quelli identify-related sono i servizi di base e più importanti, Information **Aggregation** raccolgono i dati dai sensori che poi devono essere processati ed inviati alle applicazioni IoT, Collaborative-Aware usano i dati rilevati per prendere decisioni e reagire di conseguenza, **Ubiquitous** Services forniscono i servizi Coll-Aw in ogni momento e in qualunque luogo sono necessari.

Principali vantaggi di MPLS, rispetto a una rete IP standard

Il rilancio dei pacchetti è notevolmente semplificato e quindi si ottiene un miglioramento delle prestazioni di un router IP; Tabelle di routing molto piccole e look-up molto veloce (il router deve leggere una label, invece di fare longest prefix match degli indirizzi); Virtual Private Network; un insieme di pacchetti può essere forzato a seguire in rete un cammino fissato a priori indipendentemente dalle indicazioni fornite dal tradizionale instradamento IP (Traffic engineering);

Servizi offerti dal livello Link

- **Framing :** I protocolli incapsulano i datagrammi del livello di rete all'interno di un frame a livello di link. Per identificare origine e destinatario vengono utilizzati indirizzi MAC(controlla l'accesso al mezzo).
- **Consegna affidabile :** È considerata non necessaria nei collegamenti che presentano un basso numero di errori sui bit (fibra ottica, cavo coassiale e doppino intrecciato).
- **Controllo di flusso :** Evita che il nodo trasmittente saturi quello ricevente.
- Rilevazione degli errori : Il nodo ricevente individua la presenza di errori grazie all'inserimento di un bit di controllo di errore all'interno del frame.
- **Correzione degli Errori :** Il nodo ricevente determina anche il punto in cui si è verificato l'errore, e lo corregge.
- **Half-duplex e full-duplex**

Quali sono i limiti per cui il TCP necessita di nuove varianti per essere utilizzato nelle 'Long, Fat Networks'

Un limite per cui sono necessarie nuove varianti del protocollo TCP è perché la crescita della larghezza di banda sta superando la capacità di TCP di gestire il throughput.

Quali sono le categorie di protocolli di accesso multiplo

Si possono classificare in una di queste tre categorie :

• Protocolli a suddivisione del canale (channel partitioning) che suddivide un canale in "parti più piccole" (slot di tempo, frequenza, codice).

• Protocolli ad accesso casuale (random access) -I canali non vengono divisi e si può verificare una collisione. -I nodi coinvolti ritrasmettono ripetutamente i pacchetti.

• Protocolli a rotazione ("taking-turn") -Ciascun nodo ha il suo turno di trasmissione, ma i nodi che hanno molto da trasmettere possono avere turni più lunghi.

Quali sono le differenze tra hub e switch

Utilizzare hub è il modo più semplice per interconnettere le LAN, permette di incrementare la distanza tra i nodi. Lo Switch filtra e inoltra i pacchetti Ethernet, esamina l'indirizzo di destinazione e lo invia all'interfaccia corrispondente alla sua destinazione, quando un pacchetto è stato inoltrato nel segmento, usa CSMA/CD per accedere al segmento.

Differenze passive e active scanning nella fase di associazione in 802.11

Quando una stazione che intende inserirsi in rete individua un esistente BSS e vuole accedervi ha bisogno di acquisire la sincronizzazione relativa alle informazioni dall'Access Point. La stazione può acquisire questa informazione nei seguenti modi **:**

- **PASSIVE SCANNING |** La stazione aspetta di ricevere una Beacon Frame dall'AP. La Beacon è una frame periodicamente inviata dall'AP contenente l'informazione relativa al sincronismo di trasmissione dei dati.
- **ACTIVE SCANNING |** La stazione tenta di localizzare un AP attraverso la trasmissione di una Probe Request Frame e attende che un AP risponda con frame Probe Response. Lo Scanning Passivo è praticabile solo quando il numero di canali da indagare è ristretto oppure è breve il Beacon Interval relativo a ciascun canale. Per il resto entrambi i metodi sono validi e la scelta tra uno o l'altro viene effettuata in funzione di esigenze di consumo o di incremento delle prestazioni.

Quali sono le differenze tra switch e router

Entrambi sono dispositivi store-and-forward, i router sono dispositivi a livello di rete mentre gli switch a livello di link. I router mantengono tabelle d'inoltro e implementano algoritmi d'instradamento, gli switch mantengono tabelle di commutazione e implementano il filtraggio e algoritmi di autoapprendimento.

