RETI E SICUREZZA

CLEI - Una facoltà in via di estinzione
Appunti di Reti e Sicurezza di *Giovanni Gardini*
Professore: ***Mauro Gaspari***
Anno di corso: 2° anno – 2° trimestre
Versione degli appunti: v0.4 sulla via definitiva
Ultimo aggiornamento: martedì 26 giugno 2007
Ultima revisione eseguita da: Giovanni

Introduzione alle Reti – Alcune terminologie specifiche

Due tipi di tecnologie trasmissive:

- collegamenti **broadcast**: un solo canale di comunicazione che è condiviso tra tutte le reti. Ciascuna macchina invia un messaggio (**pacchetto**) a tutte le altre. Se il pacchetto è destinato ad una determinata macchina viene processato, altrimenti ignorato.
- collegamenti **punto punto**: ci sono molte connessioni tra singole coppie di macchine. Per andare dalla sorgente alla destinazione un pacchetto deve visitare una o più macchine intermedie.

Multicasting: alcune reti broadcast supportano la trasmissione verso sottoinsiemi di macchine, specificando speciali bit nell'indirizzo del destinatario.
Unicasting: trasmissione punto punto con una macchina che trasmette ed una che riceve.

Dimensione delle reti

LAN – Local Area Network: sono reti private installate all'interno di un singolo edificio o area geografica di dimensioni massime dell'ordine di pochissimi chilometri. Collegano pc e workstation negli uffici allo scopo di condividere risorse, ad es. stampanti. Lavorano a velocità basse, dell'ordine di 10-100 Mbps.

- rete a bus: con cavo lineare che collega tutte le macchine, una sola delle quali è master in uno stesso istante.
- rete ad anello: ogni bit si propaga in modo autonomo facendo il giro dell'anello.
- IEE 802.3 ETHERNET: rete broadcast a bus. I pc connessi trasmettono quando vogliono, se i pacchetti collidono i pc attendono un tempo casuale poi ritrasmettono.
- IEE 802.5: token ring IBM, con regole che arbitrano l'accesso alla trasmissione in anello.

MAN – Metropolitan Area Network: ad esempio la rete tv via cavo americana. Uno stesso segnale viene distribuito a più utenti (case ad es.) mediante uno stesso cavo. Lo stesso cavo può essere utilizzato per comunicazioni bidirezionali (es: accesso ad Internet).

WAN – Wide Area Network: copre un'area estesa (nazione – continente), collegando **host**, ovvero macchine che eseguono programmi applicativi di utenti finali.
Subnet o communication subnet: l'insieme delle tecnologie ed infrastrutture di rete che mettono in comunicazione gli host, solitamente è di proprietà da ISP o

dalla compagnia telefonica. La subnet è composta da:

- **linee di trasmissione**: i cavi o i collegamenti wireless;
- **elementi di commutazione**: computer o hardware dedicato che smista il traffico tra tre o più linee di trasmissione (**router**).

Subnet packed-switched: subnet a commutazione di pacchetto. Il pacchetto viene ricevuto da un router intermedio, memorizzato e indirizzato alla porta necessaria appena libera.
Algoritmo di routing: se sono possibili più percorsi tra router intermedi è necessaria una decisione sul miglior percorso possibile, elaborata da appositi software integrati nelle macchine instradatrici.
Reti wireless
Tre categorie principali:

- **connessioni all'interno di un sistema**: tecnologia Bluetooth che mette in comunicazione le periferiche di un singolo host;
- **LAN wireless**: ogni host ha un sistema radio con cui può dialogare con altri sistemi e punti di accesso ad una rete condivisa. Tipico esempio la sede di E.I. di via Pratella.
- **WAN wireless**: sistemi di connessione su aree geografiche molto estese, come ad esempio la rete per la telefonia mobile. Queste WAN sono solitamente a basso bitrate, ma sono in sviluppo anche reti a banda larga e copertura estesa (Wi-Max) che forniranno connessione ad Internet senza necessità di transitare attraverso l'attuale rete telefonica.

Le WAN wireless, se disporranno in futuro di banda sufficientemente larga, potrebbero sostituire tutte le attuali reti duplicate esistenti (GSM, TV, Radiofonia, GPRS, UMTS, trasmissioni televisive da satellite, telefonia fissa, ecc..), offrendo servizi migliori (web tv, web radio, social networking, ecc...) a costi probabilmente più bassi e con minore potenza emessa complessiva.

Reti domestiche

In futuro probabilmente le abitazioni avranno una rete interna che collegherà la maggior parte degli elettrodomestici, sistemi di allarme e sorveglianza, sistemi di intrattenimento, ecc.. Requisiti fondamentali di tali reti saranno:

- facilità di installazione (es: access point wireless)
- interfacce a prova di idiota
- basso costo
- banda larga (a causa dei requisiti richiesti dai sistemi di intrattenimento)
- uniformità di standard stabile nel tempo.

Reti tra sistemi

Gateway: sistemi che forniscono servizi hardware e software di interconnessione e conversione tra reti differenti.
Internetwork o internet insieme di reti interconnesse.
Subnet, reti e internetwork: subnet, in contesto WAN, riferisce all'insieme di router e linee di comunicazione. Rete è la combinazione di subnet ed host utilizzatori. Internetwork è l'insieme di più reti.

Software di rete

Gerarchia di protocolli: per diminuire la complessità le reti sono organizzate

come pile di molteplici strati o livelli. Ogni strato fornisce servizi agli strati di livello superiore. L'implementazione di ciascuno strato non viene mostrata all'esterno.
Interfaccia: tra ciascuna coppia di strati contigui si trovano le definizioni delle operazioni elementari e dei servizi che lo strato inferiore mette a disposizione dello strato superiore.
Protocollo: un accordo tra le parti che comunicano sul modo in cui far procedere la comunicazione. Generalmente sono implementati nel sistema operativo.
Peer: entità che formano strati di pari livello su diversi dispositivi (pc, router, ecc..)
Architettura di rete: l'insieme di strati e protocollo.
Stack (Pila) **di protocolli**: elenco di protocolli usati da uno specifico computer o dispositivo.

Servizi orientati alla connessione e senza connessione

Servizio orientato alla connessione: servizio che attiva una connessione, la utilizza e rilascia le risorse impiegate. L'ordine di invio delle informazioni è solitamente conservato.
Negoziazione: operazioni preliminari di accordo sui parametri da utilizzare per la connessione.
Servizio senza connessione: ogni pacchetto di informazioni è instradato in modo indipendente dagli altri ai quali è legato. E' probabile che l'arrivo a destinazione non sia nello stesso ordine della spedizione.
Servizi affidabili: è fondamentale che non venga perduto nemmeno un pacchetto facente parte dell'invio originale di dati. A tale scopo viene sempre inviato un segnale di conferma della ricezione (sicurezza di integrità = ritardi e maggior consumo di banda).
Servizi inaffidabili: a volte è preferibile perdere alcuni bit (es: trasmissione voce o video digitale) in favore di tempi di trasmissione real time, senza ritardi.
Datagram: servizio senza connessione non affidabile.
Datagram con conferma: servizio senza connessione affidabile.
Chi vorrebbe un servizio non affidabile? un servizio affidabile potrebbe essere non disponibile (Ethernet), oppure non accettabile per i ritardi introdotti.

Primitive di servizio

Primitive: un servizio è formato da in insieme di operazioni che i processi utente hanno a disposizione per accedere al servizio.
Primitive per un servizio orientato alla connessione:

- LISTEN: attesa che blocca il processo server in attesa di una connessione in arrivo;
- CONNECT: stabilisce una connessione tra pari in attesa;
- RECEIVE: attesa che blocca il processo server in attesa di un messaggio in arrivo;
- SEND: manda un messaggio allo strato pari (peer);
- DISCONNECT: termina una connessione

Esempio di connessione:

- il server è in attesa (LISTEN)

- il client invia una richiesta di connessione (CONNECT) ed aspetta (RECEIVE)
- il server risponde con una conferma (acknowledgement mediante SEND) ed aspetta (RECEIVE)
- il cliente invia la richiesta dati (SEND) ed aspetta (RECEIVE)
- il server risponde con i dati richiesti (SEND) ed aspetta (RECEIVE)
- il client riceve i dati e può chiedere ancora oppure disconnettersi (DISCONNECT)
- il server si disconnette (DISCONNECT) e si rimette in attesa (LISTEN)

E' fondamentale la temporizzazione secondo cui avvengono tutti questi processi.

Relazione tra servizi e protocolli

Servizio: è un insieme di primitive (operazioni) che uno strato offre a quello superiore (interfacce tra gli strati).
Protocollo: è un insieme di regole che controllano il formato ed il significato dei pacchetti, o messaggi scambiati tra entità di pari strato (peer) situate su computer diversi.

Modello di riferimento ISO OSI

E' composto da sette strati:

- **STRATO FISICO**: si occupa della trasmissione di bit grezzi sul canale di comunicazione. A questo livello si trattano bit (0,1), Volt di corrente, tempi di durata della trasmissione,tipi di cavi o di antenne, ecc...
- **STRATO DATA LINK**: il compito principale di questo strato è la correzione degli errori in modo da non dover trasmettere pacchetti corrotti allo strato superiore. Questo strato suddivide i dati in ingresso in **data frame** che vengono trasmessi sequenzialmente verso la destinazione. Con servizio affidabile vine inviato un segnale di acknowledgement. Altri compiti sono il controllo del flusso di dati (per non saturare destinazioni più lente) e, nelle reti broadcast, il controllo dell'accesso al canale condiviso (**sottostrato MAC**).
- **STRATO NETWORK**: controlla il funzionamento della subnet, si occupa delle modalità per inoltrare i pacchetti dalla sorgente alla destinazione. Controlla inoltre la congestione della rete, in modo da evitare colli di bottiglia gestendo la **qualità del servizio**.
- **STRATO TRASPORTO**: accetta dati dallo strato superiore (sessione), li divide in unità più piccole se necessario, le trasmette allo strato inferiore (network) e si assicura che tutto arrivi integro al processo pari
- **STRATO SESSIONE**: permette ad utenti su computer diversi di stabilire tra loro una sessione, ovvero vari servizi tra cui controllo del dialogo (turni di trasmissione), gestione dei token (evitare sessioni critiche allo stesso tempo) e sincronizzazione (supervisione di una lunga trasmissione per riprenderla in caso di crash).
- **STRATO PRESENTAZIONE**: si occupa della sintassi e della semantica dell'informazione trasmessa.
- **STRATO APPLICAZIONE**: una varietà di protocolli comunemente richiesti dagli utenti. HTTP, FTP, POP, SSL, ecc...

Perché il modello OSI non ha avuto successo e non è stato implementato?

- Poca tempestività: lo standard era pronto quando già si erano fatti considerevoli investimenti in TCP/IP
- Tecnologia scadente: troppo complesso e mal organizzato
- Carenza di implementazioni
- Difficoltà politiche di promozione dello standard

Il modello di riferimento TCP/IP

Nel modello TCP/IP non sono presenti lo strato sessione e presentazione del modello OSI; inoltre lo strato trasporto è detto strato internet. TCP/IP è l'evoluzione del precedente sistema ARPANET, una rete sperimentale che connetteva centinaia di campus ed università degli stati uniti e, successivamente, basi militari. Un obiettivo (necessità militare) da soddisfare per TCP/IP è la sopravvivenza della rete a prescindere dalla improvvisa perdita di porzioni del suo hardware, senza interrompere le trasmissioni in corso. Richiesta inoltre architettura flessibile per soddisfare necessità divergenti (trasferimento file, trasmissione voce, ecc..)

- **STRATO INTERNET**: è stato scelto un sistema di rete a commutazione di pacchetto basato su uno strato internetwork senza connessione. Consente di mandare pacchetti in qualsiasi rete, facendoli viaggiare in modo indipendente l'uno dall'altro fino alla destinazione. Se arrivano in ordine diverso è compito di strati superiori riordinarli.
  - **IP**: il formato ufficiale per i pacchetti e il protocollo per trattarli.
- **STRATO TRASPORTO**: consente la comunicazione tra entità pari di sorgente e destinazione. Vi sono due protocolli di trasporto:
  - **TCP**: è un protocollo affidabile orientato alla connessione (flusso di byte). Crea pacchetti di dati e li consegna allo strato internet. Il TCP ricevente ricompone il flusso di byte. Gestisce inoltre il controllo di flusso.
  - **UDP**: protocollo inaffidabile senza connessione per le applicazioni che non vogliono la garanzia di ordinamento e di controllo di flusso di TCP. E' applicato dove la consegna rapida è più importante dell'accuratezza.
- **STRATO APPLICAZIONE**: contiene tutti i protocolli di livello superiore (TELNET, FTP, SMTP, DNS, NNTP, HTTP, SSL, SSH, ecc...

Sotto lo strato internet il modello TCP/IP non dice cosa ci debba essere, limitandosi a segnalare che si debba usare un qualche protocollo che consenta di spedire pacchetti IP.
Lo standard TCP/IP non dice nulla su ciò che sottostà allo strato applicazione. ISO OSI è stato perciò utile per discutere le reti dal punto di vista teorico. Al contrario i protocolli tcp/ip sono stati largamente usati. Per implementare gli strati datalink e fisico ci si è basati soprattutto sui protocolli discussi in OSI.

INTERNET

Internet è una raccolta di reti differenti che usano certi protocolli e offrono alcuni servizi comuni.
Storia di Internet:

- ARPANET: anni '50, rete militare in grado di resister ad attacchi atomici senza cadere completamente. Le università americane iniziarono a essere collegate da prototipi in modo tale da poter condurre lo sviluppo e lo studio

sulle reti.
- NSFNET: anni'70, unione via rete di tutti i gruppi universitari americani
- NAP (network access point): anni '90, ISP (internet service provider) commerciali iniziano a costituire l'attuale rete mondiale.

L'architettura che si è sviluppata è composta prevalentemente secondo uno stesso schema:
- dal cliente, attraverso la linea telefonica, si arriva ad un POP (point of presence) dell'ISP (tipo www.Libero.it), che possiede una sua rete regionale;
- se il pacchetto è diretto ad un destinatario interno alla rete dell'ISP, viene inoltrato, altrimenti viene passato all'operatore di backbone (ovvero il monopolista che possiede la rete fisica, tipo Telecom);
- I router del backbone indirizzano il pacchetto a livello nazionale, oppure attraverso interconnessioni con altre reti. I backbone possiedono **carrier hotel**, ovvero armadi he affittano alle grandi aziende che possiedono **web farm**, ovvero sistemi che servono migliaia di pagine web al secondo.
- I backbone sono interconnessi tra loro da router ad grande velocità detti NAP, ovvero grandi sale piene di router interconnessi, uno per ogni backbone.

