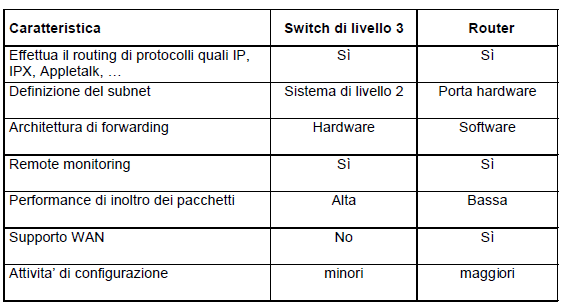
**APPUNTI DI DATA SCIENCE**

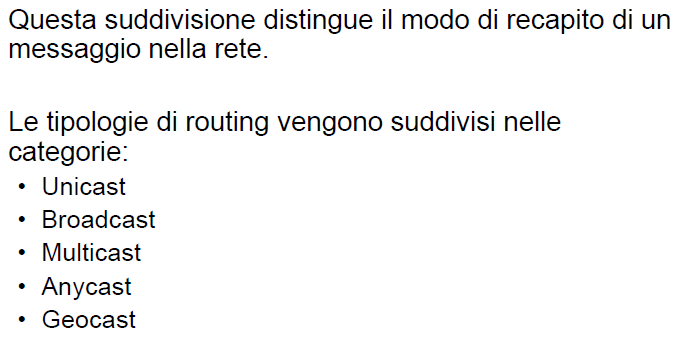
**Router o switch di livello 3**



**Layer 3 protocols**

Protocolli di rete non IP, protocolli di routing

**SCHEMA DI ROUTING: NOZIONI**



Unicast: il messaggio viene recapitato ad un nodo specifico (metodo più usato nelle reti locali e in internet)

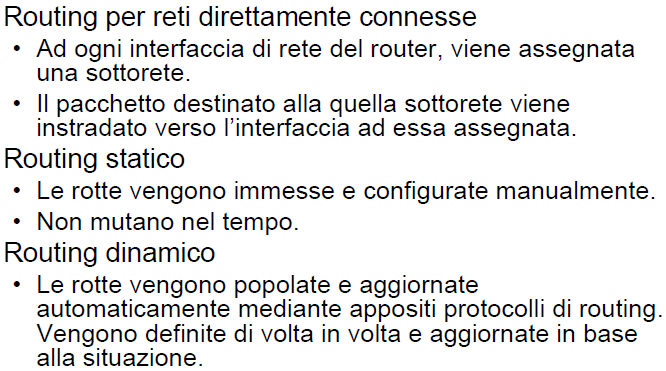
Broadcast: messaggio viene recapitato contemporaneamente a tutti i nodi (ARP, DHCP)

Multicast: relazione 1:molti però i destinatari non sono tutti i nodi. Usa il protocollo IGMP, che gestisce le sottoscrizioni dei nodi destinatari a ricevere i messaggi.

Anycast: rel 1:molti. I destinatari fanno parte di un gruppo, i destinatari del gruppo vengono scelti in base a dei criteri (più vicino, più veloce). Usato dal protocollo BGP, principio usato dalle reti peer-to-peer.

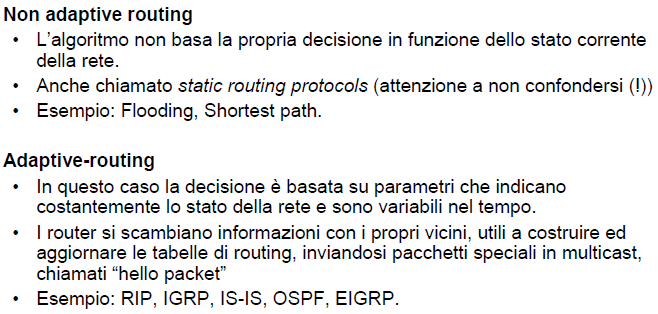
Geocast: il gruppo di nodi destinazione è scelto in base alla loro locazione geografica.

**TIPOLOGIE DI ROUTING**



**PROTOCOLLI DI ROUTING**

Due tipologie di protocolli. Che definiscono le rotte di instradamento.



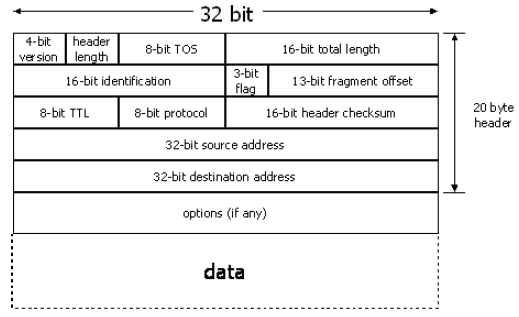
**Non adaptive routing:** il pacchetto in ingresso viene inoltrato su tutte le linee tranne alla sorgente

**Adaptive routing(shortest path): DIJKSTRA** la misura è chiamata metrics ed è data dal numero di hops. Mentre con il RIP (Routing Information Protocol) usa bellman-ford. IGRP basato sul vettore delle distanze. Creato per superare le limitazioni del RIP che poteva avere solo 15 hops al max. mentre questo ne può avere 255. OSPF basato sullo stato del link. Hanno una visione completa della topologia della rete. EIGRP basato sul vettore delle distanze. E’ un ibrido fra distance vector e link state.

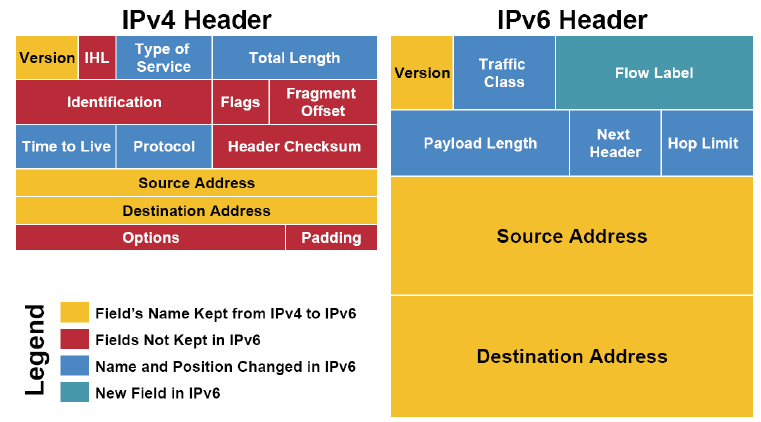
**ADRESSE RESOLUTION PROTOCOL:** fornisce la mappatura tra l’indirizzo IP a 32 bit di un device e il suo MAC addresse (48bit). Tiene traccia delle risposte ottenute in cache. Non prevede meccanismi per autenticare le risposte ricevute. L’host che invia quella richiesta si fida che la risposta arrivi al legittimo proprietario dell’indirizzo IP richiesto.

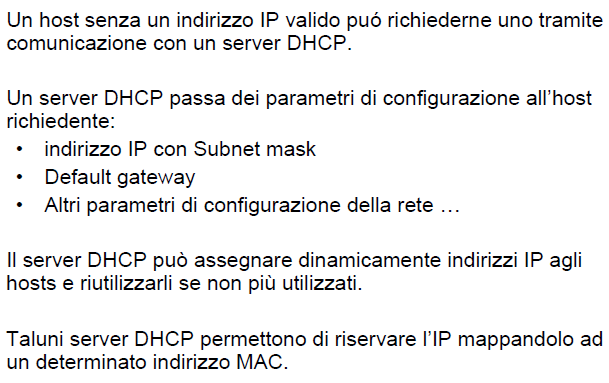
**PROTOCOLLO ICMP:** si preoccupa di trasmettere info di controllo, malfunzionamenti o messaggi fra i vari componenti della rete IP. Incapsulato direttamente in IP, non è quindi garantita la consegna a destinazione dei pacchetti. Usato da Ping e traceroute

**IPV4 STRUTTURA FRAME**



PROTOCOLLO IPV6 VS IPV4



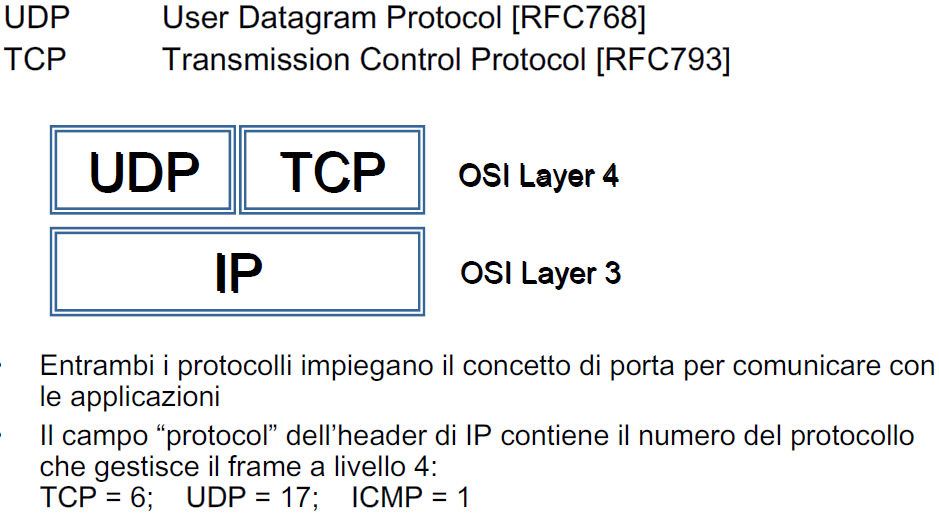
**PROTOCOLLO DHCP:** 

**DHCP** Elimina necessità configurazione manuale, include controlli amministrativi per admin di rete, fornisce stack protocol e parametri di config agli hosts. Plug and play, spostare indirizzi da un ufficio ad un altro e da una rete ad un'altra. Rinumerare, Mobile IP, muovere infrastrutture(portabilità)

**LAYER 4 (Transport)**

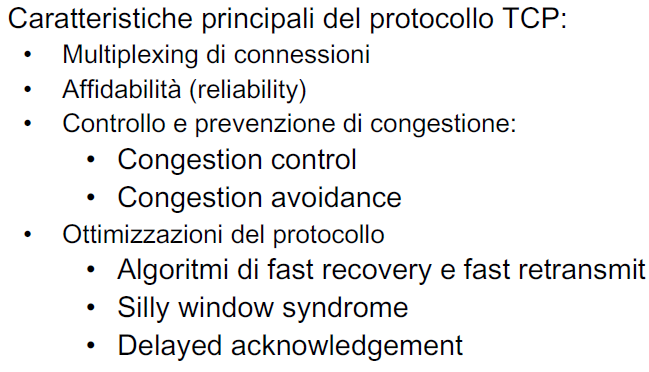
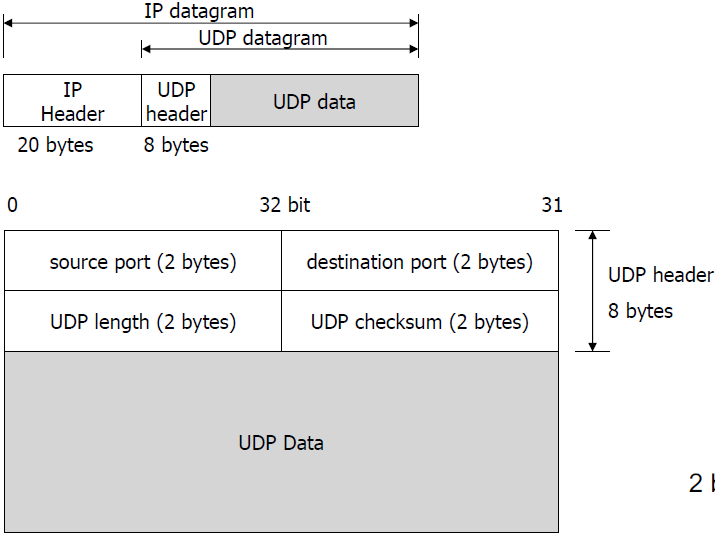
Permette scambio dati tra host utilizzando IP e le porte di comunicazione. Offre diversi servizi tra cui controllo di flusso, garanzia di correttezza dei dati e affidabilità di comunicazione.