Architetture del Livello Applicazione

Le architetture del livello applicazione sono :

- **Peer to peer (P2P) :** in questo tipo di architettura non c'è un server sempre attivo e coppie arbitrarie di host (**peer**) comunicano direttamente tra loro. Questo tipo di architettura è facilmente scalabile ma difficile a gestire
- **Client Server :** In questo tipo di architettura c'è un server che è host sempre attivo con IP fisso in attesa di essere contattato e che fornisce un servizio e un client che richiede un servizio al server, esso ha un IP dinamico e non può comunicare direttamente con altri client
- Architetture Ibride (Client - Server e P2P).

Indirizzo IP e SubNet Mask

Il segreto sta nell'abbinamento dell'indirizzo IP alla SubNet Mask, ossia nella distinzione di quali siano i Bit che identificano l'indirizzo specifico di un computer, da quali siano i Bit che specificano la rete di appartenenza. Si potrebbe fare l'esempio degli indirizzi postali che identificano miliardi di abitazioni in tutto il mondo: occorre sia precisato sia la "Nazione e Città", (la rete), sia la "via e numero civico", (ossia l'indirizzo). Se si specificasse solo l'indirizzo (ad esempio: via Dante Alighieri, 23) e non si specificasse la città (la rete), sarebbe improbabile che la lettera sia recapitata.
Scriviamo un indirizzo IP, a caso : **192.168.15.3**. Di per sé, questo numero non indica nulla, perché non è univoca quale sia la parte che identifica la rete dalla parte che identifica il computer di quella rete. In un indirizzo IP, composto da 4 byte (di 8 bit ognuno), la SubNet Mask identifica e separa la parte indicante la rete, dalla parte indicante quel computer specifico.

Per esempio :

l'indirizzo IP : 192.168. 15.3

avente SubNet Mask : 255.255.255.0

specifica che ci riferiamo al computer con indirizzo 3, (corrispondente al byte 0 della SubNet Mask), facente parte della rete 192.168.15, (i 3 byte diversi da zero [255] della SubNet Mask).

Indirizzi IP pubblici ed indirizzi IP privati

Gli indirizzi IP si distinguono in indirizzi IP pubblici e in indirizzi IP privati a seconda che appartengano a reti pubbliche o a reti private. Gli indirizzi pubblici sono assegnati da un organismo internazionale, affinché essi siano univoci in tutto il mondo e non vi siano due computer aventi il medesimo numero IP (immaginiamo i numeri telefonici delle reti pubbliche). Gli indirizzi IP privati sono indirizzi che appartengono ad una rete privata creata localmente e che connette computer fra loro (immaginiamo i computer di un ufficio). Questi indirizzi, appartenenti alla medesima rete, possono essere identici anche ad altri indirizzi appartenenti ad altra rete privata, però non vi sarà confusione fra essi, poiché appartengono a reti private diverse (ad esempio: immaginiamo i numeri di interno assegnati agli ingressi degli appartamenti nei palazzi; ogni palazzo avrà i numeri di interno da 1 a 50 (secondo il numero degli alloggi), però ciò non crea confusione con i medesimi numeri di interno che esistono in altri palazzi, poiché trattasi di numerazione privata all'interno del palazzo). Stesso concetto vale per la numerazione con indirizzo IP all'interno di reti private, anche se interconnesse alla rete internet, tramite Gateway con indirizzo pubblico.

Le Classi degli indirizzi IP

Gli indirizzi IP pubblici sono suddivisi in "classi". È una forma di classificazione.

La classe A : ha SubNet Mask **255.0.0.0**, ossia i primi 8 bit. A questa classe appartengono gli indirizzi da: **1.0.0.0 a 127.255.255.255**, quindi in essa si possono avere 127 reti, ognuna delle quali può essere costituita da 16.777.214 computer. Infatti (256 x 256 x 256) – 2 = 16.777.214.

La classe B : ha SubNet Mask : **255.255.0.0**, ossia i primi 16 bit. A questa classe appartengono gli indirizzi da: **128.0.0.0 a 191.255.255.255**, quindi si possono avere: (191-128+1) = 64 x 256 = 16384 reti ognuna composta da (256 x 256) – 2 = 65534 computer.