ATM

Asyncronous **T**ransfer **M**ode: rete asincrona orientata alla connessione.
Asincrona: la maggior parte delle trasmissioni telefoniche è di tipo sincrono, ovvero legato ad un ciclo di clock come segnale di sincronia.
La rete attiva canali di trasmissione virtuali:
- un pacchetto attiva la trasmissione: i router si configurano riservando risorse per mettere in comunicazione i due host;
- i pacchetti inviati effettuano lo stesso percorso all'interno dei router fino alla fine della comunicazione tra i due host (**connessione** o **circuito virtuale**);
- similmente alle linee affittate presso un operatore telefonico, le reti ATM supportano **circuiti virtuali permanenti**.

I pacchetti ATM sono detti **CELLE**. La consegna delle celle non è garantita, lo è l'ordine.

Ethernet (IEEE 802.3)

Sistema di connessione tra molti computer in una LAN (aziende, università, scuole, uffici, case,...). La prima versione era composta da grossi cavi coassiali lunghi fino a 2,5 Km, capaci di sostenere fino a 256 computer collegati in parallelo (**cavo multidrop**).

LAN senza fili 802.11 – Wi-Fi

Standard nato con i pc portatili: inizialmente esistevano molte soluzioni proprietarie, poi IEEE creò questo standard in modo simile alla LAN ethernet. 802.11 venne reso compatibile con Ethernet sopra lo strato datalink.
Problemi:
- ci sono tre computer, A – B – C.
  Se A vuole comunicare con B, potrebbe iniziare a trasmettere, ma B sta già

ascoltando C. A non riesce a sentire C poiché sono troppo lontani.
- un segnale può essere riflesso da superfici solide e ricevuto più volte (**multipath fading**).
- molto software non è concepito per la mobilità
- un computer viene spostato in zone coperte da punti di accesso alla rete (antenne) differenti: è necessario un sistema, in analogia alle telefonia cellulare, che commuti il segnale a cui agganciarsi in modo trasparente all'utente.

Standard **de facto**: impostisi senza piani formali
Standard **de iure**: formali, adottati da qualche organismo di standardizzazione.
Organismi "standardizzatori":
- ITU: International Communication Union, ha 200 membri governativi. Le raccomandazioni ITU sono solo dei suggerimenti. Gli standard si impongono mano a mano che tanti paesi li adottano, a causa delle esternalità di rete positive prodotte.
- CCITT: altro nome di ITU
- ISO: International Standard Organization, organismo che emette standard per quasi qualunque cosa..
- ANSI: costola america dell'ISO
- IEEE: Istitute of Electrical and Electronic Engineer, la più grande organizzazione professionale del mondo.

Breve riepilogo reti Ethernet

ATM

Una tecnologia a commutazione di cella capace di trasmettere dati, voce e video. Le informazioni vengono impacchettate in celle da 53 byte ciascuna spedita autonomamente a destinazione come nella commutazione di pacchetto. Solo che, a differenza della commutazione di pacchetto, qui la cella non contiene l'indirizzo del destinatario ma contiene il numero del circuito virtuale su cui deve viaggiare e non deve andarsi a cercare il percorso per raggiungere il destinatario. Il circuito virtuale si comporta come se fosse un circuito fisico creato tra due punti terminali della linea di comunicazione, ma in realtà può consistere di diversi percorsi fisici, così che diverse celle viaggino in parallelo su linee diverse arrivando contemporaneamente alla stessa macchine. In questo modo si ottiene un'elevata scalabilità della capacità trasmissiva (da 1,5 Mbps a 622 Mbps).

ARP

Un protocollo di basso livello della famiglia TCP/IP che serve a ricavare l'indirizzo fisico della macchina (quello della scheda) partendo dal suo indirizzo IP. All'intera rete viene inviato un messaggio broadcast contenente la richiesta ARP. Il nodo che dispone di quell'indirizzo risponde fornendo il proprio indirizzo hardware. Da quel momento in poi sarò in grado di ricevere i pacchetti ad esso indirizzati.

Commutazione di pacchetto

Un metodo trasmissivo che suddivide il messaggio in diversi pacchetti ciascuno dei quali può seguire un percorso diverso per raggiungere la medesima destinazione. La rete si fa carico di controllare che all'altro estremo i pacchetti vengano riassemblati nella giusta sequenza. Con questa tecnica è possibile far coesistere diversi utenti sula medesima linea fisica, ottimizzandone l'impiego e ricucendo i costi. In questo caso i costi sono proporzionati al volume di traffico e non al tempo di connessione oppure alla distanza di collegamento, come avviene nelle reti a commutazione di circuito.

Connectionless network

Una rete dove ciascun pacchetto viaggia per conto proprio e non è necessario creare una connessione fisica tra due interlocutori prima di trasmettere informazioni. Queste vengono spedite assumendo che il destinatario sia in ascolto e pronto a riceverle, Come quando si imbuca una lettera, lasciamo che sia il servizio postale a consegnarla, presumendo che il destinatario non abbia cambiato indirizzo. E' un sistema veloce e pratico per le reti locali piccole, dove i tassi di errore di consegna sono estremamente bassi.

Connection-oriented network

Una rete in cui, prima di iniziare qualunque trasmissione, ci si assicura che il destinatario sia pronto a ricevere, scambiando con esso una sequenza di messaggi di servizio che servono a creare una sessione di collegamento tra il mittente ed il destinatario. Tale sessione rimarrà attiva fino al termine del trasferimento dati, dopodiché verrà chiusa.
Datagramma
Un pacchetto il cui instradamento e la cui interpretazione sono indipendenti dagli altri pacchetti generati da l medesimo host; ha una lunghezza definita e contiene informazioni sufficienti per essere trasportato dal mittente al destinatario. Ogni datagramma deve contenere un indirizzo di provenienza ed uno di destinazione poiché non può contare sui pacchetti che lo hanno preceduto, né s informazioni memorizzate sui dispositivi che attraversa durante il suo percorso. I datagrammi consentono di suddividere le informazioni in pacchetti indipendenti, ciascuno dei quali segue una strada (anche differente) per giungere a destinazione, lasciando che sia il destinatario a ricostruire la sequenza corretta. In questo modo la comunicazione passa anche se la linea di comunicazione principale viene a mancare. Tecnicamente si può definire come l'unità minima d'informazione che viene scambiata tra i protocolli UDP e IP.

FDDI (Fiber Distributed Data Interface

Una rete a 100 Mbps che trasmette pacchetti d'informazione su un anello in fibra ottica a cui sono collegate tutte le macchine. Per sicurezza l'anello può essere doppio; in tal caso i pacchetti girano in senso inverso nei due anelli. Dato l'elevato costo questo tipo di rete viene utilizzato prevalentemente per la realizzazione di dorsali cui interconnettere reti locali più lente.

NetBIOS

Una estensione al BIOS dei computer sviluppata nel 1984 per consentire alle applicazioni di vedere le risorse della rete senza conoscere l'architettura di quest'ultima.

NetBEUI

Un protocollo veloce e abbastanza efficiente sviluppato da Microsoft per LAN di tipo dipartimentale (da 20 a 200 utenti), con possibilità di integrazione con un mainframe. A differenza del protocollo NetBIOS formalizza il formato della trama.

IP

Il principale strumento per la comunicazione di pacchetti su una rete Internet. IP convoglia l'indirizzo del mittente e del destinatario di ogni pacchetto; Ciascun indirizzo è composto di 32 bit suddivisi in quattro ottetti. Una parte di questi ottetti viene utilizzata per identificare la rete di destinazione ed il resto identifica uno specifico nodo di quella sottorete. Gli ottetti vengono normalmente rappresentati mediante il numero decimale corrispondente (0-255) e ogni ottetto viene separato dal successivo mediante un punto (es: 134.87.255.2). Esiste un ente centrale che assegna gli indirizzi IP.
Il primo elemento di una rete Ethernet è il ripetitore, un apparecchio che

amplifica e rigenera il segnale in arrivo su ciascuna delle sue porte. In una rete che usa come cablaggio un doppino non schermato il ripetitore prende il nome di hub. Diversi hub possono essere collegati in cascata tra loro e ciascuno di essi può avere diverse macchine collegate. L'insieme di questi nodi costituisce una **shared media LAN**, ossia una rete locale a condivisione d'accesso: la singola rete e la sua capacità trasmissiva viene ripartita tra tutti gli utenti collegati. Su LAN molto grandi si arriva presto alla congestione del traffico.
Salendo nella gerarchia troviamo il **bridge**, un dispositivo che funziona come *ponte* tra diversi segmenti di rete. Ciascun segmento costituisce un dominio di collisione autonomo, cioè il bridge fa passare da un segmento all'altro solo i pacchetti validi e filtra le collisioni. Un bridge ethernet è trasparente, funge cioè da intermediario tra due o più segmenti senza che questi si accorgano della sua presenza. Non verifica a chi sono diretti al contrario del **learning bridge**, un dispositivo capace di memorizzare al proprio interno gli indirizzi fisici delle macchine presenti su ciascun segmento, così da regolare la diffusione del traffico.
Il prossimo passo evolutivo è lo **switch**, o commutatore. Si tratta di un learning bridge che esegue la manipolazione delle trame attraverso circuiti dedicati, anziché attraverso un processore di uso generale. Lo switch dispone di una tabella di configurazione abbastanza ampia da contenere gli indirizzi di tutte le possibili macchine presenti nella LAN. Lo switch elimina i ritardi di propagazione introdotti da un bridge, moltiplicando di due-dieci volte l'efficienza della rete. Il limite dello switch è che la propagazione del traffico avviene senza priorità. Non è possibile distinguere un trasferimento di file da una sessione di streaming audio-video. Inoltre fa passare anche i pacchetti di broadcast; questi pacchetti sono un male necessario poiché propagano informazioni di manutenzione e configurazione, ma tendono ad affogare la rete.
L'unico dispositivo in grado di controllare la propagazione dei broadcast è il **router** o instradatore. Esso si colloca al vertice della gerarchia dei prodotti di networking e costituisce il più complesso tra gli apparati di smistamento e di controllo. Non può sostenere grandi volumi di traffico: esistono router veloci, ma il loro prezzo è alto.
Uno switch in grado di emulare alcune funzioni tipiche di un router costituisce l'essenza d una **VLAN** (LAN virtuale). Il primo obiettivo di una VLAN consiste nell'isolare zone della rete cosicché ciascuna di esse costituisca un dominio di collisione autonomo: i broadcast di una VLAN non si propagano in un'altra. Come seconda funzione può riconoscere il tipo di traffico ed assegnare una priorità di consegna.
Il router trova il percorso migliore per recapitare un pacchetto spedito da una rete ad un'altra rete. Esso svolge gran parte delle proprie funzioni mediante uno specifico strato di software e non mediante circuiti hardware dedicati. Pertanto è estremamente versatile, ma lento, cosa che comunque non dovrebbe preoccupare in quanto il suo compito è instradare dati su linee geografiche la cui banda ad esso riservata è solo una frazione della velocità della rete locale.
Il sistema di routing più elementare consiste in un server munito di tante schede di rete quante sono le reti da interconnettere e con speciali funzioni software installate. In una soluzione di questo tipo la debolezza sta nella scarsa versatilità della rete a fronte di un guasto sul server. In ogni caso la vocazione primaria del router è la connessione geografica di diverse reti, che uno switch o un bridge non potrebbero gestire in modo efficiente. Immaginiamo che la porta verso il modo di

un LAN sia uno switch, esso dovrebbe conservare in locale una tabella contenente gli indirizzi fisici di tutte le macchine con cui si è entrati in contatto. Il router risolve la situazione ponendosi come intermediario: costruisce al proprio interno una tabella degli indirizzi fisici di tutte le macchine connessa nella sottorete cui il router appartiene e degli altri router con cui è in contatto e attraverso i quali può raggiungere una certa destinazione. Disponendo di un elenco di tutti i percorsi possibili, il router può valutare percorsi alternativi per portare a destinazione un pacchetto.
Quando un frame arriva ad un router esso ne estrae il pacchetto contenuto, ne legge l'indirizzo del destinatario e prepara una trama in cui includere il pacchetto che trasporta l'informazione o ad un router successivo, usando il formato di trama richiesto tra i due, o proprio alla destinazione finale. La tram contiene l'indirizzo fisico (**MAC address**) della stazione ricevente.

Lo strato Fisico

Le basi teoriche

Le informazioni possono essere trasmesse variando alcune proprietà fisiche del mezzo di trasmissione. Nel caso di un cavo metallico **tensione** e **corrente**.
I segnali trasmessi su mezzi fisici in generale corrispondono a tensioni o correnti variabili nel tempo. Ad esempio i segnali in uscita da un microfono, da una telecamera o da una sorgente di dati come un computer vengono rappresentati mediante funzioni reali del tempo, ma può risultare comodo anche rappresentare questi dati come una oscillazione sinusoidale modulata (a parametri variabili).
Sia il valore della tensione (o della corrente) una funzione del tempo ***g(t)***. E' possibile studiare questa funzione mediante l'analisi matematica e modellarne il comportamento.
Secondo Fourier qualunque funzione periodica sufficientemente regolare g(t) con periodo **T** può essere ottenuta sommando un numero idealmente infinito di funzioni seno e coseno.
Un segnale di durata finita, come ad esempio una trasmissione di dati binari su cavo, può essere trattato matematicamente immaginando che esso si ripeta ogni periodo T di tempo.
Immaginando di dover trasmettere la sequenza 0100110 avremo:

Nel mondo fisico reale non è possibile far mutare la corrente o la tensione dal valore 0 al valore 1, e viceversa, in modo istantaneo: vi sono dei periodi di transitorio in cui crescono/decrescono rapidamente. Mediante le trasformazioni di Fourier è possibile trovare un segnale reale (fatto di corrente / tensione elettrica) generabile che, se trasmesso su un mezzo adatto, riproduce con sufficiente approssimazione il segnale “ideale” che si voleva rappresentare.
$1/T = f_0$ è la **frequenza base**. Per ogni multiplo intero della frequenza base esiste un **coefficiente** per le funzioni seno e coseno. Quindi, rappresentando su un diagramma tutte le frequenze possibili, per ciascuna di esse c'è un coefficiente che ha una certa ampiezza (oppure vale 0). Il diagramma delle frequenze è detto **spettro** (a righe, delle ampiezze, ecc..).
Il numero di **coefficienti** di seni e coseni sommati per rappresentare il segnale originario rappresenta l'accuratezza con cui viene riprodotto il segnale. Se un mezzo di trasmissione consente il passaggio di solo alcune bande di frequenze, allora solo alcuni dei coefficienti che rappresentano il segnale originale secondo Fourier potranno essere utilizzati: ciò fa perdere in accuratezza, ma se si tratta di rappresentare segnali binari, ovvero 0 ed 1, allora anche con poche frequenze è

possibile ricostruire il segnale originale.