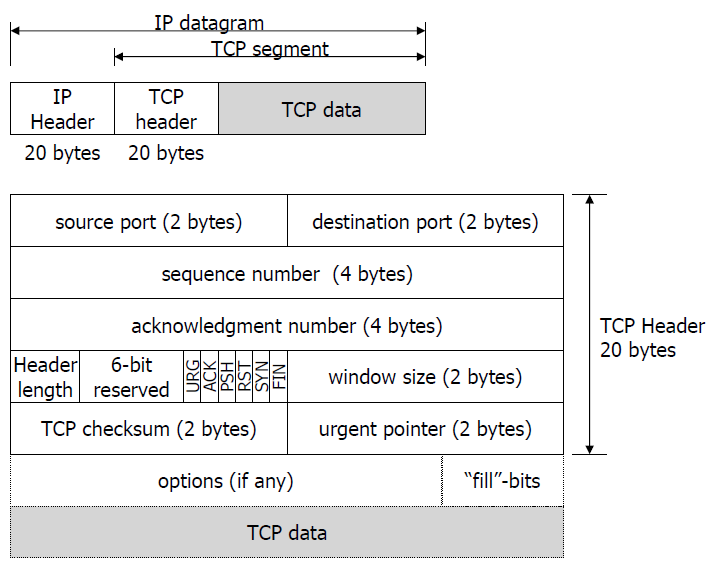
Standard più utilizzati



UDP: offre alle applicazioni accesso diretto al servizio di scambio di datagrammi IP, senza connessione, può esssere usato per broadcast, non affidabile-> lascia le seguenti responsabilità alle applicazioni: controllo ordine dei dati giusto, controllo se i dati sono giunti, controllo se dati sono duplicati controllo se porta aperta e se pacchetto bloccato o rifiutato.

FRAME UDP PROTOCOLLO TCP:



FRAME TCP: 

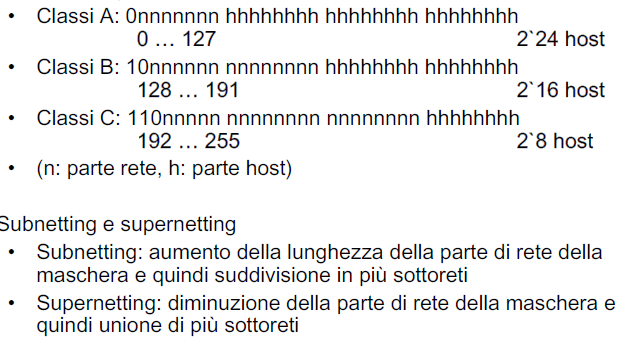
**Repeaters o HUB:** estendono LAN ascoltano segnali elettrici su tutte le porte, rigenerano e ripetono tutti i segnali su tutte le altre porte. Non inoltrano collis.

**Bridges:** segmentano traffico e riducono congestioni, può connettere tipi di lan simili, non usato per avere delle buone performances.

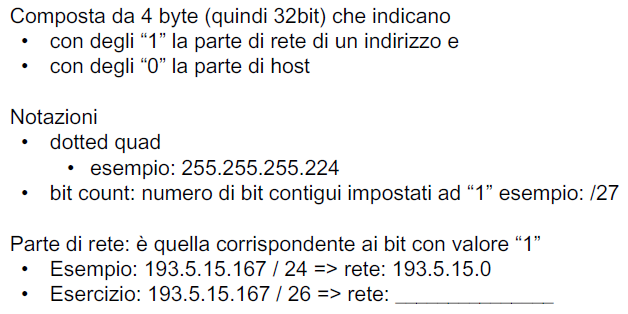
**Switches:** Segmenta traffico, riduce congestioni, può basarsi su frame o celle (ATM), incrementa le performance, low cost e facile da usare, LAN only

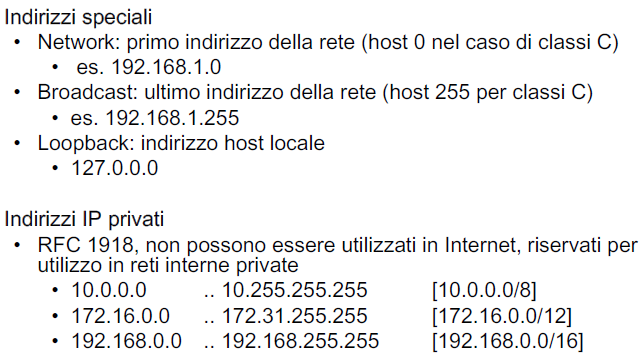
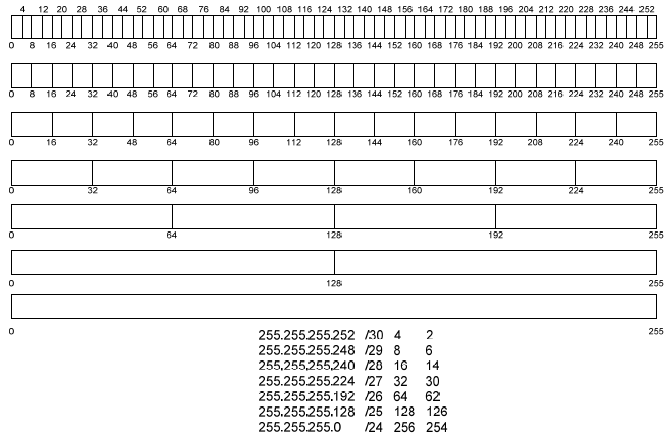
**LIVELLO 3 OSI: CLASSI DI INDIRIZZO IP**

Si usavano maschere di rete implicite a 8, 16, 24 bit

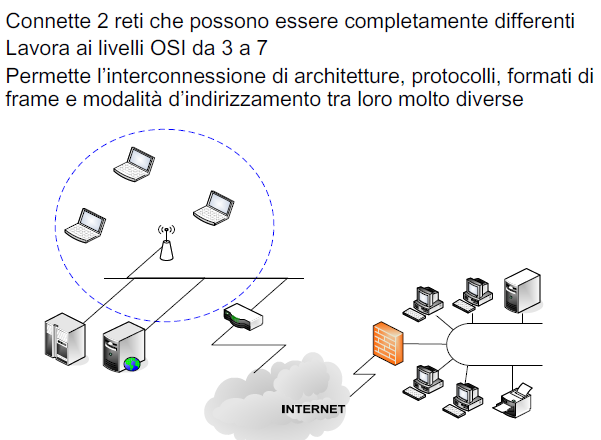


**SUBNET MASK**



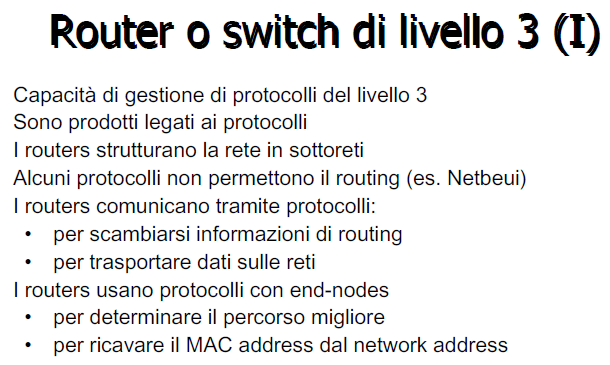
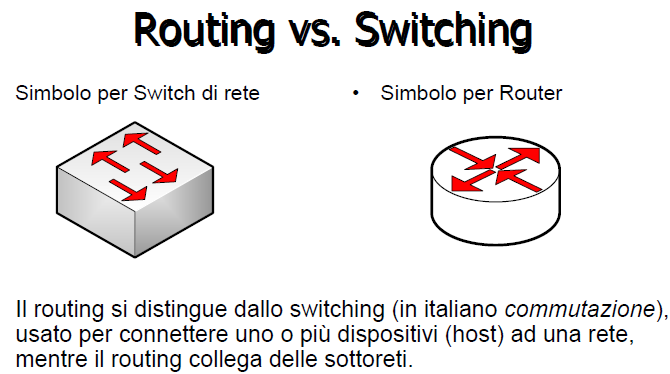


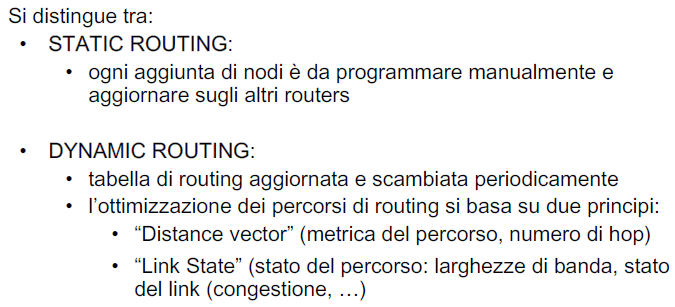
**GATEWAY**



**ROUTING(opera a livello 3 dell’OSI)**

In italiano vuol dire instradamento. L’oggetto da instradare è il pacchetto. Il routing è la decisione di come instradare il pacchetto. Utilizza tabella di instradamento che contiene info che indicano come smistare i pacchetti provenienti da una specifica sottorete.



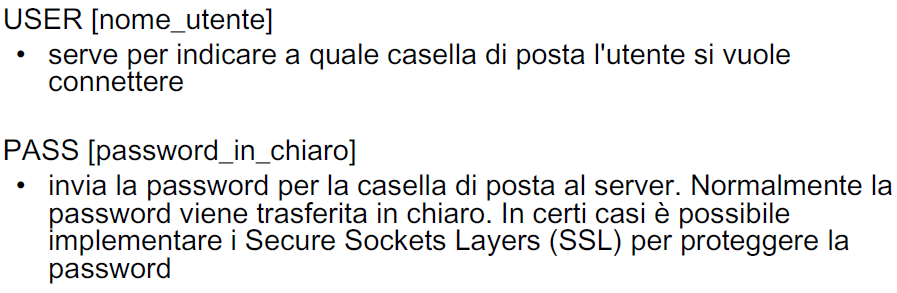
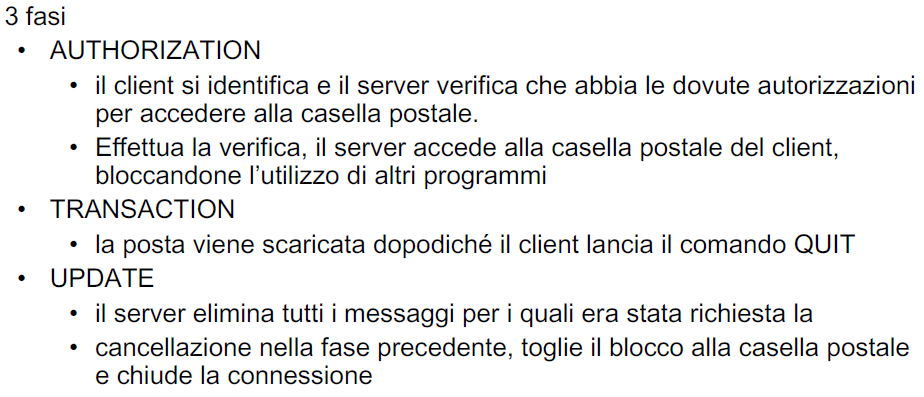


**SMTP**

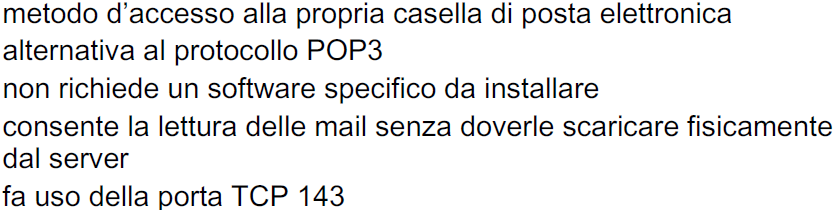
Protocollo utilizzato per trasmettere messaggi di posta elettronica tra due host. Utilizza protocollo di trasporto TCP, e rimane in ascolto sulla porta 25. Il server si occupa di trasferire i messaggi nelle caselle dei destinatari, oppure in caso non fosse il responsabile ai server che dovranno farlo.