La classe C : ha SubNet Mask **255.255.255.0**, ossia i primi 24 bit. A questa classe appartengono gli indirizzi da: **192.0.0.0 a 223.255.255.255**, quindi si possono avere (32 x 256 x 256) = 2.097152 reti da (256 – 2) = 254 computer ognuna.

La classe D e la classe E sono utilizzate per usi particolari o futuri. Tramite la NETMASK, le reti A, B, C possono essere ulteriormente suddivise in sotto reti : "SubNetting".

Esempio :
con indirizzo IP : 193.234. 24. oppyre (Indirizzo pubblico di classe C),
con NetMask : 255.255.255.192 si ottengono due sottoreti:

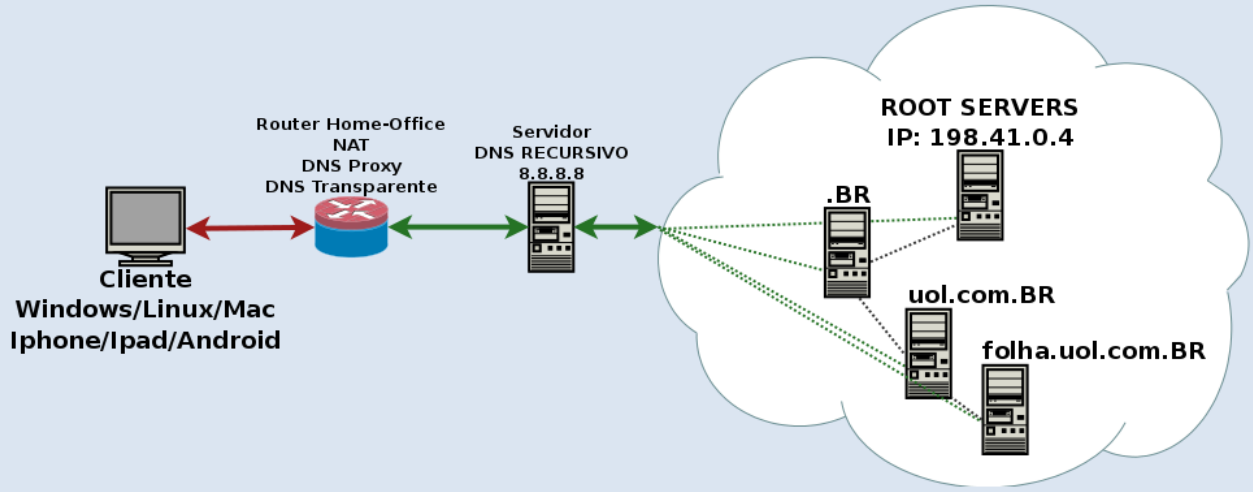
Prima Sottorete composta da 64 Computer :

- indirizzo di rete : 193.234.24.64
- host dal numero : 193.234.24.65 al numero 193.234.24.126
- indirizzo di broadcast : 193.234.24.127

Seconda Sottorete composta da 64 Computer :

- indirizzo di rete : 193.234.24.128
- host dal numero : 193.234.24.129 al numero 192.234.24.190
- indirizzo di broadcast : 193.234.24.191.

Diagramma di sistema Server proxy Rete di computer Server



Indirizzi IP per RETI Private

In ogni classe, una porzione di indirizzi è riservata agli indirizzi IP privati.

Classe A : Indirizzi da : 10.0.0.0 a 10.255.255.255 con **SubnetMask** da 8 bit (i primi 8)
Classe B : Indirizzi da : 172.16.0.0 a 172.16.255.255 con **SubnetMask** da 12 bit
Classe C : Indirizzi da : 192.168.0.0 a 192.168.255.255 con **SubnetMask** da 16 bit

Prendendo ad esempio la classe C, avente la SubNet Mask a: 255.255.0.0, significa che trattandosi di rete privata è possibile creare, secondo le proprie possibilità e esigenze **:**