UTP Unshielded Twisted Pair

Sono cavi non schermati che rappresentano l'evoluzione dei doppini semplici.
Sono composti da quattro coppie di doppini intrecciati inseriti in una guaina di teflon. Ogni cavo è isolato. Un cavetto UTP termina con un connettore RJ45 a 8pin che va inserito in una adeguata presa.
Rumore e attenuazione: la potenza permette di fare un percorso che dipende:

- Dalla classe del cavo.
- Dalla tolleranza del rumore elettromagnetico.

Lo standard TIA/EIA568 raccomanda una lunghezza dei cavi UTP non superiore ai 100 metri; TIA/EIA (Telecommunications Industry Association/Electronic Industrial Alliance) cooperano per proporre gli standard che riguardano I mezzi di trasmissione negli USA. Se questo limite viene osservato difficilmente ci saranno errori dovuti a rumore e propagazione. Si tratta di una soluzione basata su tecnologie semplici a basso costo, ma funziona molto bene.
I doppini riducono le interferenze elettromagnetiche (EMI) esterne perché le interferenze crosstalk tra i due cavetti interferiscono a vicenda eliminandosi quasi completamente. Alla fine i cavi non sono intrecciati e qui intervengono due semplici regole che ci dicono:

- Limitare la distanza a 100 metri per controllare I problemi dovuti a rumore e attenuazione.
- Non srotolare i cavi prima del connettore per una lunghezza superiore a 1.25 cm per controllare l’interferenza crosstalk terminale. Se queste regole sono strettamente osservate i problemi dovuti alla propagazione sono irrisori.

Lo strato Datalink

Introduzione

Lo strato datalink fornisce algoritmi e protocolli per la trasmissione dei dati e la correzione o rilevazione degli errori di trasmissione.
Siano A e B due macchine adiacenti connesse attraverso un canale di comunicazione (un mezzo fisico qualunque tra quelli analizzati nel precedente capitolo) che dialogano sullo strato datalink. La macchina A invia i dati a B bit a bit, uno alla volta, in sequenza rapidissima; B li preleva. Purtroppo qualunque mezzo di trasmissione è soggetto a disturbi, perdite di segnale, rumore, ecc..
Inoltre è sempre presente un tempo di propagazione del segnale, per quanto piccolo. Lo scopo dello strato data link è principalmente risolvere questi tipi di problemi: disturbi e ritardi di propagazione.

Progetto

- Fornire un ben definito servizio di interfaccia verso lo strato superiore, ovvero trasferire dati dallo strato network di A allo strato network di B;
- Gestire gli errori di trasmissione;
- Regolare il flusso dati in modo che i dispositivi riceventi lenti non vengano intasati da chi trasmette velocemente;

Lo strato datalink prende pacchetti di dati dallo strato network e li inserisce in un frame prima di trasmetterli. Ogni frame contiene una intestazione (header), il pacchetto da trasmettere ed una coda (trailer).

Header + pacchetto + Trailer

Servizi forniti allo strato network

- **Servizio unacknowledged senza connessione**: A invia a B dei frame indipendenti senza che B debba inviare un messaggio di conferma (acknowledgement). Se un frame va perso non viene effettuato nessun tentativo di correzione o recupero (nello strato datalink). Es: traffico voce, streaming video,...
- **Servizio acknowledged senza connessione**: non usa nessun tipo di connessione logica ma invia il segnale di conferma in modo che A sia sicuro che B ha ricevuto il frame. Es: reti wireless, ...
- **Servizio acknowledged orientato alla connessione**: il trasferimento avviene in tre fasi:
  - si stabilisce la connessione inizializzando contatori e variabili per tenere traccia dei frame ricevuti ed inviati;
  - trasmissione dei frame;

- chiusura della connessione e rilascio delle risorse riservate.

L'acknowledgement è sempre implementabile anche a livelli superiori, magari incaricando lo strato network di chiedere l'ack dei pacchetti. Se l'ack non arriva entro un certo tempo, lo strato network può richiedere il re-invio di tutto il messaggio.
IMPORTANTE: i frame hanno una grandezza fissa imposta dall'hardware (router, switch, hub, ecc..), mentre i pacchetti dello strato network no. Il pacchetto viene tipicamente spezzato in tanti frame e trasmessi uno alla volta. Se si perde il 20% dei frame a causa del rumore, può essere necessario molto tempo per trasmettere un pacchetto. Se invece i frame vengono numerati e confermati individualmente a livello datalink, i pacchetti vengono trasmessi molto più velocemente.

Suddivisione in frame

Per servire lo strato network lo strato data link deve sfruttare il servizio fornito dallo strato fisico sottostante, ovvero la trasmissione di un singolo bit alla volta (è possibile trasmettere più bit alla volta codificandoli con vari li velli di tensione elettrica ma supponiamo sempre x semplicità che venga inviato un bit alla volta lungo il canale).
Il flusso di bit può contenere errori ed il compito dello strato datalink è di rilevarli e correggerli. Allo strato network non devono arrivare pacchetti corrotti.
Checksum: algoritmo che, a partire dal frame da trasmettere, fornisce in output una sorta di firma che viene allegata al frame da trasmettere. Alla ricezione il checksum viene ricalcolato su ciò che si è ricevuto e confrontato con il checksum allegato al frame: se coincidenti il frame è corretto.
Per suddividere i pacchetti in frame si sono usate varie tecniche:

- divisione temporale: intervallo di tempo tra due trasmissioni (non in uso)
- conteggio dei caratteri: il primo dato trasmesso indica la lunghezza del frame (non in uso)
- flag byte con byte stuffing: una apposita sequenza marca inizio e fine del frame. la la stessa sequenza occorre nei dati la si marca con una sequenza di bit di escape. lo strato data link rimuove i bit di escape.
- flag bit e bit stuffing: ogni 5 uno consecutivi viene inserito uno zero: questa sequenza delimita i frame.

Anche più di uno di questi metodi possono essere usati per suddividere i pacchetti i n frame.

Controllo degli errori

Per assicurare l'affidabilità dell'arrivo dei dati è necessario dare a al ricevente una qualche forma di reazione per segnalare lo stato della ricezione. Chi riceve può mandare indietro speciali sequenze di controllo delle acknoledgement, positive o negative. E' possibile che a seguito di picchi di rumore interi frame vadano completamente persi, per cui chi riceve non risponderà mai nulla. In questo caso chi trasmette potrebbe aspettare per sempre, a meno che non sia previsto un timer. Se dopo il tempo necessario all'invio del frame ed al conseguente ritorno del l'ack non è arrivata nessuna risposta il timer scatta e fa richiedere la ritrasmissione del frame. SE in vece viene perso solo l'ack di

risposta, il frame ritrasmesso potrebbe essere ricevuto 2 o più volte dallo strato data link del destinatario e passato allo strato network. E' necessario quindi numerare i frame in modo che la destinazione riesca a distinguerli.

Controllo di flusso

Cosa fare quando la sorgente A trasmette in modo molto più veloce di quanto B non riesca a ricevere? Anche se la trasmissione non presenta errori, si arriverà ad un certo punto in cui la destinazione sarà sommersa ed incapace di trattare i messaggi in arrivo.

- Controllo di flusso tramite feedback: la destinazione manda indietro alla sorgente delle informazioni per darle il premesso di mandare altri dati o per informarla sul suo stato
- Controllo di flusso tramite limitazione della velocità: il protocollo contiene meccanismi che limitano la velocità di trasmissione, sincronizzandosi con il destinatario.

Rilevazione e correzione degli errori

- **Codifica a correzione di errore**: nel blocco trasmesso si introducono informazioni supplementari ridondanti che consentono non solo di rilevare ma anche di correggere un errore. Su canali molto rumorosi, come il wireless, conviene utilizzare questa tecnica, poiché il ritrasmettere tutto degraderebbe troppo la qualità del servizio e non sarebbe comunque garanzia di non avere errori alla successiva ritrasmissione.
  - codifiche di Hamming
- **Codifica a rilevazione di errore**: viene introdotta una ridondanza sufficiente a rilevare ma non a correggere un o più eventuali errori. Su canali molto veloci, come le fibre ottiche, questa è la strada preferita.
  - CRC, codifica polinomiale

Protocolli datalink elementari

Gli strati fisico, datalink e network sono costituiti da **processi** indipendenti che comunicano scambiandosi dei messaggi l'un l'altro.

- Strato fisico e data link sono eseguiti da speciali chip integrati nelle schede (di rete, degli switch, ecc.. hardware dedicato insomma).
- Lo strato network gira sulla CPU principale.
- A vuole inviare a B una consistente quantità di dati con un servizio affidabile e orientato alla connessione.
- Gli strati datalink non si preoccupano di crash dei computer a cui forniscono servizi.

All'inizio A non ha niente da fare, attende che succeda qualcosa. Quando lo strato datalink di A riceve un pacchetto lo incapsula in un frame (eventualmente spezzandolo in più parti ed inviando più frame) aggiungendo una intestazione (**header**) ed una coda (**trailer**) ed invia alla macchina B.
Quando il frame arriva a destinazione viene calcolato il checksum, ed eventualmente viene ritornato un errore. Se il frame è integro invece, vengono controllate le intestazioni e si passa il messaggio allo strato network, privato delle intestazioni iniziali e finali del frame.

Il motivo per cui strato lo strato network non deve vedere ne header ne trailer è poiché questi due strati devono essere indipendenti e sostituibili con tecnologie differenti in qualunque momento.
Un frame è composto da 4 campi: **kind, seq, ack e info**. I primi tre contengono le informazioni di controllo, l'ultimo i dati.
Kind descrive il tipo di dati contenuti, cioè se sono informazioni di controllo come un acknowledgement oppure un pacchetto.
Seq e **ack** si usano per i descrivere la sequenza di frame e per l'acknowledgement.
Info contiene i dati da inviare.

Esempi di trasmissione

A trasmette a B in una sola direzione (trasmissione simplex o half-duplex):

- preleva un pacchetto dallo strato network
- scompone il pacchetto in parti
- numera queste parti (in particolare distingue il frame attualmente in trasmissione dal successivo)
- instrada il frame sulla porta giusta
- lo strato fisico trasporta il frame allo strato fisico di B e da lì passa allo strato data link
- vengono effettuati i controlli di integrità
- B invia un acknowledgement ad A
- A attende l'ack di B prima di trasmettere il successivo frame (protocolli **stop-and-wait**) per non intasare B
- se i canali sono rumorosi i frame possono andare perduti, sia che siano dati che siano ack di risposta
- servono due oggetti:
  - un timer che attende l'ack di risposta: se A non riceve conferma da B, reinvia il frame. Ma se si perde l'ack di risposta viene inviato frame duplicato.
  - un modo per numerare i pacchetti: se A trasmette un frame duplicato (poiché ha perso l'ack), B scarta il duplicato in arrivo poiché non ha il numero di sequenza corretto.

Per avere una trasmissione dati full-duplex sono necessari due canali half-duplex, uno per l'invio dei dati da A a B, l'altro per le risposte da B ad A. In questo modo tuttavia si spreca la banda in ritorno (gli ack sono sempre molto più piccoli dei pacchetti da trasmettere). Un altro modo è trasmettere simultaneamente su entrami i canali ed agganciare gli ack di risposta di B sui frame che B invia ad A (**piggy-backing**).

Lo strato datalink in Intemet

Internet consiste in una serie di macchine individuali (host e router) e nell'infrastruttura che le connette. Dentro ad aziende ed edifici si usano spesso LAN, mentre tutto il resto dei collegamenti è fatto da linee punto-punto dedicate.
Struttura tipica: LAN costituite da tanti host, collegate mediante uno o due router ad altri router remoti. Il **backbone** è la LAN (spina dorsale) che collega i router tra loro. Tanti backbone sono collegati tra loro da router. Questi router e le linee

che li collegano costituiscono Internet.
Internet utilizza il protocollo datalink PPP per i collegamenti punto-punto che gestisca il framing, il controllo degli errori e le altre funzioni descritte finora.

PPP (Point to Point Protocol)

- Metodo di framing che delimita in modo non ambiguo la fine e l'inizio di un frame.
- Protocollo per gestire la linea, negoziare le opzioni di collegamento e di disconnessione (**LCP**).
- Negoziazione delle opzioni per dialogare con molteplici varietà di strati Network (**NCP**).

A si vuole connettere: aziona un modem e chiama un modem del router B del proprio ISP (Internet Service Provider). Stabilita una connessione e definita una velocità di trasmissione dati compatibile con il rumore della linea, A manda a B dei pacchetti LCP e NCP dentro a dei frame PPP per negoziare il tipo di trasmissione. B assegna ad A un indirizzo IP. A è connesso ad internet.