**Pop3**

Lettura di e-mail senza collegamenti permanenti utilizza tcp porta 110 messaggi ascii sono leggibili



**Protocollo IMAP**



IMAP rispetto a pop3 ha più caratteristiche e maggiore complessità, permette di modificare mailbox come se fosse locale permette di ottenere singole parti del messaggio(ad es. solo intestazione), ma non tutti gli ISP lo supportano

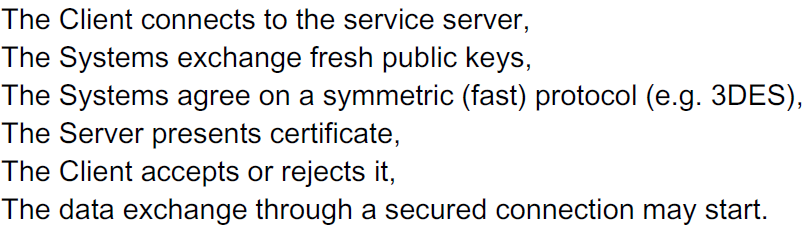
**FASI DI SESSIONE IMAP**

Instaurazione connessione->autorizzazione->transazione(comprende client, dati del server, risultato server(4 stati)->non autenticato, autenticato, selezionato, logout))

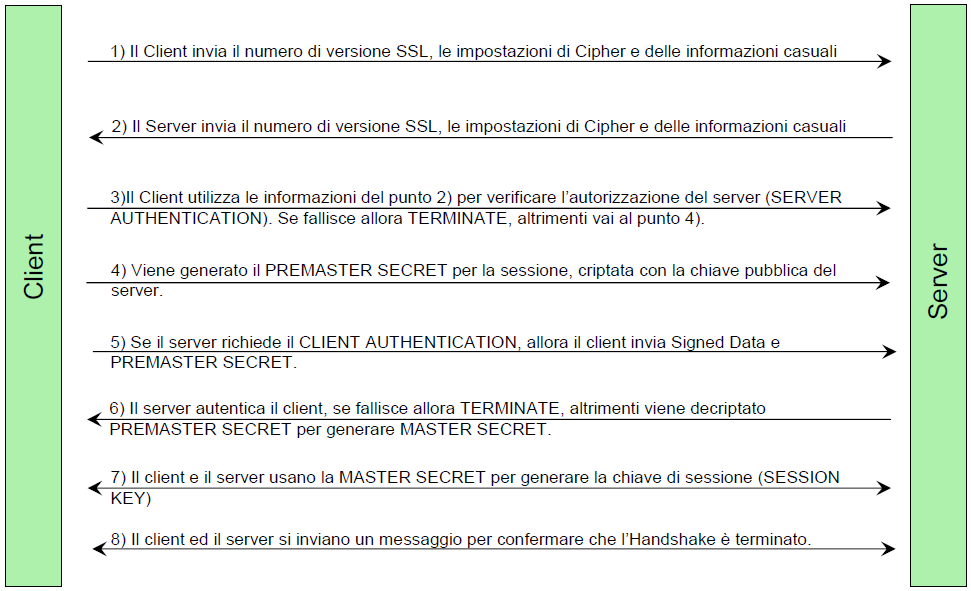
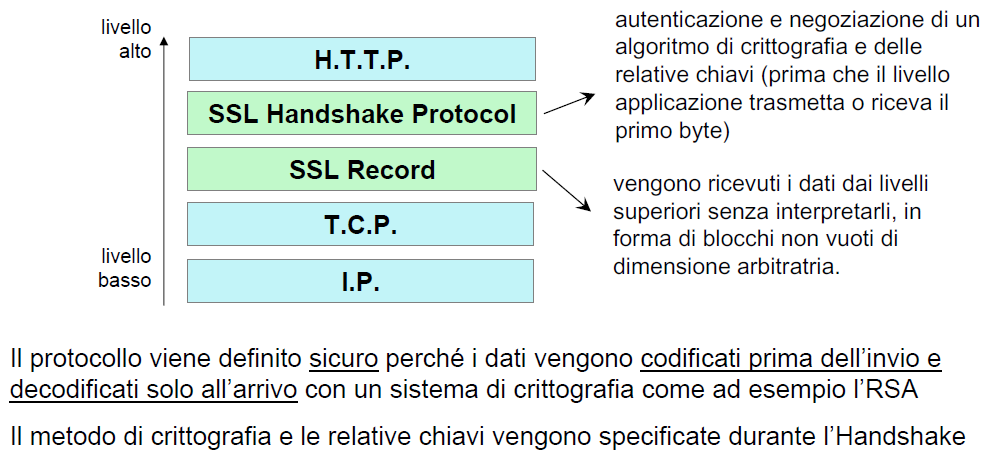
**HTTPS (http+SSL)**

Protocollo che usa porta 443 usa chiave da 40, 56 o 128 bit per algoritmo rc4 non va confuso con shhtp e si può far girare sia il protocollo http che https

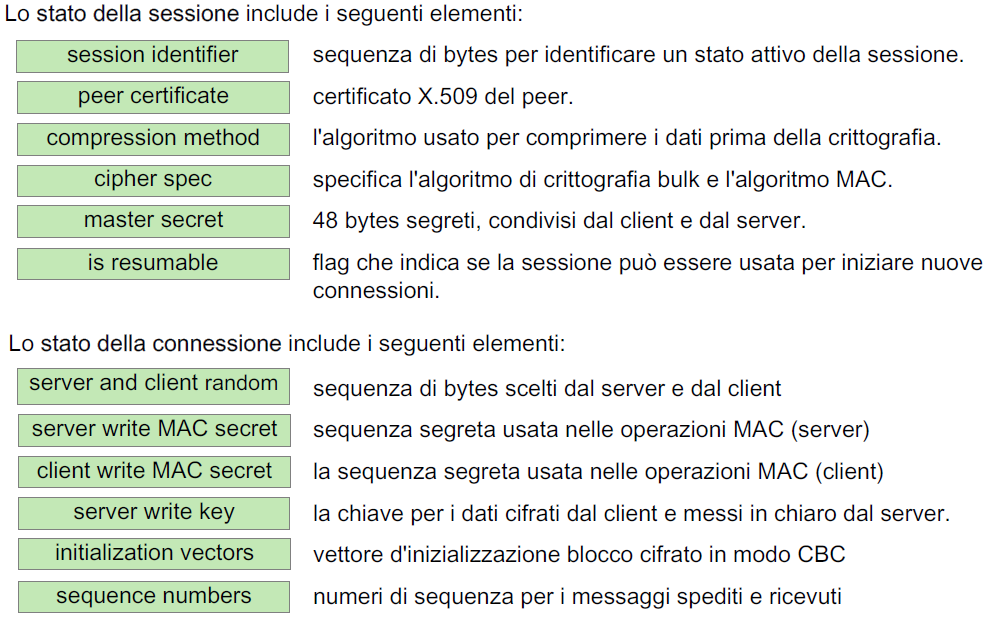
Come funziona?

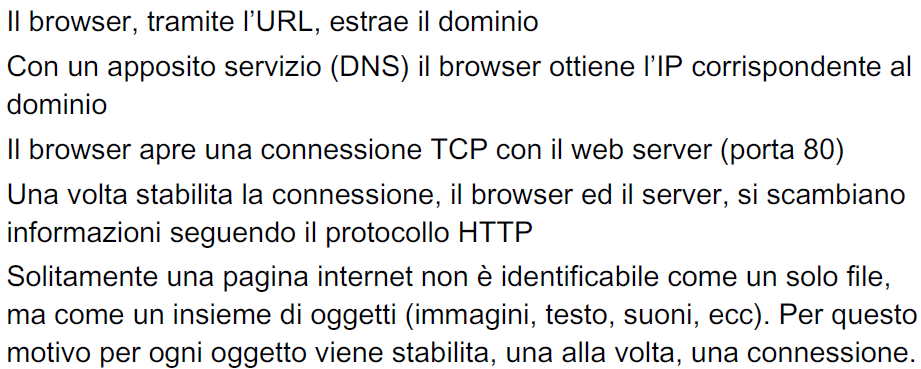


**SSL**

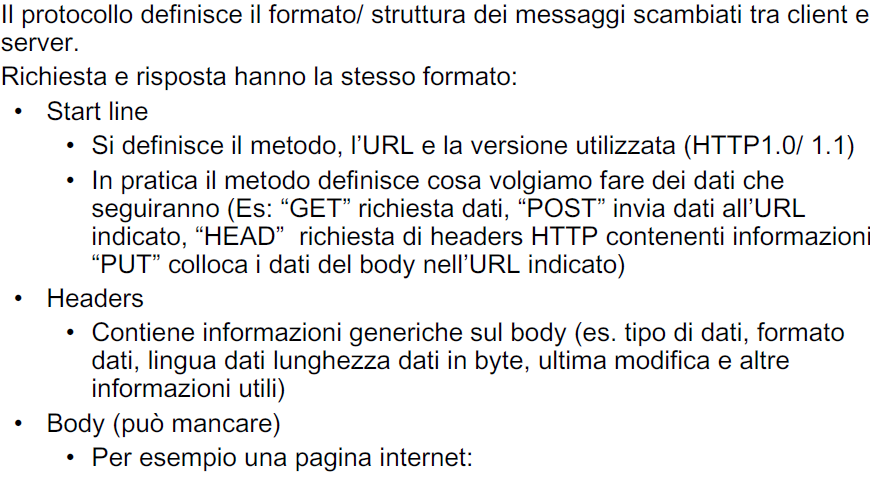
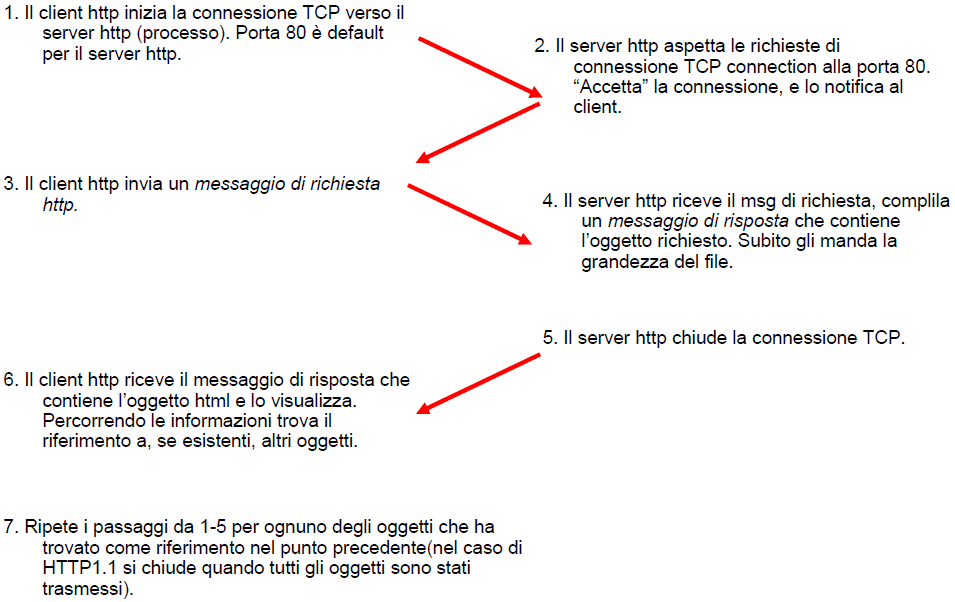
Garantisce riservatezza comunicazione, protezione dei dati crittografia autenticazione e certificati. Protocollo a due strati si basa su TCP IP e si interfaccia con applicazione di livello superiore come http che diventa https. 