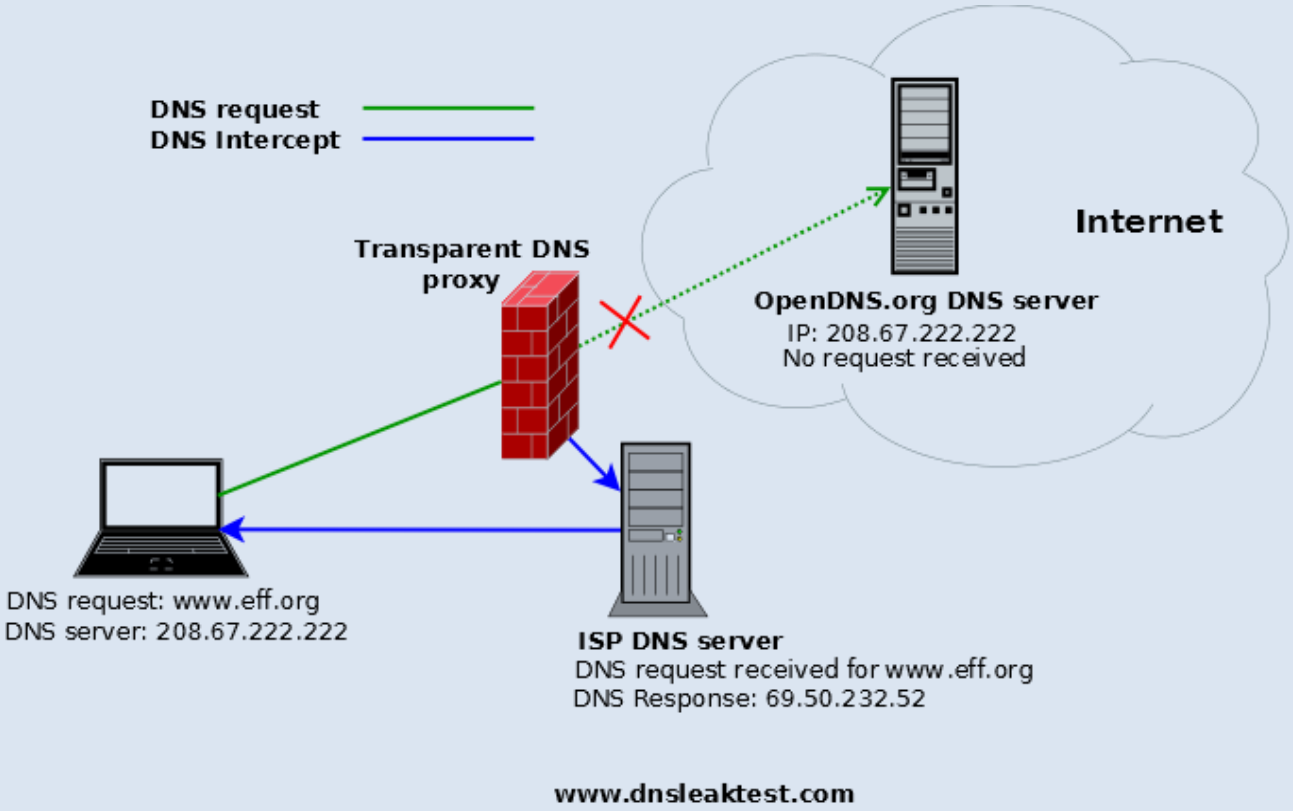
o un'unica rete che connetta (256 x 256) - 2 = 65.534 Computer;
o due reti da (62 x 256) - 2 = 15870 PC Ognuna;
o sei reti da (30 x 256) - 2 = 7678 PC Ognuna;
o 254 reti da 254 computer ognuna (questa è la configurazione classica che si ottiene mettendo il terzo byte a 255 e lasciando a zero il quarto byte della SubNet Mask.

Inoltre, ognuna di queste reti (ad esempio ognuna delle 254 reti da 254 computer) può essere ulteriormente suddivisa e composta da ulteriori sotto reti più piccole, ad esempio:

2 sotto reti da 62 PC ognuna
6 sotto reti da 30 PC ognuna
14 sotto reti da 14 PC ognuna
30 sotto reti da 6 PC ognuna.

Tutto questo viene realizzato attraverso la SubNet Mask

Domain Name System | Server Proxy | OpenVPN | Dns



La SubNet Mask
Come funziona la SubNet Mask

Quando si invia un messaggio ad un altro PC, il nostro computer confronta l'indirizzo IP di destinazione con la propria SubNet Mask ed effettua l'AND logico **:**

1 AND 1 = 1 / 1 AND 0 = 0 / 0 AND 1 = 0

Se il risultato dell'operazione ottiene un numero binario che è identico a quello che si ottiene facendo la medesima operazione con proprio indirizzo IP, allora il computer sa che quell'indirizzo appartiene alla propria rete, cosicché invia normalmente il messaggio. In caso contrario il PC capisce che quello non è un indirizzo della propria rete ed invia il messaggio al computer che fa da gateway verso le altre reti, se questi esiste, altrimenti il messaggio viene perso.