ATM - Asynchronous Transfer Mode

Asynchronous Transfer Mode, o ATM è un **protocollo di rete a commutazione di cella** che incapsula il traffico in celle a lunghezza fissa (53 byte) invece che in pacchetti a lunghezza variabile come nelle reti a commutazione di pacchetto (IP o Ethernet).
ATM è stata progettata agli inizi degli anni '90 e lanciata con una fortissima spinta in quanto avrebbe dovuto soddisfare le esigenze di networking unificando voce, dati, TV via cavo, telex, etc. in un sistema integrato.
ATM è stato pensato per fornire uno standard unificato di rete per supportare canali sincroni (SDH) e reti basate su pacchetti (IP, Frame relay, etc), gestendo contemporaneamente livelli multipli di qualità del servizio per il traffico.
ATM non ha avuto il successo sperato, tuttavia è stata adottata nella rete telefonica dove il suo utilizzo è tuttora in espansione (ADSL, UMTS).
L'unità di trasmissione dei dati di ATM è detta **cella**, ed ha una dimensione fissa di **53 byte**, di cui 48 di payload (corpo) e 5 di header.
ATM utilizza una tecnica di **commutazione a circuito virtuale**: prima di inviare i dati si invia un pacchetto di handshake per configurare la connessione. Man mano che questo pacchetto attraversa gli switch, questi calcolano l'instradamento, attribuiscono un identificatore ai pacchetti di questa connessione, e riservano risorse per la connessione. D'ora in poi, tutti i pacchetti della connessione seguiranno lo stesso percorso.
Le celle successive verranno identificate sulla base di un'**etichetta**. Quando una cella raggiunge uno switch, questo dovrà consultare una tabella indicizzata da porta in ingresso ed etichetta, ricavando la porta di uscita e la nuova etichetta da assegnare alla cella. Questa architettura molto semplice facilita l'instradamento in hardware, permettendo di realizzare switch ad alta velocità.
L'etichetta è composta di due valori presenti nell'header di ciascuna cella: **VPI** e **VCI**:

- Il VPI (Virtual Path Identifier) identifica il path virtuale su cui il circuito virtuale è stato attivato.
- Il VCI (Virtual Connection Identifier) identifica la connessione virtuale su cui il circuito virtuale è stato attivato.

Gerarchicamente si ha che un circuito virtuale viene stabilito tramite il collegamento di più connessioni virtuali VC. Il VP è un canale virtuale gerarchicamente superiore al VC ed infatti un VP può contenere fino a 2^{16} VC. Appositi dispositivi hardware, ad esempio switch ATM, sono in grado di gestire VP (con tutti i VC in essi contenuti) o anche direttamente i singoli VC.
Visto che tutti i pacchetti seguono la stessa strada, è garantita la consegna in ordine, ma non che tutti i pacchetti siano consegnati, perché sono sempre possibili code sugli switch e conseguenti perdite di pacchetti.
La velocità va da 2 Mbps a 622 Mbps, e anche oltre. È questa la velocità adatta alla tv ad alta definizione. ATM, inoltre, consente di segmentare la banda sui diversi canali virtuali per i diversi tipi di servizi di trasmissione appunto tramite l'uso dei VCC (VPI:VCI).
Per supportare varie tipi di traffico su ATM (**Qualità di servizio**), sono stati definiti una varietà di modelli di servizio, che si adattano al traffico telefonico (CBR: banda costante, forti garanzie su banda e ritardo) o a quello IP (VBR: banda variabile, nessuna garanzia).
Sono definiti anche molteplici **strati di adattamento** ("Adaptation Layer"), per permettere il trasporto su ATM di vari tipi di dati.

Trasporto di IP su ATM

Per trasportare traffico IP si usa l'Adaptation Layer 5 (**AAL5**), che segmenta il pacchetto IP in celle. AAL5 prevede dunque la possibilità di segmentare pacchetti di dimensioni variabili fino a 2^16 byte su un numero sufficiente di celle ATM con un overhead minimo. Ogni pacchetto AAL5 è coperto da un CRC. Mentre un pacchetto AAL5 verrà trasmesso su più celle in AAL2 una cella potrà trasportare più pacchetti AAL2.

Il sottostrato MAC

Canali multiaccesso o canali ad accesso casuale

Esistono due tipi di reti:

- quelle che utilizzano connessioni punto-punto, ovvero a tutte le entità connesse arrivano solo i pacchetti davvero ad esse destinati;
- quelle che utilizzano **canali broadcast**, che ricevono tutti i pacchetti del canale broadcast ma che scelgono di NON SCARTARE solo i pacchetti di cui si riconoscono come destinatari.

Dunque i canali broadcast sono risorse condivise da più utenti: un problema chiave è come assegnare il diritto di utilizzare il canale in caso di più richieste simultanee. Se il canale è unico per più utenti, un solo "impulso elettrico" alla volta può essere trasmesso.
I protocolli per assegnare l'uso del canale multiaccesso appartengono ad un sottostrato del livello datalink detto **MAC** (**Medium Access Control**).
Questo sottostrato è importante soprattutto nelle LAN. Nelle WAN invece si trovano quasi esclusivamente canali punto-punto.

Il problema dell'assegnazione del canale

- **FDM** (**Frequency Division Multiplexing**): assegnazione statica del canale in LAN e MAN. Se ci sono (mediamente) N utenti la banda è divisa in N parti uguali e distribuita agli utenti.
  - Problemi:
    - alcuni utenti potrebbero aver bisogno di più banda, mentre altri potrebbero non utilizzare la propria;
    - se ci sono M<N utenti, parte della banda è sprecata;
    - se si aggiungono utenti, alcuni non hanno la possibilità di collegarsi;
- **Assegnazione dinamica del canale**.
  - Ipotesi:
    - ci sono N utenti che hanno accesso al canale broadcast
    - un solo canale assicura la comunicazione
    - due frame trasmessi contemporaneamente si sovrappongono temporalmente e creano una **collisione**, ovvero un segnale elettrico distorto.
    - La trasmissione può iniziare in qualunque istante, cioè non c'è un clock di riferimento a cui sincronizzarsi per dare inizio ad un evento
    - gli N utenti sono in grado di verificare l'occupazione del canale
    - oppure gli utenti sono in grado di verificare posteriormente all'invio di un frame se esso è arrivato con successo oppure no.
  - Verranno analizzati nei prossimi capitoli alcuni modelli dinamici di assegnazione.

ALOHA

Gli N utenti possono trasmettere ogni volta che hanno dei dati da inviare e grazie alle proprietà di feedback della trasmissione broadcast possono, ascoltando il canale, scoprire se la trasmissione ha avuto successo. Se non è possibile ascoltare il canale è necessario n meccanismo di acknowledgement. Se il frame è andato distrutto il trasmettitore resta in attesa un intervallo di tempo casuale prima di ritrasmettere. Ogni volta che due frame tentano di occupare un canale contemporaneamente si verifica una collisione che li danneggia entrambi. E' sufficiente che anche solo il primo bit del secondo frame si sovrapponga all'ultimo del primo.

Slotted ALOHA

Identico al protocollo ALOHA, si differenzia per il fatto che il tempo è suddiviso in intervalli discreti di ampiezza uguale, sufficienti alla propagazione completa del frame lungo il canale. Quando si vuole trasmettere si attende l'inizio del prossimo intervallo. Questo sistema raddoppia la capacità di trasmissione della linea.

CSMA (Carrier Sense Multiple Access) persistente e non persistente

Quando ci sono dei dati da trasmettere, la A prima ascolta il canale per scoprire se qualcun altro in quel momento sta trasmettendo. Se il canale è occupato, la stazione aspetta fino a quando non non si libera. Quando si accorge che il canale è libero manda un frame. In caso si verifichi una collisione, A attende per un periodo id tempo casuale prima di ritentare. E' detto **CSMA 1-persistente** poiché trasmette con probabilità 1 quando trova il canale libero.
Il **ritardo di propagazione** del frame sul canale è importante: finché il segnale (elettrico) non si è propagato su tutta la linea, una stazione B potrebbe ritenere libero il canale e iniziare a trasmettere. Analogamente se due stazioni ascoltano una terza che trasmette, al termine inizierebbero simultaneamente causando una collisione.
CSMA non persistente: la stazione che vuole trasmettere ascolta il canale: se è libero trasmette, altrimenti aspetta un tempo casuale prima di riascoltare il canale.
CSMA p-persistente: (per i canali suddivisi in intervalli temporali) la stazione A controlla il canale: se è libero trasmette con probabilità **p**, oppure rimanda all'intervallo successivo con probabilità **1-p**. Se nel secondo intervallo il canale è libero, ancora o trasmette con probabilità p, oppure rimanda (1-q).
CSMA/CD con rilevamento delle collisioni: in caso di collisione, le stazioni se ne accorgono immediatamente e interrompono subito la trasmissione del frame (a che scopo completarla?) generando un burst di rumore. Il tempo minimo per rilevare una collisione è pari al doppio del tempo impiegato dal segnale per propagarsi da una stazione all'altra.
Un **burst di rumore** è un impulso di intensità maggiore rispetto ai livelli elettrici delle normali comunicazioni che viene inviato nel canale per sottolineare l'avvenuta collisione.

Protocolli LAN wireless

Un sistema di computer portatili in grado di comunicare via radio può essere considerato una LAN wireless.
Configurazione a celle: un edificio con tanti access point, ciascuno con una portata di 7-8 metri. L'insieme degli access point è simile ad una rete cellulare. Quando il client che vuole avere accesso si trova in una zona di interferenza tra due access point, il segnale che riceverà sarà confuso (dato dalla sovrapposizione di due segnali).
Problema della stazione nascosta: il protocollo CSMA non è adatto poiché il luogo ove è importante rilevare le eventuali interferenze è nelle vicinanze del destinatario e non del trasmittente.

A-> B C D A ->B<- C D

A sente B; B è nel campo di trasmissione sia di A che di C. C non sente A.
Se A trasmette a B, C controlla la presenza di trasmissioni in corso nella propria area; non rilevando A crede di poter comunicare con B. C invia a B un messaggio. B è nella situazione di ricevere contemporaneamente sia da A che da B: i due frame si sovrappongono e vanno distrutti.
Problema della stazione esposta: B trasmette ad A. Se C vuole parlare con D, controlla il canale e lo trova occupato, per cui rinuncia a mandare il messaggio.

A <- B ?-C D

Ma se avesse inviato il frame, nella zona attorno a D non vi sarebbero state interferenze, poiché D è fuori dalla zona di B.
Prima di avviare una trasmissione, il trasmettitore ha interesse a sapere se c'è attività attorno al ricevitore. CSMA non lo consente.

MACA e MACAW

(Multiple Access with Collision Avoidance) – il trasmettitore incita il ricevitore a trasmettere un piccolo frame in modo che le stazioni che si trovano nelle vicinanze, rilevando questa trasmissione, evitino di interferire con la trasmissione di un frame più grande. MACAW aggiunge un frame di ack dopo ogni frame trasmesso con successo, altrimenti dei frame non andati a buon fine ci si accorgerebbe solo quando lo strato network, non trovandoli, ne farebbe richiesta (molto tempo dopo).

ETHERNET 802.3

Nome	Cavo	Lunghezza Max	Nodi	Vantaggi
10Base5	Coassiale spesso (thick ethernet)	500 m	100	Cavo originale
10Base2	Coassiale sottile (thin ethernet)	185 m	30	Non occorre un hub
10Base-T	Doppino intrecciato	100 m	1.024	Economico
10Base-F	Fibra ottica	2.000 m	1.024	Il migliore tra edifici

10Base5: cavo grosso, di colore giallo, con innesti per ogni client costituiti da una sorta di spillo che si inserisce nel cavo coassiale fino al nucleo centrale.
10Base2: più facile da piegare, ha connettori BNC che formano giunzioni a T. Economico e semplice da installare, nei punti terminali del cavo necessita di una terminazione a 50 Omh di impedenza, che consente al segnale di rimbalzare e tornare indietro. Difficile identificare quale dei tanti cablaggi è difettoso, per cui si è passati ad una struttura ad HUB.
Hub: concentratore di segnale. Ogni client è collegato ad un hub, il quale semplicemente amplifica e distribuisce i frame ricevuti a tutti i client collegati. Questo schema è chiamato **10Base-T**. Gli hub non elaborano il traffico.
10Base-T non ha cavi condivisi da più client, c'è solo l'hub a cui tutti si collegano mediante un cavo personale. Svantaggi: lunghezza massima dei cavi di 100 metri, se di categoria 5 max 200 metri.
10Base-F usa le fibre ottiche. Più sicuro ma costoso, consente lunghe distanze ed una maggiore velocità di trasmissione.
Ogni versione di ethernet può essere resa più ampia facendo uso di **ripetitori**, che non fanno altro (allo strato fisico) di rigenerare il segnale in input amplificandolo. Introducono dei ritardi. Un sistema ethernet può avere tanti cavi e tanti ripetitori, ma distanza complessiva tra qualunque coppia di client o oggetti collegati non può superare i 2,5 Km e nessun percorso tra client può dover attraversare più di 4 ripetitori.

Frame ethernet

Preamble	destinazione	origine	type	dati	riempimento	checksum

Preamble	S o F	destinazione	origine	type	dati	riempimento	checksum

Ogni frame ethernet inizia con un **preamble** (preambolo) di 8 byte, ognuno costituito da 10101010 che serve a sincronizzare la trasmissione. Poi vi sono 2 indirizzi, **destinazione** e **sorgente**. 6 byte descrivono l'indirizzo. 1 bit è riservato per indicare trasmissioni di gruppo (**multicast**), un bit è riservato per rappresentare trasmissioni **broadcast** (verso tutti). Con 46 bit disponibili si rappresentano circa 7×10^{13} indirizzi globali, ovvero ad ogni client, dispositivo, ecc.. in teoria dispone di un indirizzo che lo identifica univocamente nel mondo. Infatti ogni scheda di rete possiede un cosiddetto **MAC Address**.
Il campo **type** contiene indicazioni su a quale tipo di protocollo dello strato network passare il contenuto del frame (possono essere più di uno).
Il campo **data** contiene, appunto, i dati da trasmettere; è lungo fino a 1500 byte. Come lunghezza minima del frame è stato scelto almeno 64 byte, dal destination address al checksum inclusi, poiché a causa delle collisioni spesso sul canale girano pezzi di dati e bit sparsi. Quindi 64-(6+6+2+X+4) = 0 --> X=46. Se i dati sono inferiori a 46 byte viene usato il campo **riempimento** per arrivare a 64 byte. Il **checksum**, un hash dei dei dati di 4 byte, garantisce l'integrità del frame a livello datalink.
La **lunghezza minima** serve anche come garanzia dalle collisioni. Se ad esempio un frame viene emesso da A, un istante ε prima di arrivare, B trasmette si genera una collisione. Sia τ il tempo che impiega il frame ad attraversare il canale, 2τ è il tempo che impiega il burst generato all'istante τ per arrivare ad A.