STRUTTURA PACCHETTI

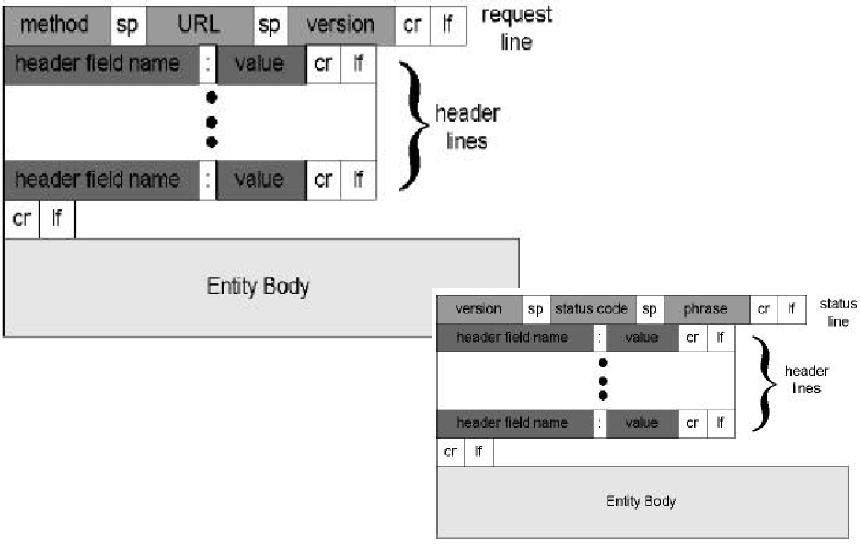




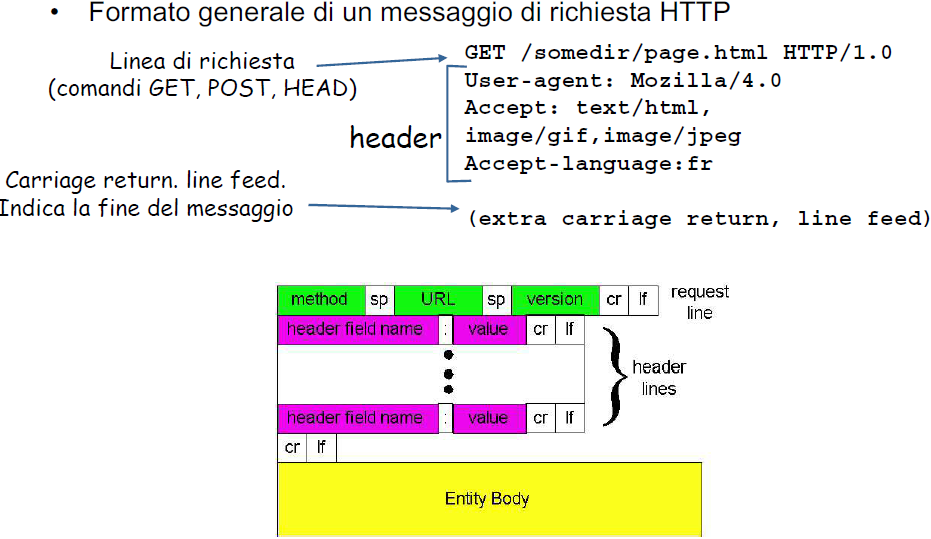
**ESEMPIO COMUNICAZIONE http**



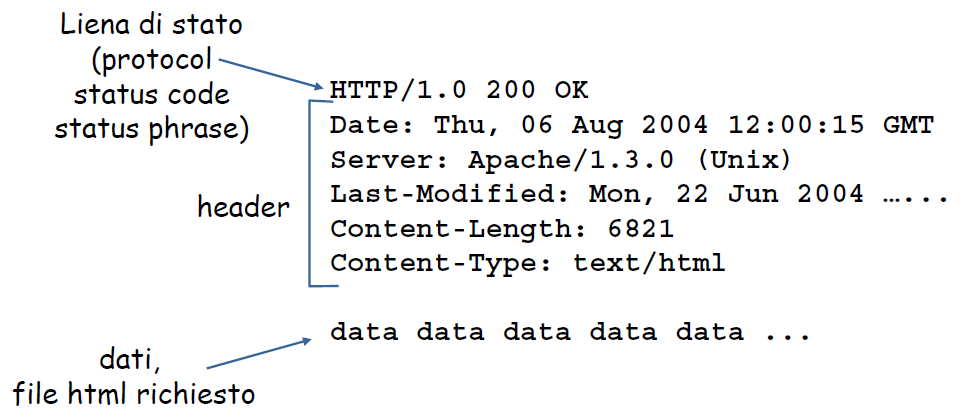
**Messaggio di richiesta e risposta**



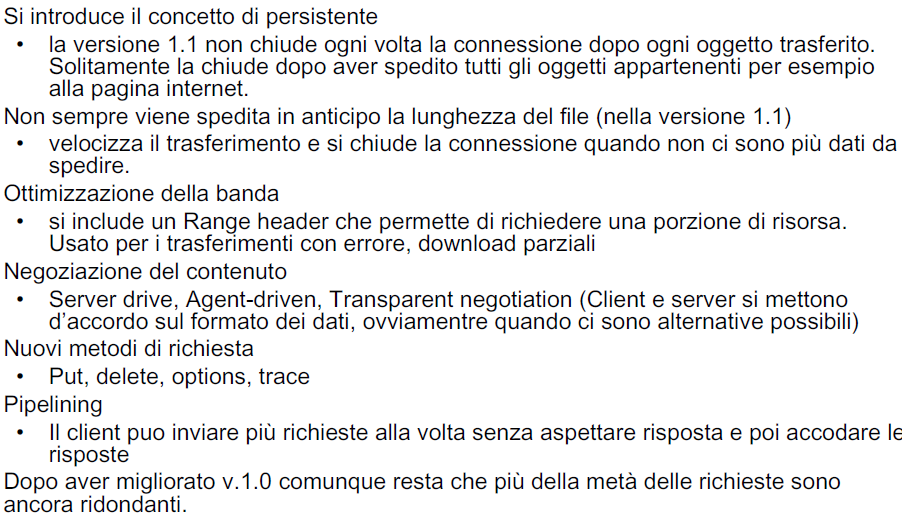
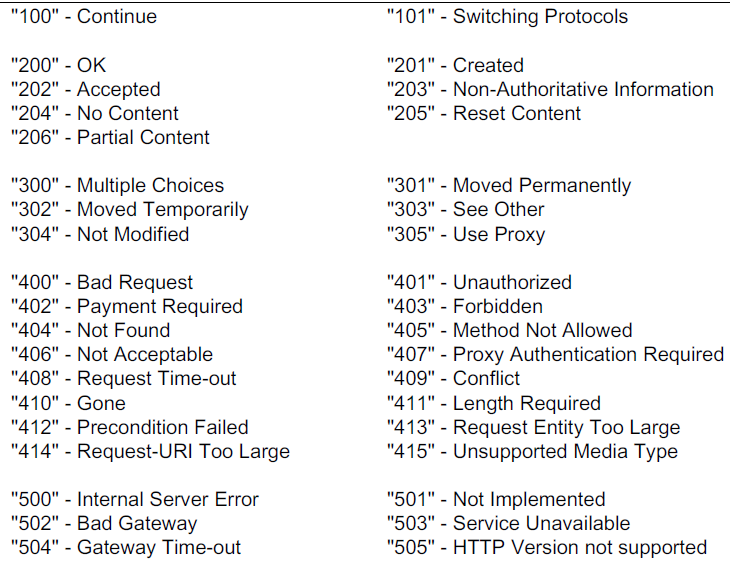
**MESSAGGIO DI RICHIESTA ESEMPIO**