Come si calcola la SubNet Mask.

Un Esempio Classico :
Indirizzo IP : 192.168.0.0
SubNet Mask : 255.255.255.0

Con questa SubNet Mask abbiamo una rete identificata da **:** 192.168.0, alla quale possono appartenere 254 computer: dal numero 1 al numero 254, come per esempio **:**

192.168.0.0 indica l'indirizzo della RETE
192.168.0.1 ; (Primo PC);
192.168.0.2 ; (Secondo PC);
192.168.0.3 : (Terzo PC);

192.168.0.n : (ennesimo PC);

192.168.0.253;
192.168.0.254.

Adesso il numero 255 è riservato al servizio broadcast cioè quello verso tutti i computer.

Mettendo il terzo byte dell'indirizzo di rete a 1, avremo un'altra rete da 254 PC:

192.168.1.0 indica l'indirizzo di questa seconda rete 192.168.1.1 (primo PC)
192.168.1.2 (secondo PC. ecc.)
Ecc. come sopra.
192.168.1.255 indica l'indirizzo di broadcast.

Se non ci interessasse una rete da 254 PC, e preferissimo suddividere ulteriormente quella rete (ad esempio la rete: 192.168.1.x) per avere ad esempio 6 sottoreti da 30 PC, dovremmo calcolare quale valore immettere nel quarto byte della SubNet Mask, che attualmente è a zero.
Poiché dobbiamo mettere a "1" i primi tre bit del byte (che attualmente è a 0), dobbiamo fare: (128 + 64 + 32) = 224,

[in numerazione binaria, 128, 64, 32, 16, 8, 4, 2, 0, sono il valore che ha ogni singolo bit del byte]

. . . quindi la **SubNet Mask** sarà: 255.255.255.224
e questi sono gli indirizzi che daremo ai vari computer di ogni rete **:**

Prima RETE :
Indirizzo di RETE : 192.168.1.32;
Primo PC : 192.168.1.33;
Ennesimo PC : 192.168.1.X; | con X compreso tra 33 e 62 esclusi |
Trentesimo PC : 192.168.1.62;
Indirizzo Broadcast : 192.168.1.63.

Seconda RETE :
Indirizzo di RETE : 192.168.1.64;
Primo PC : 192.168.1.65;
Ennesimo PC : 192.168.1.X; | con X compreso tra 65 e 94 esclusi |
Trentesimo PC : 192.168.1.94;
Indirizzo Broadcast : 192.168.1.95.

Terza RETE :
Indirizzo di RETE :192.168.1.96;
Primo PC : 192.168.1.97;
Ennesimo PC : 192.168.1.X; | con X compreso tra 97 e 126 esclusi |
Trentesimo PC :192.168.1.126;
Indirizzo Broadcast :192.168.1.127.

Quarta RETE :
Indirizzo di RETE :192.168.1.128;
Primo PC :192.168.1.129;
Ennesimo PC : 192.168.1.X; | con X compreso tra 129 e 158 esclusi |
Trentesimo PC :192.168.1.158;
Indirizzo Broadcast :192.168.1.159.

Quinta RETE :
Indirizzo di RETE :192.168.1.160;
Primo PC :192.168.1.161;
Ennesimo PC : 192.168.1.X; | con X compreso tra 161 e 190 esclusi |
Trentesimo PC :192.168.1.190;
Indirizzo Broadcast :192.168.1.191.

Sesta RETE :
Indirizzo di RETE :192.168.1.192;
Primo PC :192.168.1.193;
Ennesimo PC : 192.168.1.X; | con X compreso tra 193 e 222 esclusi |
Trentesimo PC :192.168.1.222;
Indirizzo Broadcast :192.168.1.223.

Conclusione

In questo Tutorial ho cercato di fornirvi molte tra le nozioni necessarie al fine di poter affrontare un percorso formativo verso la Cyber Security. Il risultato di tale lavoro rispecchia il quadro generale delle Reti e Telecomunicazioni dei giorni nostri. Buona Lettura a tutti voi.

… alla prossima