Se il frame è molto corto, cioè se la trasmissione dell'intero frame dura meno di 2τ, allora A potrebbe iniziare una seconda trasmissione senza accorgersi della collisione (poiché il burst non è ancora arrivato indietro). Per questo motivo il frame deve essere sufficientemente lungo in modo tale che non sia possibile una tale situazione. In una LAN lunga al max 2500 m e con al max 4 ripetitori un bit impiega al max 50 µsec a fare andata e ritorno. A 10 Mbps un bit viene emesso in 100 nsec. Quindi in 50 µsec vengono emessi 50 [µsec] / 100 [bit/nsec] = 500 bit. per avere più margine si è arrotondato a 512 bit, cioè 64 byte.

L'algoritmo di backoff esponenziale binario

Come viene gestita l'attesa casuale dopo una collisione? Il tempo viene suddiviso in intervalli discreti di durata 2τ. Dopo la prima collisione le stazioni aspettano 1 o 0 intervalli e poi trasmettono. Se al primo tentativo scelgono lo stesso si verificherà una collisione con probabilità ½. A questo punto possono scegliere di aspettare 0, 1, 2, o 3 intervalli, quindi la probabilità è ¼. Con una terza collisione si procede allo stesso modo aspettando tra 0 e 2^i-1 intervalli. Dopo 16 collisioni consecutive il chip rinuncia e va a casa.

Ethernet commutata - SWITCH

Al crescere delle stazioni aggiunte il traffico aumenta e la LAN si satura. Si può aumentare la velocità da 10 a 100 Mbps, ma comunque si raggiungerebbe presto la capacità massima.
Uno **switch** è costituito da una scheda (backplane) ad alta velocità su cui sono innestate da 4 a 32 schede, ciascuna con 8 connettori (**porte**)a cui sono collegati o singoli client oppure altri swtch o porzioni di LAN. Quando una stazione vuole inviare un frame ethernet lo invia allo switch: esso controlla se il pacchetto è destinato ad una delle stazioni di lavoro collegate ad una delle sue porte. In caso positivo lo switch copia il pacchetto solo sulla porta del destinatario, altrimenti inoltra il messaggio sulle porta collegata alla scheda backplane (cioè verso altre sezioni di rete ethernet).
Dominio di collisione. Se due macchine inviano frame nello stesso istante? Dipende da come sono fatte le 4/32 schede dello switch. Ciascuna di esse potrebbe essere assimilata ad una LAN dove vi è un unico canale di trasmissione condiviso per tutti, per cui vale il protocollo CSMA/CD. Tutte le schede possono trasmettere contemporaneamente, ma in ciascuna solo uno degli 8 può occupare il canale. Oppure lo switch può avere un buffer di memoria dove memorizzare i frame per poi inoltrarli. Tutte le porte inviano e ricevono contemporaneamente e non possono esservi collisioni.

Fast Ethernet

Gigabit Ethernet

IEEE 802.2: LLC (Logical Link Control)

Ethernet i protocolli 802.xx offrono un servizio a datagrammi best-effort: un pacchetto IP viene incapsulato in un frame e spedito, se si perde non importa. IEEE ha definito un protocollo datalink con controllo di errore e di flusso, che può

operare sopra ethernet e gli altri protocolli 802 offrendo una interfaccia e un formato unico verso lo strato network. LLC forma la metà superiore dello strato data link, il sottostrato MAC si trova immediatamente sotto.
Lo strato network passa a LLC un pacchetto; LLC aggiunge una intestazione contenente numeri di sequenza e acknowledge. La struttura risultante è inserita nel campo carico utile di un frame 802 che viene poi passato allo strato fisico. Chi riceve fa il procedimento inverso.
LLC offre tre modalità di servizio: datagram inaffidabile, datagram con acknowledge e servizio affidabile orientato alle connessioni.
L'intestazione LLC contiene tre campi:

- access point di destinazione
- access point sorgente
- un campo di controllo

Retrospettiva sul succesSo di Ethernet

Lan Wireless 802.11

Le LAN wireless si possono configurare in due modi: con o senza punto d'accesso alla rete. In 802.11 il sottostrato MAC stabilisce il metodo di allocazione del canale, cioè chi deve trasmettere per primo. Allo strato fisico esistono numerose tecniche di trasmissione operanti in diverse bande di frequenze.

Logical Link Control					
Sottostrato MAC					
Infrarosso 802.11	FHSS 802.11	DSSS 802.11	OFDM 802.11a	HR-DSSS 802.11b	OFDM 802.11g

Il protocollo del sottostrato MAC di 802.11

A causa delle difficoltà che si incontrano nel wireless, il sottostrato MAC è leggermente differente da Ethernet. In ethernet una stazione si limita ad aspettare che il canale diventi silenzioso, poi si trasmette il frame e si attende un eventuale burst di rumore per i primi 64 bit di trasmissione: se non arriva quasi certamente la destinazione ha ricevuto il frame. I problemi della stazione nascosta ed esposta rendono necessarie alcune modifiche. Vi sono due modalità operative: **DCF** (Distributed Coordination Function) e **PCF** (Point Coordination Function). L'implementazione di DCF è obbligatoria.
DCF utilizza un protocollo detto **CSMA/CA** (CSMA Collision Avoidance) che controlla sia il canale fisico che quello virtuale attraverso due modalità operative:

- la stazione controlla se il canale è libero prima di trasmettere; durante la trasmissione la stazione non controlla il canale ma trasmette l'intero frame, che può comunque rimanere danneggiato. Se il canale è occupato la stazione rimanda l'operazione di un tempo casuale finché non lo trova libero. In caso di collisione le stazioni coinvolte rimangono in attesa un tempo casuale poi ritentano.

A -> B C D

- Viene controllata la presenza di un canale virtuale. A vuole trasmettere a B. C sente A. D non rileva A.
  A vuole inviare dati a B e chiede il permesso inviando un piccolo frame RTS. B riceve e può concedere il permesso con un frame CTS. A riceve e fa partire il frame e fa partire un timer per l'acknowledgement. B riceve i dati ed invia l'ack. Se il timer ack scade prima dell'arrivo dell'ack di B il protocollo ricomincia.
  Dal punto di vista di C, egli riceve il frame RTS, vedo di non essere il destinatario e, per il bene della trasmissione, calcola la durata dell'intera procedura e si mette in uno stato denominato **NAV** (Network Allocation Network).
  D non sente il frame RTS, ma sento il CTS, per cui allo stesso modo entra in uno stato NAV.

Le reti wireless sono rumorose ed inaffidabili, per cui la probabilità che un frame arrivi sano a destinazione aumenta al diminuire della grandezza. 802.11 ammette la frammentazione dei frame (ethernet) in parti più piccole, ognuna dotata di un proprio checksum di controllo. I frammenti sono numerati e ricevono un ack individualmente e sono trasmessi con un protocollo del tipo stop-and-wait (successivo invio solo dopo aver ricevuto l'ack per il precedente).
La **frammentazione** aumenta la capacità del canale poiché permette di ritrasmettere solo i frammenti danneggiati e non tutto il frame.
Nella modalità DCF dunque le stazioni competono per il controllo del canale.
In PCF una stazione base sonda le altre stazioni chiedendo se hanno frame da trasmettere e controlla gli ordini di trasmissione di tutti i client connessi, evitando le collisioni.
Con una trasmissione broadcast 10-100 volte al secondo di un frame di segnalazione che contiene i parametri di sistema: sequenze di salto, clock, sincronizzazione, ecc.. Appena una stazione aderisce al servizio di interrogazione riceve una certa porzione di banda.
802.11 gestisce anche il risparmio energetico, importante per dispositivi mobili, a batteria.

Servizi

Lo standard 802.11 definisce 9 servizi che ogni LAN wireless conforme deve fornire: cinque di distribuzione e quattro di servizi stazione.

- **Associazione**. All'arrivo nell'area a portata di una stazione base, un client si annuncia trasmettendo modalità supportate, identità (MAC) e velocità possibili. La stazione base può accettare o rifiutare il nuovo arrivato.
- **Separazione**. Una stazione mobile può lasciare il raggio d'azione della stazione base.
- **Riassociazione**. Una stazione mobile può cambiare l'access point cui è associato.
- **Distribuzione**. Definisce come saranno instradati i frame verso l'access point
- **Integrazione.** Se un frame deve essere trasmesso attraverso una rete diversa da 802.11, questo servizio gestisce la traduzione di formato

Quattro servizi di stazione:

- **Autenticazione**. poiché i dati vengono inviati tutto attorno, solo le stazioni che si autenticano ricevono l'autorizzazione a trasmettere dati. Il

client mobile deve essere accettato nella cella dell'access point. Il client cifra un challenge ricevuto dall'access point e lo invia. Se il risultato è corretto il client mobile è registrato nell'access point.
- **Invalidamento**. Si invalida un client mobile che si allontana dall'access point.
- **Riservatezza**. Le informazioni inviate in 802.11 devono essere cifrate.
- **Trasferimento dati**. 802.11 è modellato sulla base di Ethernet, dunque non è completamente affidabile nella consegna dei dati. Gli strati superiori devono gestire gli errori.

Wireless a banda larga

Bluetooth

Commutazione nello strato Datalink

Più LAN possono essere interconnesse da un dispositivo particolare: il **bridge**.
Esso non esamina il contenuto del frame ma solamente l'indirizzo datalink e instrada di conseguenza il frame; supporta quindi frame di qualsiasi tipo (ATM, Ipv4, ecc..). Vari i motivi per avere più LAN da interconnettere.
- Geografia fisica dei locali ove installare le LAN;
- Sicurezza: più uffici o reparti possono voler essere separati.
- Reggere il carico di lavoro: può essere utile suddividere l'insieme dei client in modo tale che la rete non sia soggetta a congestione.
- Distanza elevata delle LAN;
- Affidabilità: un nodo difettoso può paralizzare una rete a condivisione del canale, per cui i bridge possono essere posti in posizioni chiave.
- Sicurezza: le interfacce di rete consentono, in **modalità promiscua**, di ascoltare tutto il traffico passante sul canale condiviso. Uno o più bridge posizionati opportunamente limitano l'accesso ad informazioni sensibili.

Bridge tra 802.x e 802.y

___A___ -> ___Bridge___ -> __B__

A (terminale mobile wireless 802.11) vuole comunicare con B, che si trova in un'altra LAN, di tipo 802.3 (ethernet). Il pacchetto dallo strato network scende al sottostrato LLC e riceve una intestazione; poi al sottostrato MAC dove viene inserito in un frame. Infine al livello fisico viene trasmesso.
Il bridge riceve il frame, rimuove la struttura 802.11 aggiunta dal sottostrato MAC mantenendo l'intestazione LLC. A seconda del tipo di LAN in cui deve indirizzare il pacchetto, il bridge crea un nuovo datagramma di tipo 802.3 e lo spedisce sulla LAN ethernet.
B riceve il frame 802.3, rimuove le intestazioni MAC, rimuove l'intestazione LLC e passa il pacchetto allo strato network.
Difficoltà:
- ogni LAN utilizza un diverso formato di frame;
- qualunque operazione di copia tra LAN diverse richiede un nuovo calcolo del checksum e una nuova formattazione;

- LAN interconnesse non funzionano necessariamente alla stessa velocità;
- LAN 802.xx adottano diverse lunghezze per i frame (es: il wireless ha frame molto piccoli, ethernet ha lunghezze del frame dipendenti dalla lunghezza dei cavi, ecc..). I protocolli prevedono che un frame arrivi oppure no, ma non che esso possa essere scomposto.
- 802.11 e 802.16 supportano la cifratura allo strato datalink, ethernet no, per cui tali servizi vanno perduti quando il traffico viene instradato da un bridge su una ethernet, oppure ethernet non è in grado di decifrare i dati che riceve.
- ethernet non gestisce la qualità del servizio, al contrario di 802.11;

Internetworking locale

Ethernet dovrebbe funzionare in modo semplice ed economico: attacchi un cavo e tutto funziona. Il bridge trasparente opera in modalità promiscua, cioè accetta ogni frame da ogni rete cui è collegato. Estrae l'indirizzo MAC di destinazione e lo confronta con quelli elencati in una grande tabella (hash) che ha in memoria in cui ogni destinazione conosciuta è associata ad una porta del bridge.
All'inizio la tabella è vuota: il bridge, che non sa dove si trova la destinazione, allarga la ritrasmissione del frame su tutte le porte (flooding) tranne quella da cui il frame è arrivato e memorizza che il mittente è su quella determinata porta. Col tempo i bridge imparano dove sono tutte le destinazioni. poiché le macchine si possono spostare, il bridge annota anche un riferimento temporale nella tabella. Dopo qualche minuto le voci in tabella vengono cancellate.

Ripetitori, hub, bridge, switch, router e gateway

Strato applicazione	Gateway di applicazione
Strato trasporto	Gateway di trasporto
Strato network	Router
Strato data link	Bridge, switch
Strato fisico	Ripetitore, hub

Questi dispositivi operano su strati diversi e a seconda del dispositivo vengono utilizzate informazioni diverse per eseguire la commutazione.
I **ripetitori** lavorano sullo strato fisico, amplificano e ritrasmettono un segnale elettrico lungo una LAN.
Gli **hub** hanno diverse linee in ingresso e i frame in arrivo su una vengono ritrasmessi su tutte le altre. Un hub è un **dominio di collisione**.
Nello strato datalink troviamo **bridge** e **switch**, già analizzati in precedenza.
Lo switch, al contrario del bridge, è soprattutto usato per connettere client, di conseguenza deve contenere molte più schede di linea. Ogni scheda ha un buffer e costituisce un dominio di collisione. Se il buffer esaurisce lo switch inizia a scartare i frame in eccesso. Per attenuare il problema gli switch iniziano ad inoltrare il frame appena è arrivata l'intestazione con l'indirizzo del destinatario.
Il **router** agisce al livello 3: strappa le intestazioni MAC e LLC, ricostruisce il pacchetto e lo inoltra allo strato di software che s occupa dell'instradamento.
Un **gateway di trasporto** funge invece da traduttore tra tecnologie differenti,

modificando i formati secondo necessità.