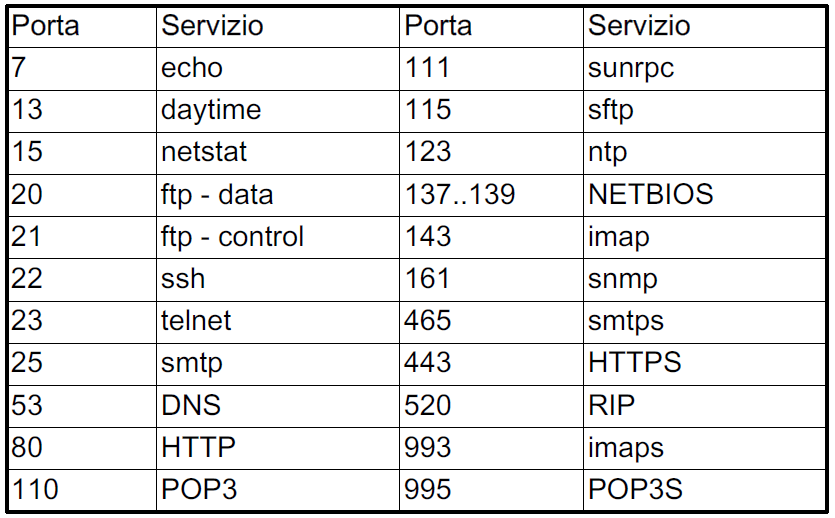
**MESSAGIO DI RIPOSTA http**



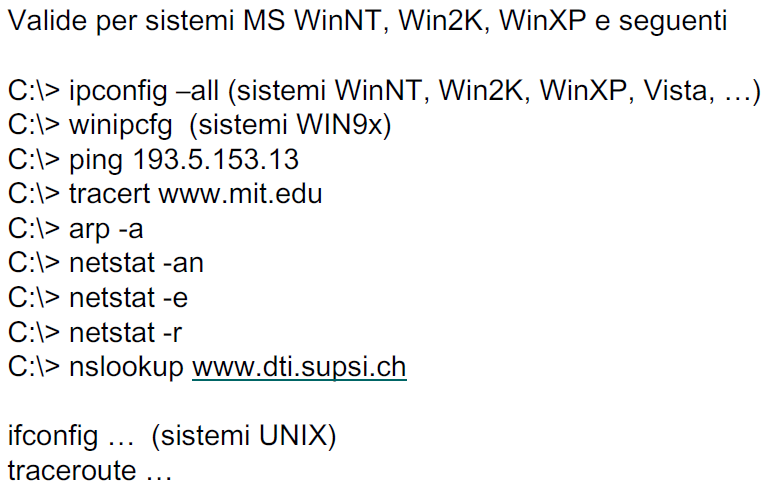
**CODICI DI STATO**



**ELENCO PORTE PIU CONOSCIUTE**

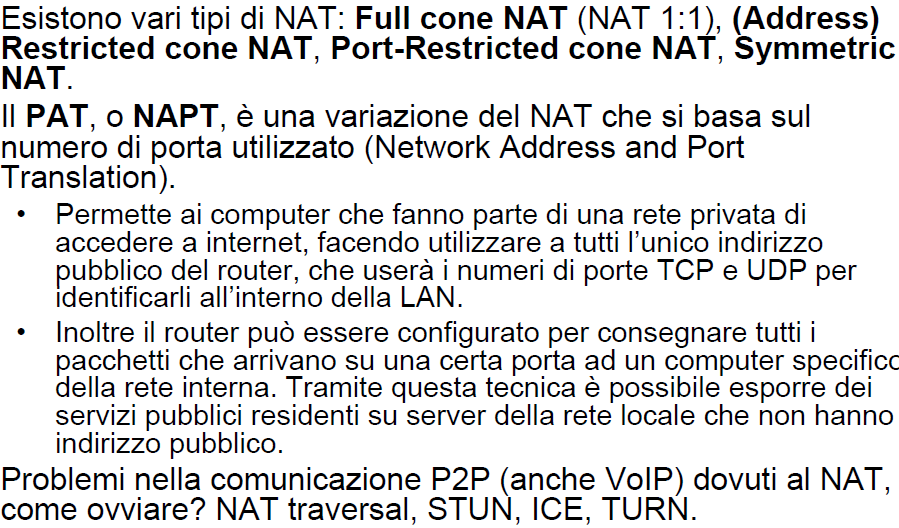
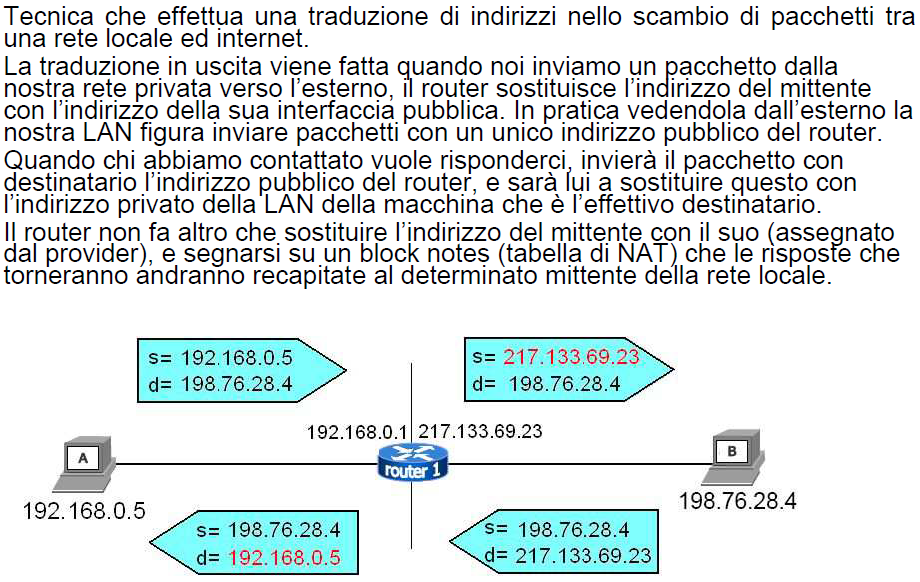


ISTRUZIONI UTILI

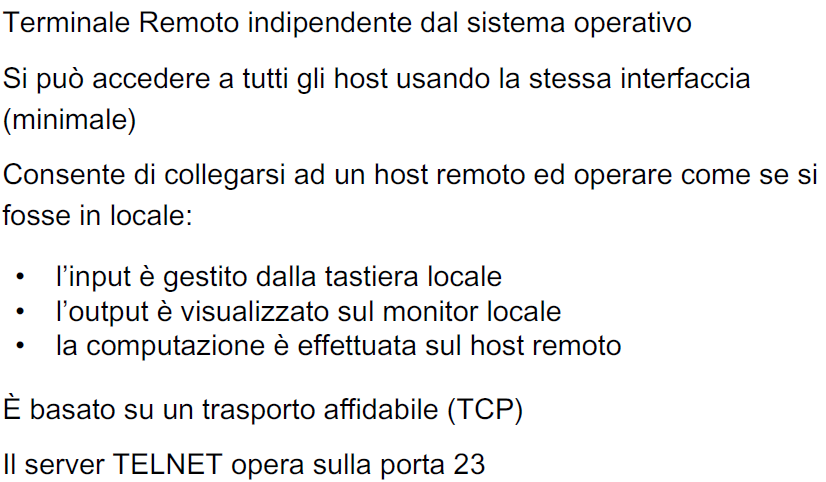


**NAT**

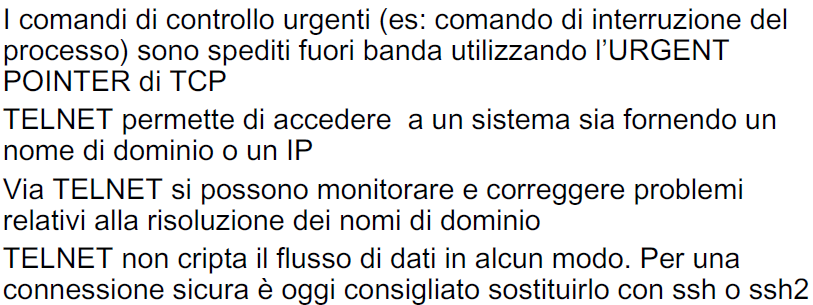
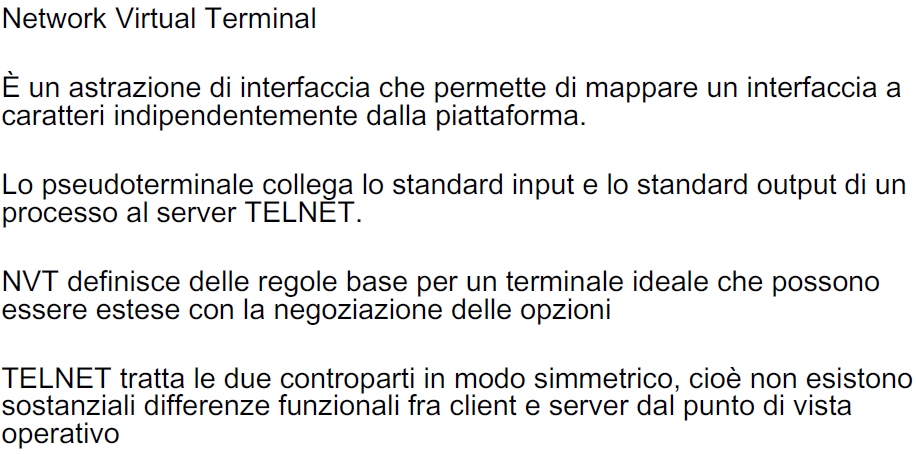
**Tecnica**



**TELNET**



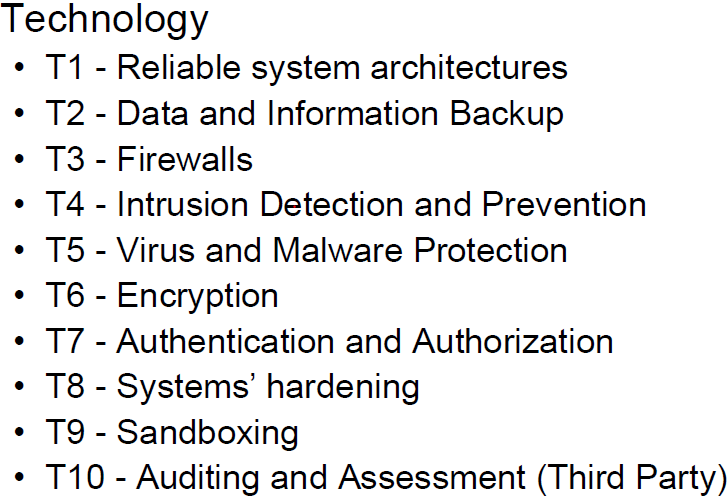
**NETWORK VIRTUAL TERMINAL**



**http**



**Componenti**



**STRATEGIE**



**POLITICHE DI SICUREZZA**

Assicurarsi che siano sempre aggiornate, comprensive, complete, supportate dal management, consegnate ed effettivamente disponibili a tutto lo staff. È il fondamento per l’auditing, valutazione, controlli, formazione e legislazione all’interno di un organizzazione.

**Having a Security Policy document is not enough ...**

**Its contents MUST be implemented !!!**

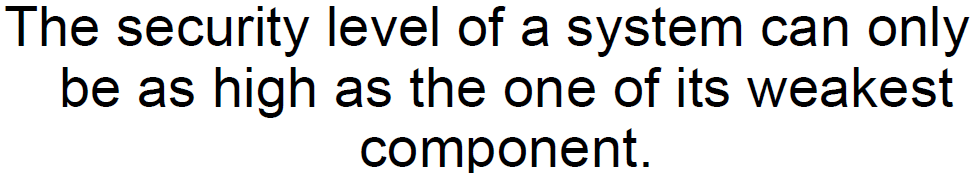
Consapevolezza deve essere sparsa attraverso: mettings interni, articoli promozionali, slogans motivazionali, posters e volantini, tests interni.

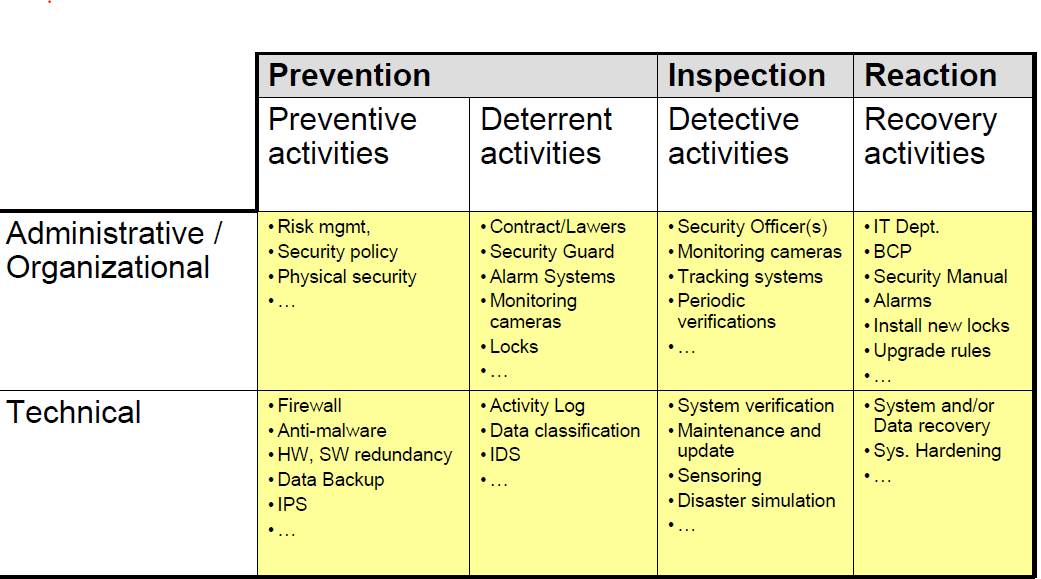
**Sicurezza Fisica**

Questa deve garantire che nessun intruso posso addentrarsi alla struttura, evitare penetrazione attraverso emissioni elettroniche attive, passive, danni da contaminanti ambientali.

**Analisi di rischio**

Comprende identificazione, classificazione di tutte le risorse e dei loro punti deboli





**Standards Applicabili:**

Servono standard per certificazioni applicazioni e prodotti IT , per la corporate governance, definizione politiche di sicurezza. Ad esempio per l’utente finale esiste ISO TR 13335 1-5, per IT-Solutions ITSEC, COMMON CRITERIA ISO 15408.