Router e gateway: per le comunità Internet le due parole significano esattamente la stessa cosa, ovvero un apparato che svolge funzioni di instradamento. Ma non sono esattamente sinonimi. Router enfatizza la ricerca del percorso fisico ed il conseguente instradamento dei pacchetti. Gateway sottolinea la funzione d'interfaccia che il router svolge tra la rete locale e la rete geografica.
Dal punto di vista dell'**ISO**, l'International Organization for Standardization , il router svolge le funzioni definite al livello 3 del modello **OSI** (Open System Interconnet) mentre il gateway si colloca al livello 7. Nella definizione data dall'ISO il gateway mette in comunicazione tra loro sistemi e reti che non hanno nulla in comune, eseguendo tutte le necessarie conversioni di protocollo, di formato dei dati, di linguaggio e di architettura. Si tratta di una applicazione che lavora su un computer che lavora su entrambe le reti e che passa informazioni dall'una all'altra eseguendo le conversioni necessarie.
Esempio: il passaggio di messaggi di posta tra differenti organizzazioni. I gateway convertono indirizzi tra diversi sistemi di indirizzamento, convertono pacchetti da protocolli differenti (POP e IMAP), convertono i formati di codifica (ASCII, UTF-8, ecc..).

LAN virtuali

Lo strato Internet (Network)

Servizi forniti allo strato trasporto

Lo strato network fornisce servizi allo strato trasporto attraverso una interfaccia che soddisfa i seguenti obiettivi:

- i servizi non dovrebbero essere legati alla tecnologia del router;
- allo strato trasporto dovrebbero essere nascosti dettagli quali il numero, il tipo e la topologia dei router;
- gli indirizzi di rete disponibili allo strato trasporto dovrebbero utilizzare uno schema di numerazione uniforme anche attraverso le LAN e le WAN.

Lo strato network dovrebbe fornire o meno un servizio orientato alle connessioni??

La comunità Internet risponde che il lavoro dei router è spostare pacchetti da un punto all'altro, che la sotto rete è intrinsecamente inaffidabile e che dunque gli host dovrebbero accettare questo fatto e provvedere autonomamente alla correzione degli errori. Non si dovrebbe pertanto fornire alcun servizio di ordinamento dei pacchetti ne di controllo del flusso.
Le compagnie telefoniche sostengono invece che il servizio dovrebbe essere orientato alle connessioni e dunque enfatizzare la qualità del servizio.
Sostanzialmente INTERNET contro ATM.
Se il servizio è senza connessione i pacchetti sono inoltrati nella sotto rete individualmente e instradati indipendentemente l'uno dall'altro; non occorre una configurazione anticipata. I pacchetti sono spesso chiamati **datagrammi**.
Se il servizio è orientato alle connessioni, prima di inviare si deve stabilire un percorso che colleghi il router sorgente al router destinazione. Questa connessione è chiamata **CV** (Circuito Virtuale) e la sotto rete è detta **sottorete a circuito virtuale**.

Sottorete a datagrammi

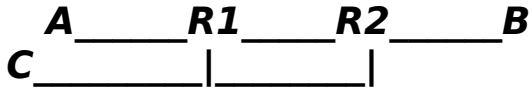
- Un processo su **A** ha un lungo messaggio per **B**
- B appartiene ad un'altra sottorete molto distante da A, collegata per mezzo di una “catena” di router (Internet)
- Lo strato trasporto di A aggiunge una intestazione al messaggio e lo passa allo strato network
- Sia il messaggio lungo tre volte la dimensione massima del pacchetto.
- Lo strato network spezza il messaggio in quattro parti, le numera (sottostrato LLC) e invia un pacchetto dopo l'altro al router **R** a cui è collegato.
- Il router R ha una tabella interna che indica dove devono essere indirizzati i

pacchetti diretti ad ogni possibile destinazione.
- Nella tabella vi sono coppie di valori, destinazione – porta da utilizzare.
- non appena i pacchetti raggiungono **R** viene calcolato il checksum per verificare l'integrità, poi viene consultata la tabella e individuata la porta su cui inoltrare, infine il pacchetto è incapsulato un un frame datalink che ha come destinatario il router successivo.

Algoritmo di routing: l'algoritmo che gestisce le tabelle e prende le decisioni di instradamento.

Sottorete orientata alle connessioni (commutazione di etichetta)

Co i circuiti virtuali l'idea è non dover scegliere una nuova strada ogni volta che si deve inviare un pacchetto. Quando viene stabilita una connessione, il percorso dal client sorgente alla destinazione viene archiviata nelle impostazioni del router. Quel percorso è identico per tutte le comunicazioni ed il funzionamento è identico a quello del servizio telefonico.



- A invia un pacchetto a R1, R1 numera la connessione da A e verso R2 con 1.
- R2 riceve da R1 e numera la connessione da R1 e verso B con 1.
- tutto il percorso da A a B è contrassegnato da un 1 e per tutti i pacchetti da A a B si utilizzerà la connessione 1.
- Se C trasmette a B, R1 non può numerare questa connessione sempre con 1, altrimenti R2 non sa con chi sta parlando, se con A o con C. Perciò la connessione da A a R2 (in R1) e da R1 a B (in R2) viene numerata con un 2.

Confronto tra sottoreti a circuito virtuale e a datagramma

Algoritmi di routing

Percorso più breve

Flooding

Algoritmo statico in cui ogni pacchetto in arrivo è inviato a tutte le linee tranne quella in entrata. Questo meccanismo genera potenzialmente infiniti pacchetti duplicati (topologia a mesh con loop infiniti), ma con un contatore che si decrementa al ogni passaggio da un router si limita questo problema. In alternativa si potrebbe assegnare un numero al pacchetto registrandolo su una tabella: se ritorna indietro lo si scarta subito.
Nel **flooding selettivo** il pacchetto viene inviato solo su quelle linee che approssimativamente vanno nella direzione giusta. Nelle applicazioni militari, dove molte cose possono essere danneggiate, questo algoritmo è ritenuto assai valido.

Routing gerarchico

La dimensione delle tabelle di routing cresce proporzionalmente alla dimensione della rete. Una tabella troppo grande può non essere consultabile in tempi accettabili per la qualità del servizio.
Nel routing gerarchico i router sono divisi in regioni: ogni router conosce tutti i dettagli relativi al routing dei pacchetti diretti a destinazioni nella stessa regione ma non sa nulla della struttura interna di altre zone. In tale modo la tabella di routing si accorcia notevolmente; per contro aumentano i passaggi da un router all'altro. Tuttavia è stato calcolato che il numero ottimale di livelli in un routing gerarchico tra N router è uguale a *ln(N)* e che l'aumento medio di lunghezza del percorso è sufficientemente piccolo da essere accettabile.

Principi e criteri generali per il controllo della congestione

Label switching e MPLS

Differenze e connessione tra le reti

Tunnelling

Il protocollo IP

Indirizzi IP

La colla che tiene unito internet è il protocollo sullo strato network **IP** (Internet Protocol). Il suo compito è quello di fornire un servizio di tipo non garantito per trasportare i datagrammi inviati da una sorgente a una destinazione, senza tener conto delle macchine e della presenza di reti intermedie.
Lo strato trasporto prende i flussi di dati e li divide in datagrammi che hanno una dimensione da 64 a non oltre 1.500 byte. il datagramma è trasmesso su Internet, magari frammentato in unità più piccole. A destinazione lo strato network ricostruisce il datagramma e lo passa allo strato trasporto.
I **datagrammi IP** sono costituiti da una intestazione e dallo spazio per il messaggio. L'intestazione ha una parte fissa di 20 byte ed una parte opzionale di lunghezza variabile. La lunghezza dell'intestazione variabile è indicata nella parte fissa (campo IHL). l'intestazione è composta di **parole** (gruppi di bit) di 32 bit, in numero minimo di 5 (cioè i 20 byte).

<table>
<tr><td colspan="2">Version</td><td>IHL</td><td colspan="2">Type of Service</td><td colspan="4">Total lenght</td></tr>
<tr><td colspan="5">Identification</td><td>DF</td><td>MF</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to live</td><td colspan="3">Protocol</td><td colspan="4">Header checksum</td></tr>
<tr><td colspan="8">Source address</td></tr>
<tr><td colspan="8">Destination address</td></tr>
<tr><td colspan="8">Opzioni</td></tr>
</table>

- **Time to live** è il contatore che decrementa ad ogni router che attraversa.
- **DF** e **MF** tengono traccia della frammentazione.
- **Protocol** indica quale processo di trasporto è in attesa del pacchetto

Indirizzi IP

Ogni scheda di rete di host e ogni router di Internet hanno un indirizzo IP: è unico, non possono esistere allo stesso tempo due macchine con lo stesso IP. L'indirizzo è lungo 32 bit storicamente suddivisi in 4 ottetti scritti in notazione decimale da 0 a 255.

- Classe A: da 1.0.0.0 a 127.255.255.255, 128 reti con ciascuna 16 milioni e rotti di host.
- Classe B: da 128.0.0.0 a 191.255.255.255, 16.384 reti da 64 e rotti host.
- Classe C: da 192.0.0.0 a 223.255.255.255, 2 milioni e rotti di reti con 256 host.
- Classe E: indirizzi che iniziano con 1110 riservati al multicast.
- Classe D: indirizzi che iniziano con 1111 riservati a utilizzi futuri.
- i valori 0 (tutti zero) significano “questo host”.
- i valori -1 (tutti uno) significano broadcast su questa rete.
- per questi due ultimi motivi 0 e -1 non sono mai disponibili.
- 127.0.0.0 è l'indirizzo di loopback, ovvero questi pacchetti non escono dal computer ma vengono trattati come pacchetti in arrivo.

Sottoreti

Tutti gli host di una rete devono avere lo stesso numero di rete (es: 130.34.xx.yy è il numero di rete di classe B, xx.yy.132.12 è il numero dell'host).
Come suddividere in modo ottimale il pool di indirizzi a disposizione? Se un'azienda dispone di un indirizzo di classe B ad esempio, ha indirizzi IP per 65.536 client. Se vuole suddividere questi indirizzi facendo uso del sistema tipo classe C potrebbe fare 254 sottoreti (parti della rete) da ciascuna 254 host, ma se questa azienda non avesse 254 filiali con ciascuna meno di 254 computer?
Se avesse 32 filiali ciascuna con 1000 pc? Si possono usare, dei 16 bit che identificano l'host, una parte per numerare la sottorete ed il resto per numerare gli host. ad esempio 6 bit per numerare le filiali e 10 per gli host.
Per implementare le sottoreti è necessario demarcare una separazione tra i bit che identificano la sottorete e i bit per gli host.
La **maschera di sottorete** fa questo compito, ed è notata in decimale (es: 255.255.255.0) oppure con la notazione alternativa /xx, dove xx indica il numero di bit dove sta la separazione.
Gli indirizzi di classe B sono un problema enorme di Internet. Sono stati assegnati con troppa facilità all'inizio, senza prevedere la crescita del sistema. Per la maggior parte delle aziende un pool di indirizzi di classe B da 64.000 host è troppo grande e giace inutilizzato; un pool di classe C (256 host) è troppo piccolo. Se le reti di classe C avessero avuto 10 bit (1.022 host) sarebbe stato perfetto.

NAT (Network Translation Address)

Protocolli di controllo Intemet – ICMP

Il funzionamento di Internet è monitorato attentamente dai router. Quando avviene qualcosa di imprevisto l'evento è comunicato attraverso il protocollo **ICMP**. Sono definiti una dozzina di messaggi ICMP, tra cui:

- DESTINATION UNREACHABLE
- TIME EXCEEDED
- ECHO
- ECHO REPLY
- TIMESTAMP REQUEST e REPLY

I messaggi ICMP vengono incapsulati in un pacchetto IP, poi in un frame ed infine spediti sulla rete verso la destinazione.

Protocolli di controllo Intemet – ARP

L'hardware che opera allo strato data link non sa nulla di pacchetti IP, indirizzi IP e quant'altro accade al piano superiore. Qualsiasi scheda di rete Ethernet, ad esempio, comprende solamente indirizzi MAC a 48 bit.
Ogni produttore di schede Ethernet richiede ad una autorità centrale un blocco di indirizzi e ne mette uno dentro ad ogni scheda di rete che produce. Di fatto ogni scheda di rete è unica.
Ora, ad ogni scheda di rete (collegata in rete) è associato un indirizzo IP unico che la identifica nel mondo. Per le schede che hanno IP locali ovviamente questo non vale, ma non scendiamo in dettagli troppo tecnici che ho fretta, cazzo!
Come fa il livello datalink a capire chi degli indirizzi MAC che conosce è quello specifico indirizzo IP??
Supponiamo che Gilberto voglia spedite un messaggio ad Anacleto: chiede prima al DNS di tradurre “Anacleto” nel corrispondente IP, poi manda un pacchetto broadcast a tutti chiedendo “sei tu questo IP?”. Chi si riconosce in quell'IP, ovvero Anacleto, risponde in modo affermativo allegando il MAC address.
A questo punto Gilberto ha il MAC address e può inviare il pacchetto IP.
ARP (Address Resolution Protocol) è il protocollo utilizzato per fare questa domanda.
Se ti stai chiedendo: “ma i pacchetti broadcast non vengono inoltrati dal router!!” sei molto bravo/a e ancora sveglio, infatti come si fa ad oltrepassare il router con ARP?
Il router potrebbe essere appositamente configurato per farlo, oppure semplicemente l'host potrebbe accorgersi che la destinazione è su una rete remota, per cui passa il pacchetto a chi gestisce le comunicazioni con l'esterno, cioè il router. Il router a sua volta fa lo stesso con un altro router usando eventualmente ARP se non ne possiede l'associazione IP-MAC. E così via fino a destinazione.

Protocolli di controllo Intemet – DHCP

DHCP (Dynamic Host Configuration Protocol) assegna automaticamente un indirizzo IP a chi ne fa richiesta. Con DHCP è possibile anche assegnare manualmente indirizzi IP. Chi ha bisogno di un IP lancia un pacchetto DHCP DISCOVER: il server DHCP rileva e risponde assegnando un IP. Se il server è in

un'altra sottorete è necessario un **agente di inoltro DHCP**. Se il client si disconnette l'IP viene restituito poiché per esso è stabilita una scadenza temporale (**leasing**).

Mobile IP

Lo strato trasporto

Lo strato Applicazione

DNS: il sistema dei nomi di dominio

A causa della ovvia difficoltà a ricordare indirizzi IP per raggiungere persone, macchine e siti web (es: se vuoi scrivermi, ti sarà più facile ricordare giuaniz@gmail.com piuttosto che giuaniz@135.54.233.45) sono stati introdotti nomi ASCII, ovvero in caratteri per separare i nomi propri dagli indirizzi IP.
Tuttavia la rete sa interpretare solo numeri, per cui

La sicurezza nelle reti

Problemi

La sicurezza nelle reti deve fare in modo che:

- intrusi non riescano a leggere o modificare di nascosto messaggi destinati a terzi;
- impedire l'accesso a determinate macchine connesse alla rete o a servizi remoti;
- accertare l'identità di un mittente;
- impedire l'intercettazione durante una trasmissione;
- accertare l'autore di un determinato evento;
- altro....

i soggetti che potrebbero rappresentare un pericolo possono essere persone esterne, tecnicamente molto preparate (hacker) o semplici amatori. Molto più probabile che l'attacco possa avvenire da persone interne, dipendenti o ex dipendenti, o persone di fiducia che tradiscono.

Hacker e luoghi comuni (da wikipedia)

*"Un **hacker** è una persona che si impegna nell'affrontare sfide intellettuali per aggirare o superare creativamente le limitazioni che gli vengono imposte, non limitatamente ai suoi ambiti d'interesse, ma in tutti gli aspetti della sua vita. Un Hacker in senso stretto è colui che associa ad una profonda conoscenza dei sistemi una intangibilità dell'essere, esso è invisibile a tutti eccetto che a sé stesso. Non sono certamente Hacker in senso stretto tutti coloro che affermano di esserlo, in un certo senso gli Hacker in senso stretto non esistono, perché se qualcuno sapesse della loro esistenza per definizione non esisterebbero."*
***Cracker** indica colui che entra abusivamente in sistemi altrui allo scopo di danneggiarli (**cracking**), lasciare un segno del proprio passaggio, utilizzarli come teste di ponte per altri attacchi oppure per sfruttare la loro capacità di calcolo o l'ampiezza di banda di rete.*
***Script kiddie** è un termine che indica un utente con poca cultura informatica che segue semplicemente delle istruzioni o un how-to senza capire il significato di ciò che sta facendo. Spesso viene utilizzato per indicare chi utilizza exploit creati da altri programmatori e hacker.*
***Lamer** è uno script kiddie che utilizza ad esempio trojan per pavoneggiarsi con gli altri e far credere di essere molto esperto, ma in realtà non sa praticamente nulla e si diverte ad arrecare danno ad altri.*
*Un **newbie** (niubbo) è una persona alle prime armi in questo campo."*

Esempi di potenziali nemici

- **Studente**: legge x divertimento le mail degli altri; entra in un router wi-fi non protetto da password.
- **Cracker**: testa sistemi di sicurezza, ruba dati importanti.
- **Uomo d'affari**: spionaggio industriale.
- **Ex-impiegato**: vendetta per il licenziamento.
- **Contabile**: vendetta o ricatto.
- **Agente di borsa**: nega un accordo preso.
- **Commesso**: ruba i dati di carta di credito.
- **Spia**: ruba segreti militari di uno stato nemico.
- **Terrorista**: denial of service su servizi essenziali; paralisi infrastrutture di uno stato.

Tipi di problemi in sicurezza

- **Segretezza**: mantenere informazioni al sicuro da terzi non autorizzati.
- **Autenticazione**: stabilire l'identità del soggetto con cui si comunica.
- **Non ripudio**: autenticare l'autore di una azione.
- **Controllo dell'integrità**: protezione dell'informazione da alterazioni non autorizzate.

Esempi di attacchi comuni

- Virus;
- Sfruttamento della banda e della rete a scopo personale da parte del personale interno;
- Furti di materiale hardware;
- Accessi non autorizzati ad informazioni sensibili da parte di personale interno;
- Attacchi **DoS – Denial Of Service**, ovvero saturazione della capacità di risposta di un servizio (web). Gli attacchi DoS puntano a rendere un sistema inutilizzabile attraverso l'invio simultaneo di grandissime quantità di richieste, tipicamente sfruttando una vasta rete di computer-zombie sui quali un virus esegue richieste al server bersaglio. Il server è strutturato per essere in grado di rispondere ad un massimo M di richieste: se M viene superato la qualità del servizio peggiora fino a rendere il server inutilizzabile.
- Intrusione in un sistema informatico da parte di attaccanti esterni;
- Sabotaggio di sistema informatico;
- Frodi, truffe informatiche (phishing), furto di codici di carte di credito;
- Furto di informazioni industriali riservate;
- eccc….

Crittografia

Crittografia: scrittura segreta.
Cifrario: una trasformazione carattere per carattere (o bit per bit), senza considerare la struttura linguistica del messaggio.
Codice: rimpiazza ogni parola con un'altra o con un simbolo. Es: la lingua navajo utilizzata dai militari americano durante la seconda guerra mondiale, contro il Giappone.
Cifratura a chiave simmetrica: due persone sono in possesso della stessa

chiave segreta, che serve a cifrare e a decifrare il messaggio. I messaggi da cifrare, detti testo in chiaro, sono trasformati da una funzione parametrizzata dalla chiave. L'output del processo di cifratura è il testo cifrato che viene tramesso al destinatario. Un eventuale intruso, che non conosce la chiave segreta, può o ascoltare il messaggio trasmesso (**intruso passivo**) o tentare di alterarlo (**intruso attivo**). Un intruso che è in possesso della chiave segreta può ascoltare, decifrare ed inviare altri messaggi differenti cifrati con la stessa chiave.

$$P = \text{messaggio in chiaro}$$
$$C = E_k(P) \quad \text{(messaggio cifrato)}$$
$$K = \text{chiave segreta}$$
$$P = D_k(C) \quad \text{(decifrazione)}$$

Criptoanalisi: l'arte di decriptare i messaggi cifrati.
Crittologia: l'arte di inventare sistemi di cifratura.
Decifrare: operazione legittima di lettura di un messaggio cifrato.
Decriptare: decifrazione da parte di un criptoanalista.
Principio di Kerckhoff: tutti gli algoritmi devono essere pubblici, solo le chiavi sono segrete. La mancanza di segretezza per l'algoritmo di cifratura è fondamentale poiché pubblicizzando l'algoritmo il crittografo ottiene gratuitamente la consulenza di un gran numero di esperti accademici. Inoltre, credere di avere un algoritmo sicuro mentre invece esso non lo è, produce più danno che vantaggi.
La **chiave** è una stringa relativamente corta che identifica una particolare cifratura tra molte possibilità. Una chiave binaria a 3 cifre dà 2^3 possibilità = 8. Una chiave a 128 cifre dà $2^{128} = 3 \times 10^{38}$ possibilità diverse. Un computer 1.024 processori in grado di testare una chiave per millisecondo impiegherebbe 9,5 x e^{27} anni per eseguire una ricerca su tutto lo spazio delle chiavi. Quel giorno probabilmente non esisterà nemmeno più la Terra. Più lunga è la chiave, più lungo è il **fattore lavoro** necessario a decifrare.
Cifrario a sostituzione: ogni lettera o gruppo di lettere viene sostituito da altre. Es: A -> F, T -> L, ecc.. **Sostituzione monoalfabetica**: sostituzione carattere a carattere. L'attacco è di tipo statistico, ovvero poiché in ciascuna lingua certe lettere occorrono più frequentemente che altre, si può procedere per tentativi ed ipotesi associando le lettere più frequenti del testo cifrato e dell'alfabeto della lingua in esame.
Cifrario a trasposizione: il testo viene ordinato in una matrice ed una chiave serve a rimescolare le colonne. perdendo l'ordine delle lettere il messaggio non avrà più alcun senso. L'attacco verifica se le frequenze relative dei caratteri cifrati corrispondo a quelle normali del testo in chiaro. Successivamente di fanno ipotesi sul numero di colonne e si procede per tentativi, ipotizzando anche possibili parole che potrebbero essere contenute nel testo.

Blocchi monouso

Un semplice cifrario impossibile da decriptare.

- Si prende una chiave di bit generati a caso.
- Si converte il messaggio in formato binario.
- Si calcola uno XOR delle due stringhe.

Non è possibile un attacco statistico poiché il valor medio degli 1 e 0 è del 50%,

dunque non è possibile individuare sequenze di bit più frequenti. E' impossibile decifrarlo poiché non contiene alcuna informazione: con eguale probabilità, qualunque possibile tipo di messaggio (testo, audio, video, ecc...) è contenuto nella stessa stringa di bit.
Svantaggi:

- la chiave deve essere in possesso sia del mittente che del destinatario;
- la chiave deve essere lunga quanto il messaggio (se devo decodificare un dvd, devo avere un altro dvd contenente la chiave, gulp!!)

Due principi crittografici

- I messaggi devono contenere **ridondanza**: il destinatario, dopo aver decifrato il messaggio, deve poter stabilime la validità. Per stabilire la validità del messaggio è necessario aggiungere informazione al messaggio base in modo tale da consentire un controllo (hash). Un intruso attivo potrebbe infatti modificare alcuni bit del messaggio i quali, decifrati, possono comunque avere un significato coerente, ma errato, per il destinatario.
- **Attualità**: sono necessari dei metodi per prevenire gli attacchi di tipo ripetizione. Un intruso attivo potrebbe catturare i messaggi ed inviare al destinatario messaggi (validi) vecchi. Inserendo un timestamp (cifrato) si ha garanzia dell'attualità del messaggio.

Algoritmi a chiave simmetrica

L'idea attuale è di utilizzare algoritmi estremamente complessi ed involuti, per fare in modo che il possesso della chiave sia sempre necessario e che non sia praticamente possibile compiere una analisi differente nel messaggio. Gli algoritmi a chiave simmetrica codificano blocchi di bit del messaggio usando funzioni molto complesse parametrizzate dalla chiave di cifratura. Una tecnica comune è la permutazione dei bit, secondo uno schema indicato dalla chiave. Una cascata di permutazioni è detta **cifrario prodotto**. Algoritmi di questo tipo sono molto veloci da applicare ai messaggi. Hanno lo svantaggio che uno stesso testo in chiaro, una volta cifrato, produce sempre lo stesso testo cifrato in output, e questo fatto è la base per l'attacco di decriptazione.
Esempi:

- DES (Data Encryption Standard)
- DES triplo
- AES (Advanced Encryption Standard)
- Rijndael

Algoritmi a chiavi pubblica e privata

Un sistema crittografico a chiave simmetrica diviene inutile quando viene sottratta la chiave segreta. In ogni caso, tale chiave deve essere comunicata, in un certo momento, tra i due soggetti che devono scambiare informazione. Il sistema a doppia chiave, pubblica a privata, elimina il problema di scambio delle chiavi.
Ciascun utente possiede due chiavi, una pubblica distribuita a chiunque ne faccia richiesta, l'altra privata da mantenere assolutamente segreta. L'algoritmo è pubblico.

P = messaggio in chiaro
A = chiave pubblica del destinatario
B = chiave privata del destinatario
C = $E_A(P)$ (messaggio cifrato con chiave A)
P = $D_B(C)$ (decifrazione con chiave B)

Il metodo soddisfa queste tre proprietà:
- D(E(P)) = P, ovvero il metodo di decifratura D() è l'inverso del metodo di cifratura E();
- è estremamente difficile dedurre la chiave A dalla chiave B;
- omessa;

RSA

Si scelgono due numeri primi molto grandi, *p* e *q*.
- ***p***, ***q*** grandi almeno da dover essere rappresentati da 1024 bit;
- ***n = p * q***
- ***z = (p – 1) * (q – 1)***
- si sceglie ***d*** in funzione di ***z***;
- si trova ***e*** tale che ***e * d = 1 mod z***

Per cifrare (**chiave pubblica**) si utilizza la coppia di valori (***e;n***), per decifrare (**chiave privata**) si utilizza la coppia (***d;n***).
La sicurezza è data dal fatto che è molto difficile fattorizzare numeri molto grandi, soprattutto se sono il prodotto di due numeri primi.
Con un computer che elabori una chiave ogni msec ed il miglior algoritmo disponibile, per una chiave di 500 cifre sarebbero necessari circa 10^{25} anni.

Distribuzione a chiave pubblica di chiavi simmetriche

Gli algoritmi a chiavi pubbliche e private sono molto sicuri ma altrettanto lenti, per cui non è possibile sfruttarli per scambi di dati cifrati in tempo reale (o quasi). Quello che normalmente avviene, ad esempio durante una sessione di http sicuro, è una comunicazione iniziale di una chiave simmetrica cifrata con chiave pubblica, successivamente tutte gli scambi di informazione avvengono mediante cifratura a chiave simmetrica. Queste sessioni hanno durata limitata, oppure di tanto in tanto viene modificata automaticamente la chiave simmetrica, poiché un attaccante potrebbe tentare un attacco brute force per scoprire la chiave simmetrica.

Firme Digitali

Devono valere le seguenti condizioni, a protezione sia del destinatario che del mittente:
- il destinatario può verificare l'identità dichiarata dal mittente;
- il mittente non può ripudiare in secondo tempo il contenuto del messaggio;
- il destinatario non può falsificare il messaggio del mittente;

Firma a chiave simmetrica: una autorità centrale conosce tutti e tutti ne hanno fiducia (BigBrother). Questa fiducia incondizionata può essere un problema (BB sa tutto di tutti, quindi perché fidarsi di BB?).
- Alice viene autorizzata da BB mediante una chiave segreta K_A, consegnata di persona, dopo la verifica dell'identità.

- Anche Bob è registrato.
- Alice vuole parlare con Bob, manda a BigBrother $\mathbf{K_A(B, R_A, t, P)}$ dove **t** è un timestamp (marca temporale per garantire l'attualità), $\mathbf{R_A}$ è un numero a caso, **P** è il messaggio in chiaro.
- BigBrother riceve e verifica l'identità di Alice.
- BigBrother invia a Bob $\mathbf{K_B(A, R_A, t, P, K_{BB}(A, t, P))}$

Firma a chiave pubblica: viene evitato il passaggio da BigBrother.

- Sia $\mathbf{E(D(P)) = D(E(P)) = P}$, dove E() codifica e D() decodifica;
- Alice invia a Bob $\mathbf{E_B(D_A(P))}$, ovvero Alice codifica con la propria chiave privata il messaggio, poi lo codifica nuovamente con la chiave pubblica di Bob.
- Bob riceve e prima decifra con la propria chiave privata, poi decifra con la chiave pubblica di Alice, ovvero applica $\mathbf{D_B(E_A(P))}$.