**ARCHITETTURE DI SISTEMI AFFIDABILI**

Tutti i sistemi devono avere componenti hardware ridondanti (Mirror, RAID, Clustering), UPS(Uniterruptible power supplies), log files per identificare fallimenti, accessi anomali, saturazione risorse. Protocolli di analisi e allarmi per alcune soluzioni.

**RECOVERY POINT OBJECTIVE(RPO)**

Rappresenta il punto in cui i dati sono persi. Il RTO(Recovery Time objective) importante per stimare il tempo di recupero dei dati persi. Si usano spesso i Continuous Data Protection computer salva i dati ogni volta che avviene una modifica.

**FIREWALL**

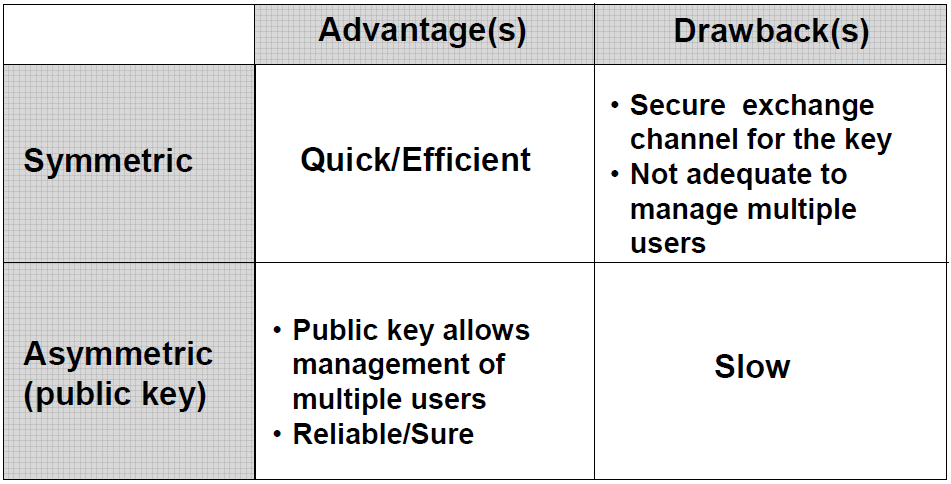
Separa una rete privata da internet governa il flusso di dati da e verso la LAN, filtra i pacchetti in uscita e in entrata, applica regole di selezione forti tra reti o parti di reti. Le diverse archietture sono: filtro di pacchetti, applicare livelli gateway, ispezione stato, rilevare e prevenire instrusioni agli assets.

**PROTEZIONE VIRUS E MALWARE**

Il software deve essere installato e aggiornato in tutti i server delle reti e computers. Funz. Shield: schermata del traffico in computer o sistema di rete.

CRITTOGRAFIA

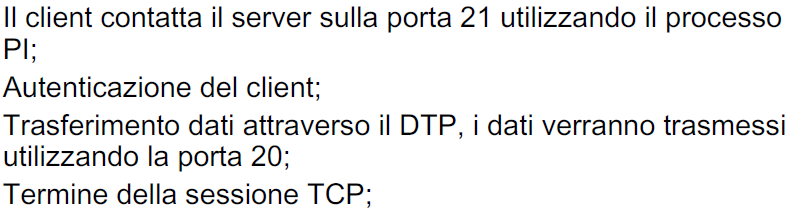
Tecniche di crittazioni comuni riguardano: VPN, S-MIME, SSL, WPA2, crittare i dati salvati nel sistema.



**FTP ANONIMO**

Situtazione dove un file server è pubblico e viene reso disponibile per il download di software. In questo caso al client viene chiesta come password l’email

**FASI DI SESSIONE DI FTP**

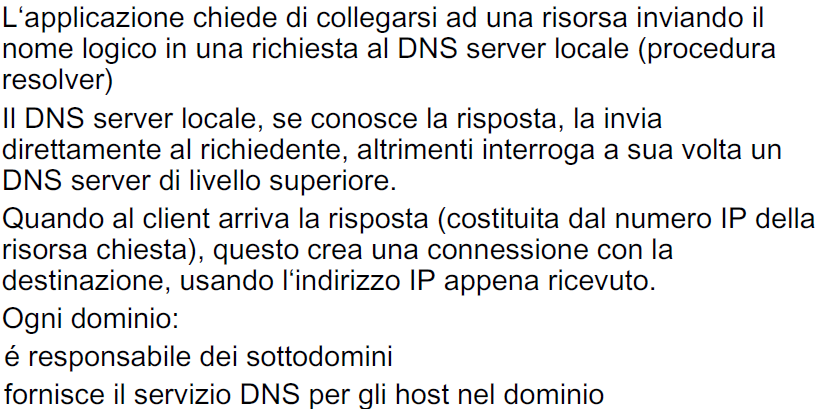


**SFTP**

Usa SSH impedisce di spedire in chiaro la password e il client deve essere abilitato a stabilire una connessione al server

**DNS**

Effettua traduzione indirizzo IP-nome logico usa la porta 53. Le basi del DNS usano schema gerarchico di denominazione, database distribuito e protocollo DNS. Diciamo che usa un db distribuito per creare una corrispondenza tra ip e nome mnemonico assegnato alla macchina. E’ distribuito perché nessun computer collegato alla rete ha una situazione completa dell’intera rete ma deve usare il protocollo previsto dal DNS per comunicare con altri sistemi e procurarsi info. Lo spazio dei nomi DNS p uno spazio gerarchico organizzato in domini e sottodomini (es. host.subdomain.subdomain3.subdomain2.subdomain1.topleveldomain). cammino inverso dalla foglia alla radice. 

Il dominio può essere anche nazionale. 

**PROTOCOLLO SSH (Secure SHell)**

Protocolli tcp/ip non sicuri unico modo di difesa: crittografia, utilizza chiave simmetrica e asimettrica implementa connessioni cifrate protegge da intercettazioni disponibile per altre piattaforme

**MIME (Multipurpose Internet Mail Extensions)**

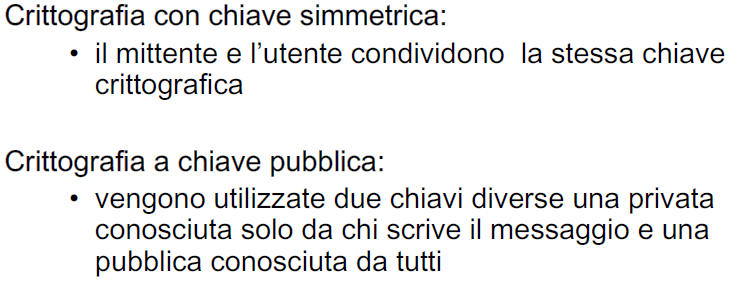
Formato standard per l’invio di messaggi di posta elettronica non testuali.

Può contenere più oggetti nel mess. Set di caratteri diversi (US-ASCII), file binari, immagini, audio ecc.

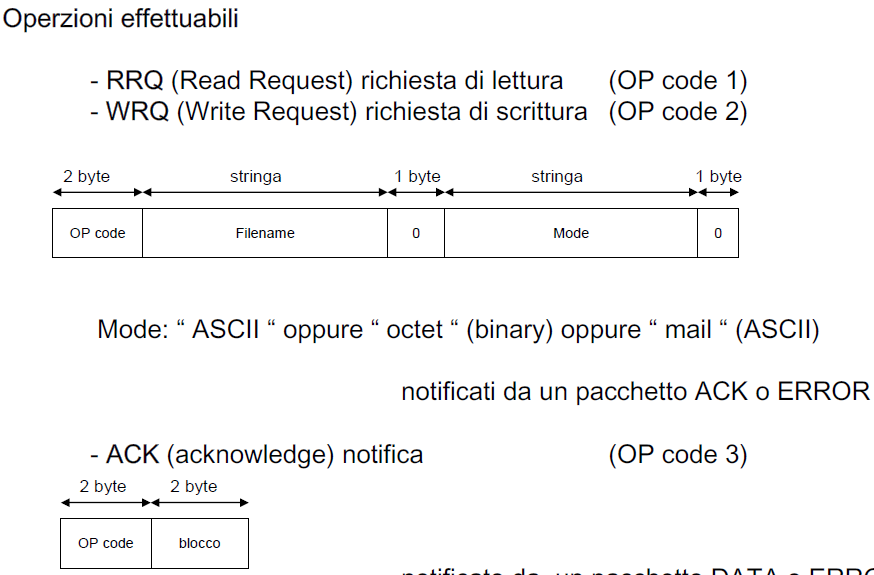
**SMIME**

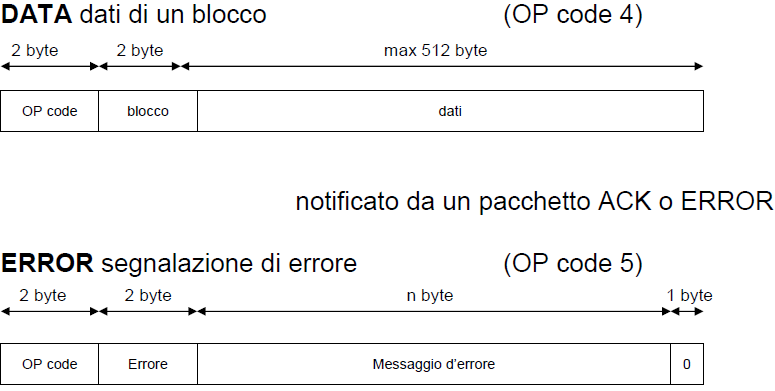
E’ la versione sicura del MIME permette l’autenticazione del mittente (firma digitale) cifratura dei messaggi basato su crittografia mista. Firma digitale si ottiene crittografando con la chiave segreta del mittente un message digest (duplice controllo).

**CRITTOGRAFIA IN S-MIME**

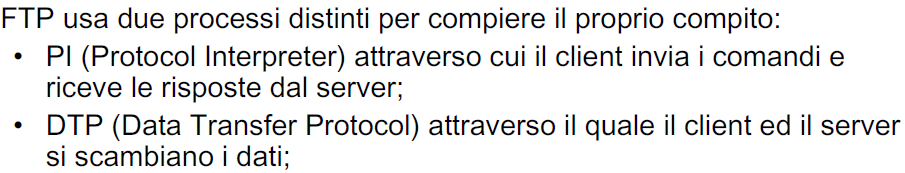


**PROTOCOLLO TFTP (Trivial File Transfer Protocol)**

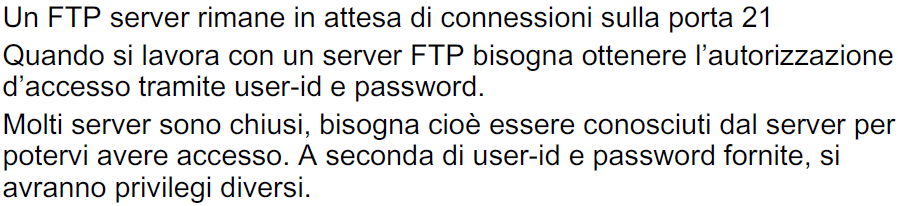
Utilizza UDP, non richiede autorizzazione, è semplice ma con basse prestazioni, inizia con richiesta di lettura e scrittura, vengono spediti pacchetti di 512 byte, un pacchetto da meno di 512 determina la fine della trasmissione, altrimenti errore utilizza minima correzione degli errori. L’elaboratore mittente sceglie TID casuale, in via la richiesta alla porta 69, il server risponde utilizzando un suo TID questi codici verranno utilizzati per il resto della comunicaz.

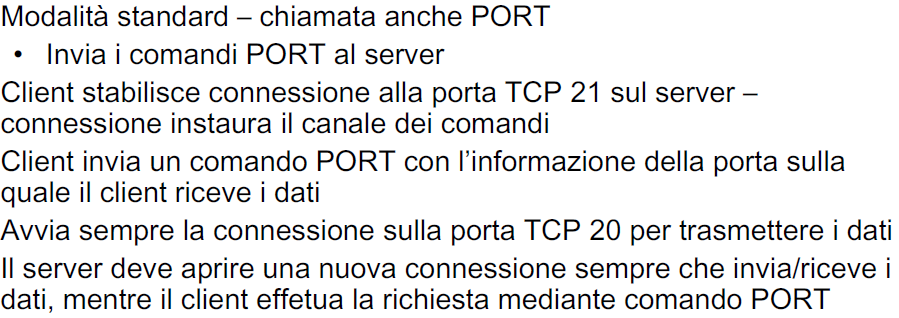


**PROTOCOLLO FTP**

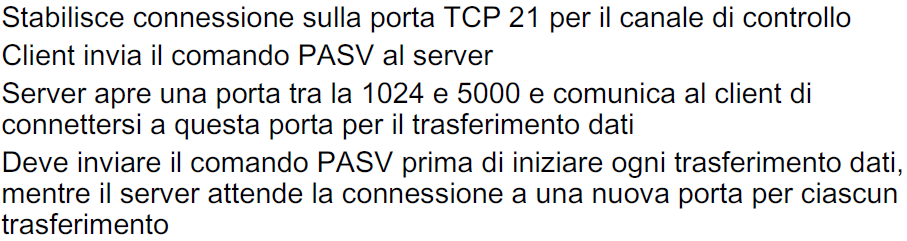
Usato per l’invio di file in internet tra due host. Permette di caricare o scaricare dati (in formato binario o testo) in modo efficiente ed affidabile. Molto veloce e adatto per trasferire file molto grossi o di molti file

**SERVER FTP**



**FTP ATTIVO** 

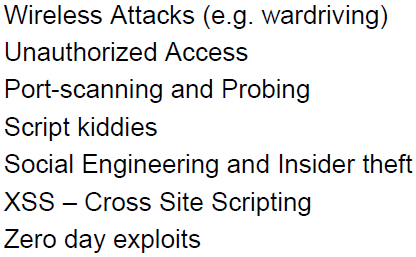
**FTP PASSIVO**



**SICUREZZA**

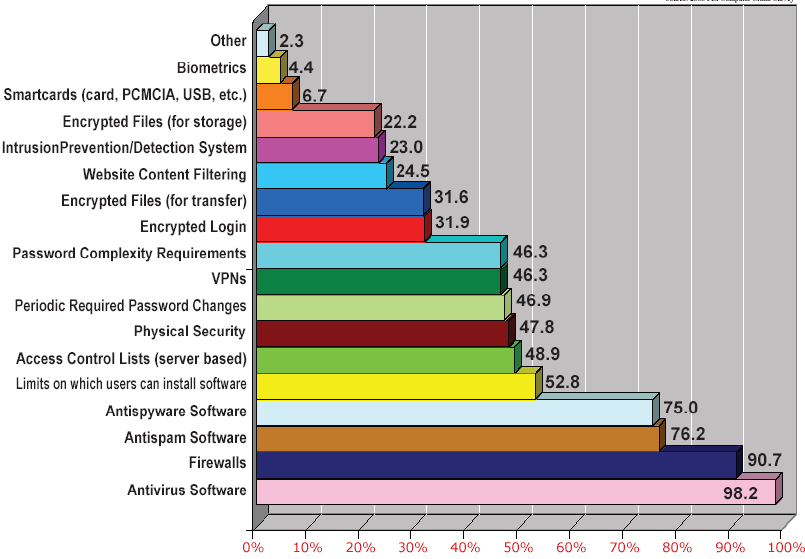
RISCHIO=Minaccia x Probabilità

3 aspetti principali della sicurezza informatica: Confidenzialità, Integrità e Disponibilità.

Debolezze: dipendenti, gestione fatta male del sistema IT (sistemi non aggiornati, configurazione malfatte), utenti del sistema, gestione malfatta password, mancanza di allenamento o informazione, debolezze del sistema non conosciute.

**Minaccia:** azione che sfrutta debolezze per causare incidenti o problemi, sicurezza e affidabilità dei sistemi, gestione sistema, virus e malware.



La sicurezza comporta avere strategie e modelli, politiche di sicurezza, analisi dei rischi e gestione dei rischi. Consiste di diversi livelli: organizzazione, sicurezza sistemi, sicurezza network. Sicurezza organizzazione comprende: politiche di sicurezza, training e consapevolezza, analisi rischi, standard applicabili, gestione dedicata, sicurezza fisica

**VOICE OVER IP**

Limite di banda è sempre tra 300 Hz e 3,4 kHz

Di solito 8 kHz ovvero 1 campionamento ogni 125 ms

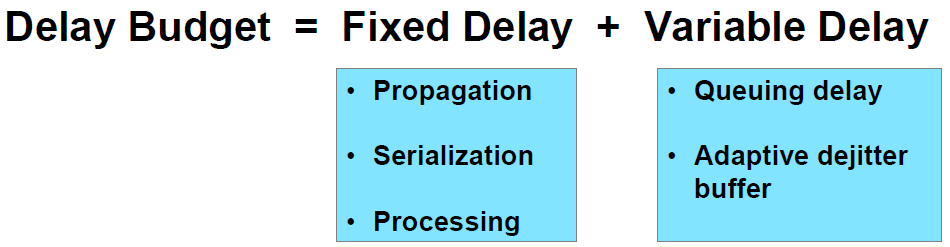
Usa: 7 bit per campione-> 56 kbps e 24 canali per frame: PCM 24 -> 1.544 Mbps

Europa: 8 bit per campione-> 64 kbps e 30 canali 2048 Mbps

Ritardo

0-150 accettabile, 150-400 ms accettabile, >400 ms non accettabile

**DELAY BUDGET**

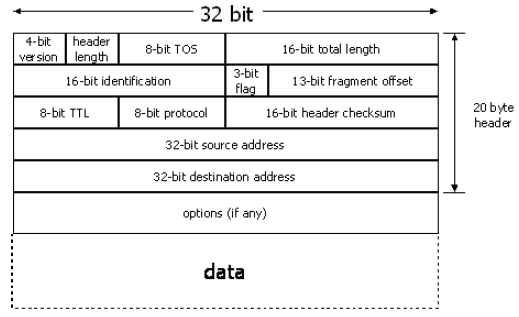


**MEGA RIASSUNTO DEL MODELLO OSI**

Il Layer 1 (Physical Layer) trasmette il segnale (segnali radio, fili di rame) e rappresenta la parte elettrica e fisica del sistema. Include tipi di cavo frequenza dei link, il layout dei pins, voltaggio e altri requisiti. Ad es. il protocollo RJ-45 specifica i cavi ethernet, wifi le onde radio sono trasmesse in 2.4 gHz o 5 gHz bande radio.

Il Layer 2 si occupa di trasferire il pacchetto da un nodo all’altro gestendo errori del physical layer. Questo livello si divide in due sottoporzioni Media Access Control (MAC) e Logica Link Control (LLC). La maggior parte degli switch operano al livello 2. Un esempio è l’ethernet frame. Nell’ethernet abbiamo il Source e dest addresse (12 byte). I primi 3 byte sono l’Organizational Unique Identifier (OUI) del MAC, seguiti da altri 3 byte che rappresentano il vero indirizzo mac. Stessa cosa per il dest. Addr.

Nel layer 3 si trovano la maggior parte delle funzionalità di cui si occupa il router. Questo layer si occupa di inoltrare il pacchetto e di fare routing.



I primi 4 bit dicono la versione ip (4 o 6). I secondi 4 bit dicono quante righe sarà lungo l’header (min. 5, max. 15). Poi abbiamo il tipo di servizio che indica le precedenze e come i dati saranno usati, affidabilità e costi minimi 1 byte. E poi la lunghezza totale (min. 20 byte max 65535 byte). Poi abbiamo 8 bit di identificazione per sapere l’identificatore del gruppo in caso si mandino gruppi di pacchetti. Il Flags invece ci dice se stiamo frammentando i pacchetti e ci dice anche se è l’ultimo pacchetto o no. Es. mando 3 pacchetti. Mando il primo. Identificatore sarebbe sempre lo stesso il flags non sarebbe attivo e fragment offset segnerebbe il nr. Pacchetto (1). Stessa cosa con il secondo e al terzo solo che con quest’ultimo ci sarebbe il flags sarebbe segnato. Poi abbiamo il time to live che indica quanti hop si potranno fare per raggiungere la destinazione. Ogni volta che passa da un router sarà decrementato. Poi il protocollo usato (TCP o UDP). Poi abbiamo l’ip mittente e destinatario. Poi abbiamo options che vengono marcate solo se ci sono e il padding per finire con 32 bit la riga.

Il layer 4 si occupa di sincronizzarsi con i dispositivi e i sistemi. (quanti dati mandare, a che velocità, a che rate, ecc.). il protocollo più usato è il TCP. Le porte del TCP e UDP lavorano in questo livello. Le porte servono ai software per comunicare con l’interfaccia della rete. Per questo che i SO devono chiedere il permesso di poter comunicare con un’interfaccia network. Le porte hanno quindi il ruolo di sapere per chi sarà processato quel pacchetto. Infatti se ricevo un pacchetto sulla porta 21 dal tcp questo sarò sicuramente di un’applicazione che trasferisce file. Le porte vanno da 0 a 65535. Le porta da 0 a 30 sono riservate a servizi che girano nel so.

**SIP ADDRESSING**

Gli inidirizzi sono anche chiamati SIP URI (Universal Resource Indicators). Come indirizzi email sono identificati da [user@host. (es](mailto:user@host.(es). [angeloconsoli@sipcall.ch](mailto:angeloconsoli@sipcall.ch)). Il client può mandare richiesta SIP direttamente al server proxy o all’indirizzo IP e porta del SIP URI corrispondente (più complicato).

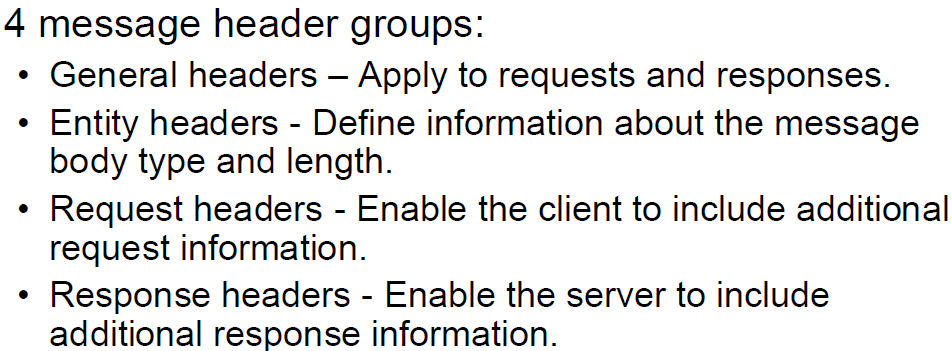
**SIP TRANSACTIONS**

Dopo la risoluzione dell’indirizzo il client manda uno o più richieste SIP e riceve uno o più risposte. Queste sono considerate parte delle transazioni. Per semplicità tutti i campi dell’header in tutte le richieste matchano quelli delle riposte. SIP possono essere trasmesse sia in UDP che TCP.

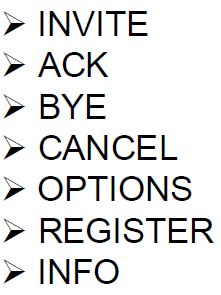
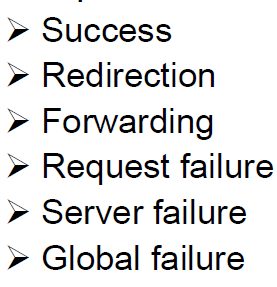
Offre possibilità di localizzare utente che può muoversi in più sistemi. Mobilità in ambiente IP: terminal mobility-> terminale si muove tra subnets, personal mobility-> differenti terminali stesso indirizzo, service mobility-> tiene stessi servizi come quelli del mobile

Le localizzazione di questi end systems possono essere registrati con il server SIP, registrati con altri SIP servers. La localizzazione dell’utente dipende dal tipo di server SIP : redirect server-> ritorna lista completa di locazioni e abilita il client a localizzare l’utente direttamente, proxy server-> prova un indirizzo in parallelo fino a che la chiamata non ha successo.

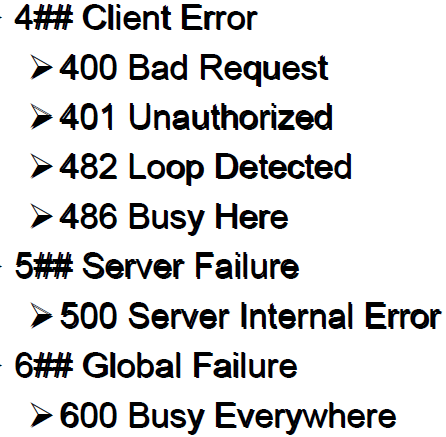
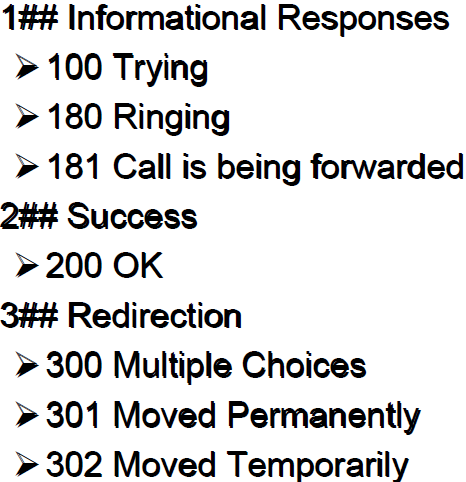
**HEADERS DEL SIP**

Utilizzati per specificare la parte chiamante e la chiamata, route e tipo di messaggio chiamata come http. 

Richieste cliente->server Risposte server->client

CODICI DI RISPOSTA





SIP for telefonia internet

Due tipi – chiamate IP e chiamate analogiche trad. la prima usa DNS e la seconda usa gateway protocols come BGP.

Protocollo corto semplice e flessibile e necessita di pochi messaggi e risposte, usa e-mail e identifica utenti più che dispositivi.

**RFC 2543**

Primo standard per SIP include internet conferenze chiamate telefono ecc. multicast o maglia di unicast. Usa session descriptors supporta mobilità usando proxing e redirecting per chidere localizzaz. Utente.

**FIREWALL**

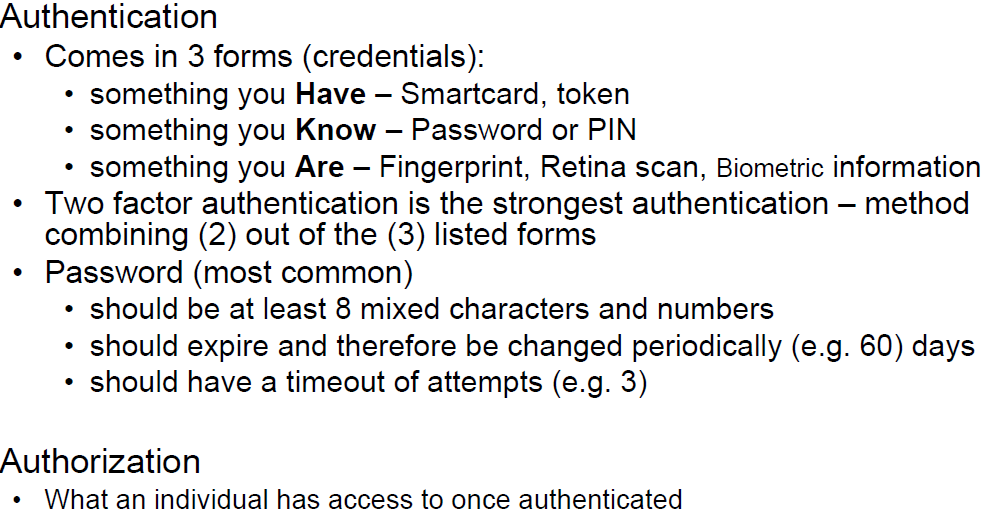
Previene attacchi di DoS e modifiche o accessi ai dati interni, permette solo chi ha il permesso di accedere alla rete. Tre tipi di catene INPUT(destinato al sistema locale), OUTPUT(originato dal sistema locale), FORWARD(entra nel sistema e inoltrato ad un altro destinatario). Tre tipi di operazioni ACCEPT, DROP (rifiuta il pacchetto silenziosamente), REJECT (rifiuta il pacchetto e risponde alla sorgente)

**HASH FUNCTIONS**

Funzioni matematiche one-way convertono grandi q.tà di dati in un piccolo output. Usato per trovare o fare confronti con files, stringhe, corrispondenze DNA ecc.

Il problema è che la signature della chiave privata è troppo lenta e genera tanto overhead. Quindi hash converte il messaggio in uno più piccolo usando un meccanismo complesso da indovinare. Questo valore (16-32 bytes) si chiama message digest o MAC (Message Authentication Code). In questo modo si può crittare solo il MAC con chiave privata per creare una firma digitale. Ricevente rigenera MAC decripta firma digitale e compare per autenticare

**AUTHENTICATION AND AUTHORIZATION**



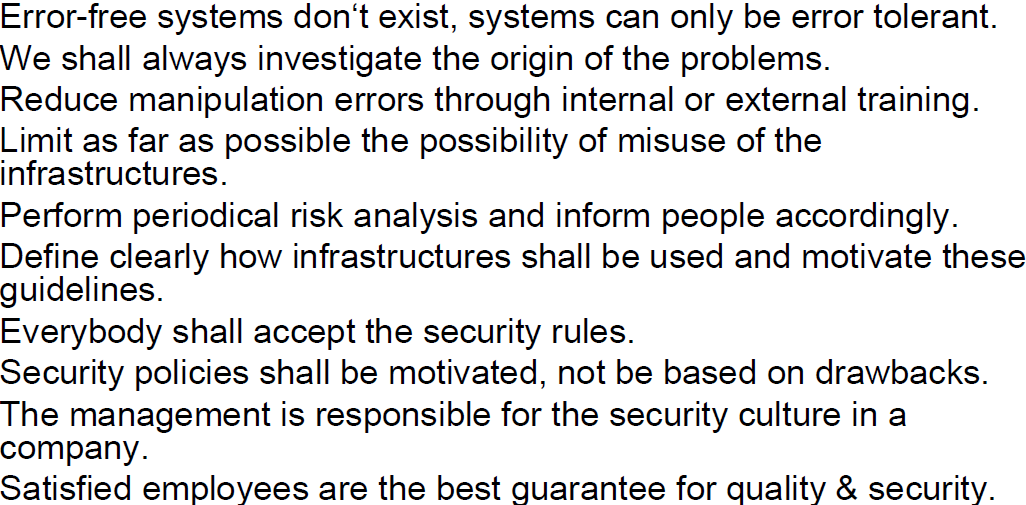
**SYSTEM HARDENING**

Processo per rendere sicuro un computer o un sistema riducendo al massimo le sue vulnerabilità (es. rimuovendo software o servizi non usato, utenti non attivi, chiudendo porte reti aperte, aggiornando sistema, anti-malware, limitando libertà utente, politiche password sicure).

**SANDBOXING**

meccanismo di sicurezza per separare i domini, dove l'ambiente è limitato e dove alcune funzioni sono vietate, usato in mobile e pc(unix usa due sandbox: di processo e a livello di userid). Permette di testare nuovi software, isolare spazi nel disco della memoria, limitare accesso alle reti.

**10 REGOLE D’ORO**

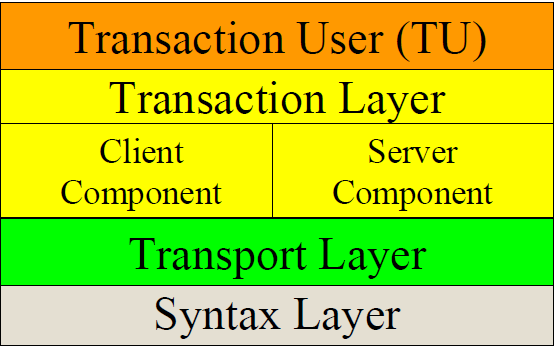


4 tipi di vpn protocols usati per il tunneling:

1. PPTP (Point-Point Tunneling Protocol)
2. L2TP (Layer 2 tunneling Protocol)
3. IPSec (Internet Protocol Security)
4. SSL
5. OPEN VPN

**SIP (Session Internet Protocol)**

Sip è un protocollo di segnalazione a livello di applicazione, è il protocollo che si occupa si avviare gestire e terminare le sessioni in internet. Le sessioni multimediali includono la telefonia via internet, ecc. coinvolgono uno o più partecipanti e possono usare unicast o multicast. Protocollo basato sul testo che fa parte del IETF, può operare con altri protocolli di segnalazione come h323



Due componenti User Agent Client (UAC) che inizializza la richiesta di SIP, ha il ruolo di fare la chiamata all’agent, e User agent Server (UAS) che riceve e ritorna risposte a nome dell’utente, ha il ruolo del chiamato. I componenti sono il network server che comprende **proxy e redirect server** e **registrar**. Il proxy contiene sia le funzioni di client che di server e interpreta o riscrive gli headers prima di passarli ad altri server. Mentre il redirect server accetta richieste SIP e rimanda la risposta al client contenente l’indirizzo del prossimo server. Non accetta chiamate o eleborazioni o inoltri richieste SIP

Layer 4

Quindi le porte con numeri piccoli sono usate per servizi che ascoltano messaggi in arrivo. Quando invece il numero è alto allora è un client che manda un messaggio ad un servizio o ad un server. Poi abbiamo il Sequence Number che serve al protocollo per capire l’ordine di pacchetti (UDP non lo usa). L’ack invece serve per il sender per capire se il pacchetto è stato ricevuto altrimenti lo rimanda. UDP non lo fa. E poi ci sono i flags che servono per comunicare il tipo di operazione (push, urgent, acknowledge)

Il layer 5 serve per poter mantenere la comunicazione tra due dispositivi. Questo layer infatti si occupa di installare, coordinare e terminare una connessione in una sessione.

Il layer 6 si occupa di rappresentare i dati. Ad es. crittandoli o decrittandoli oppure uno zip ecc.

VOIP

Per digitalizzare un segnale devi campionarlo nel tempo e poi quantizzarlo in altezza. La frequenza di campionamento consigliata è 8 kHz quindi il tempo di campionamento è di 123 ms. in Europa si usano 8 bit, USA 7 bit. Il CODEC strumento che ottimizza la compressione vocale togliendo le cose che sono superflue tipo i silenzi