Message Digest: non sempre la segretezza è richiesta, mentre lo è l'autenticazione. La funzione di ***hash MD()*** fornisce quattro proprietà:

- dato P, è facile calcolare MD(P)
- dato MD(P) è quasi impossibile trovare P
- dato P, non si può trovare P' tale che MD(P') = MD(P)
- se l'input cambia anche solo di un bit, l'output diventa completamente differente.

Inoltre:

- Si usano chiavi hash di almeno 128 bit
- l'hash è più veloce da calcolare rispetto ad una chiave pubblica.

All'interno di uno schema con firma digitale simmetrica, per autenticare l'autore del messaggio, Alice invia il messaggio P a BigBrother codificato con $\boldsymbol{K_A(A, t, P)}$. Big Brother invia P in chiaro e lo firma con $\boldsymbol{K_{BB}(A, t, MD(P))}$. In caso di contestazione, Bob mostra sia P che $K_{BB}(A, t, MD(P))$; BigBrother decodifica e trova A come mittente, t come tempo, MD(P) come hash. Poiché non si può trovare P' tale che MD(P') = MD(P), allora certamente Alice ha inviato P a Bob.

MD5 e SHA-1: le più note ed utilizzate funzioni di message digest. Mescolano i bit in ingresso in modo tale che ogni bit in ingresso sia in grado di alterare vistosamente l'output.

Una firma sicura può essere:

- Alice calcola SHA-1 di P, lo cifra con la propria chiave privata: [$\boldsymbol{P; D_A(SHA\text{-}1(P))}$]
- Bob riceve: poiché Trudy non può trovare P' tale che abbia lo stesso hash, Bob si può sempre accorgere di eventuali alterazioni.
- Bob calcola $\boldsymbol{E_A(D_A(SHA\text{-}1(P))) = SHA\text{-}1(P)}$
- Bob calcola l'hash del P ricevuto: $\boldsymbol{SHA\text{-}1'(P)}$
- Confronta i due hash, se $\boldsymbol{SHA\text{-}1'(P) = SHA\text{-}1(P)}$ allora è tutto ok.

Gestione delle chiavi pubbliche

Come pubblicare le chiavi pubbliche? Come scambiarle tra persone che non si conoscono? Su un sito web non è sicuro, poiché se Alice cerca la chiave pubblica sul blog di Bob (es www.bob.blogspot.com), Trudy potrebbe intercettare la comunicazione tra il client di Alice ed il server DNS incaricato di tradurre il nome di dominio nel corrispondente indirizzo IP e sostituire la pagina con una fasulla.

Certification Authority: organizzazione autorizzata a rilasciare certificati che associano persone fisiche o giuridiche ad una chiave pubblica. I certificati

rilasciati hanno una scadenza temporale. La CA esegue l'hash SHA-1 del certificato e lo cifra con la propria chiave privata $D_{CA}(SHA\text{-}1(certificato))$. In questo modo chi vuole verificare il certificato possiede o recupera in modo sicuro la chiave pubblica di CA, decifra l'hash e lo confronta con l'hash del certificato distribuito online: se sono uguali e tutto a posto.
Ovvero:

- Bob calcola: $E_{CA}(D_{CA}(SHA\text{-}1(certificato))) = SHA\text{-}1(certificato) = H;$
- Bob calcola: **SHA-1(certificato trovato sul sito)** = **H'**
- Se $H = H'$ è tutto ok;

Revoche dei certificati

Il certificato può essere revocato se:

- l'intestatario ne ha abusato in qualche modo vietato;
- se la chiave privata è stata esposta o rubata;
- se la chiave privata della CA è stata compromessa (grave!).

Ogni CA periodicamente emette una Certificate Revocation List – CRL contenente il numero di serie di tutti i certificati revocati.
Un utente che sta per usare un certificato altrui dovrebbe controllare che esso non sia stato revocato, sia prima che dopo averlo utilizzato (poiché tra la verifica e l'uso potrebbe essere stato revocato). Più i certificati hanno vita lunga, più le CRL sono lunghe (da interrogare): si fanno o delle suddivisioni in directory oppure si ha una lista principale e tanti piccoli aggiornamenti frequenti.

Sicurezza nelle comunicazioni - IPsec

La sicurezza in internet può essere implementata in molti dei livelli disponibili. Alcuni esempi

- Livello applicazione: password database, PgP, applicazioni firewall;
- Livello trasporto: SSL, Firewall sui pacchetti;
- Livello Internet: Ipsec, Firewall;
- Livello Data Link: PPTP. L2TP
- Livello fisico: blocchi fisici sui computer, criptaggio dati sul computer.

Avere politiche di sicurezza su più livelli significa ottenere maggiore protezione, tuttavia comporta maggiore lentezza a causa delle elaborazioni aggiuntive. Si consiglia di avere sistemi di protezione su almeno due livelli.
Una visione della sicurezza presuppone che agli utenti non capiscano cosa sia la sicurezza e che non sono in grado di utilizzarla correttamente. In questa ottica è compito dello strato internet cifrare o autenticare i pacchetti; questo non impedisce agli utenti orientati alla sicurezza di operare in modo più sicuro.
Ipsec – RFC 2401
E' un progetto che fornisce diversi servizi orientati alla segretezza, all'integrità dei dati e alla protezione da attacchi di tipo ripetizione; viene usata cifratura a chiave simmetrica. Ipsec è indipendente dall'algoritmo di cifratura, che può essere sostituito. Ipsec è orientato alla connessione (**SA** – Security Association), anche se si trova allo strato IP: c'è uno scambio di chiave da impiegare per una sessione di scambio di pacchetti.
Vengono modificati i pacchetti da trasmettere aggiungendo due nuove intestazioni per l'identificatore di sicurezza, i dati per il controllo dell'integrità e altre informazioni. (CONTINUA...)

Protocolli di autenticazione

Autenticazione: tecnica utilizzata dai processi per verificare che la loro controparte nella comunicazione sia veramente chi dice di essere, assicurare l'identità del processo con cui si sta comunicando.
Il modello generale prevede che un soggetto, Alice, invii un messaggio ad un destinatario, Bob, oppure ad una terza persona fidata KDC (Key Distribution Center). Poi vengono scambiati molti altri messaggi, che possono anche essere intercettati o modificati. Ala fine del processo, tuttavia, Alice è certa di parlare con Bob e cifrano i prossimi messaggi mediante una chiave (simmetrica) detta **chiave di sessione**.

Autenticazione basata su un segreto condiviso. MS-CHAP Challenge Handshake Autentication Protocol

- A, B = Alice, Bob
- T = Trudy, intrusa
- A e B abbiano una chiave condivisa K_{AB}
- R_i siano le richieste (i = A,B)
- K_i siano le chiavi (i = A,B)
- K_s sia la chiave di sessione

Descrizione dei passi del protocollo

- Alice invia a Bob la sua identità A
- Bob non sa se parla con Alice o con Trudy
- Bob crea un numero casuale grande R_B che invia ad Alice (il ***challenge***)
- Alice cifra R_B con la chiave condivisa: $K_{AB}(R_B)$
- Bob riceve il messaggio e sa che arriva da Alice poiché Trudy non conosce la chiave K_{AB}
- Poiché R_B è molto grande è improbabile che Trudy possa riciclarne uno vecchio
- Alice invia un challenge a Bob R_A
- Bob risponde con il challenge cifrato $K_{AB}(R_A)$
- Alice è sicura di parlare con Bob
- Alice sceglie una chiave di sessione casuale K_S, la cifra con K_{AB} e la invia a Bob
- tutti i messaggi successivi sono cifrati con K_S.

Questo protocollo tuttavia non è completamente sicuro: è soggetto infatti ad **attacchi per riflessione**.
Se infatti il destinatario dell'attacco supporta differenti sessioni, ovvero se è in grado di parlare simultaneamente con più processi contemporaneamente allora si può attaccare nel seguente modo:

- Alice vuole connettersi a Bob ma Trudy intercetta tutto
- Alice invia l'identità A in sessione 1;
- Trudy invia la falsa identità B e apre la sessione 2;
- Alice invia il challenge R_A (sessione 2);
- Trudy invia il challenge R_A ricevuto (sessione 1);
- Alice risponde con il challenge cifrato $K_{AB}(R_A)$ (sessione 1);
- Trudy invia il challenge cifrato $K_{AB}(R_A)$ (sessione 2);

- Alice invia il proprio challenge R_{A2} (sessione 1);
- Trudy riceve e rispedisce il challenge R_{A2} (sessione 2);
- Alice risponde con il challenge cifrato $K_{AB}(R_{A2})$ (sessione 2);
- Trudy completa la prima sessione restituendo $K_{AB}(R_{A2})$ (sessione 1);

Trudy ora possiede due sessioni autenticate e valide con Alice.
Soluzione: controllare che i challenge ricevuti siano a breve distanza di tempo siano sempre differenti, oppure usare altri protocolli di autenticazione.

Domande e Risposte

Che cos'è SPX?

Che cos'è una rete 10Base2?

Il secondo standard Ethernet, detto anche thin Ethernet, caratterizzato da un cavo più sottile e malleabile rispetto a 10Base5. Le connessioni sono fatte con connettori a T di tipo BNC. Economico e facile da installare.

Che cos'è una modulazione?

Per trasmettere un segnale che descrive informazione si utilizza normalmente un segnale portante costante di tipo sinusoidale. Questo segnale viene modulato, ovvero variato in una delle sue tre proprietà base: ampiezza, frequenza e fase. Variando l'ampiezza si hanno, ad esempio, alternanze disegnale a zero e segnale normale; variando la frequenza si hanno alternanze di picchi più frequenti con zone più rade.

E' possibile realizzare una fibra ottica wireless?

Si. Con due raggi laser e due rilevatori fotoelettrici montati in modo tale che l'uno possa captare il segnale dell'altro (es: in cima a due edifici). Svantaggi: pioggia, nebbia o forti correnti di calore possono alterare la trasmissione dati.

Quanti canali è possibile riutilizzare in una rete telefonica cellulare di seconda generazione costituita da 6 celle adiacenti?

Che vincoli fisici devono avere i cavi UTP?

Non possono superare i 100 metri di lunghezza

Perché i cavi UTP sono intrecciati?

Perché si riducono le interferenze esterne. Le interferenze sopravvengono nella fase terminale del cavo dove sono non intrecciati per essere inseriti nel connettore RJ-45.

La rete Ethernet funziona senza switch e hub?

Una piccola rete Ethernet funziona anche senza questi dispositivi. In una topologia ad anello su cavo coassiale con connettori BNC ad esempio, il canale diviene un dominio di collisione sul quale tutti possono trasmettere ed il

protocollo che gestisce le collisioni è il CSMA/CD unito all'algoritmo di backoff esponenziale binario. Ma anche due client connessi direttamente con un cavo UTP cat 5 incrociato e schede di rete di tipo Ethernet sono una rete.

Di che cosa si occupa il livello datalink del protocollo TCP/IP?

Che cos'è una lunghezza d'onda?

La lunghezza d'onda è la distanza che un'onda percorre mentre compie un ciclo completo, ovvero quando essa raggiunge nuovamente il valore iniziale dopo aver superato un massimo e un minimo. La lunghezza d'onda è legata alla frequenza dalla relazione $\lambda v = c$

E' possibile realizzare una rete ATM wireless?

Certamente, tutta la rete può essere di tipo ATM fino all'antenna che emette il segnale wireless. I frame emessi dall'antenna possono essere di tipo 802.11 o 802.16. Su Internet (sito IEEE) si trovano pagine che parlano di AWACS, ovvero ATM Wireless, per cui ci sarà un nuovo formato di frame oltre quelli 802.11 e .16.

Quanti canali è possibile riutilizzare in una rete telefonica cellulare di prima generazione costituita da 70 celle adiacenti?

La prima generazione di cellulari dispone di 800 canali. Assimilando la forma delle celle a degli esagoni, suddividendo e alternando l'uso dei canali è possibile ottenere un totale di (70/7)* 800 = 8000 canali

A che livello si trova il protocollo HTTP? Si tratta di un protocollo con o senza connessione?

Si consideri il livello data link: quali sono le sue funzionalità e come sono organizzati i protocolli coinvolti?

Perché le applicazioni di rete utilizzano i threads?

Che cos'è l'affidabilità?

Che cos'è un hub?

Nella stessa comunicazione in Internet è possibile spedire un frame Ethernet in un cella ATM?

E' possibile aprire una connessione UDP a livello data link?

Qual'è l'interfaccia fornita al livello di data link in un pc?

E' possibile che si verifichino collisioni con il protocollo CSMA/CA nelle reti wireless?

Che caratteristiche ha una connessione ADSL?

Che cos'è una shadows zone?

Che topologia ha in genere una piccola rete moderna?

Se un cavetto UTP risulta da un test soggetto ad una interferenza crosstalk alta quale potrebbe essere la causa?

Qual è l'interfaccia del livello di trasporto?

Che cos'è un DNS secondario?

Con che tipo di cavi si verifica una multipath interference?

Che cos'è un repeater?

Quale è la lunghezza minima del campo dati di un frame ethernet?

Che cos'è un protocollo?

Perché le fibre ottiche multimode non sono adatte per le reti geografiche?

Perché se i cavi sono troppo lunghi vi sono problemi con la propagazione dei fasci di luce.

Con che topologia è organizzata una rete ATM e perché?

La topologia è a mesh, cioè a rete, come le maglie di una rete da pesca (all'incirca!!). Il motivo è per garantire diversi cammini per raggiungere il destinatario. I diversi cammini sono scelti anche in base al momentaneo carico di lavoro dei singoli switch ATM.

Che differenza c'è tra uno switch e un hub?

Uno switch lavora in modalità' punto-a-punto mentre l'hub lavora in modalità broadcast. Una scheda di uno switch è un dominio di collisione, per cui tutti gli apparati sulla stessa scheda si contendono il canale. Ciò nonostante all'interno di una stessa scheda le trasmissioni in uscita non sono in broadcast ma solo sulla specifica porta del destinatario.

Un algoritmo di routing contatta il server DNS per reperire l'IP della destinazione?

No, poiché il pacchetto già contiene nell'intestazione l'IP della destinazione. Inoltre il DNS viene interrogato a livello di applicazione e non nello strato network ove opera il router.

Perché le celle ATM hanno dimensioni fisse?

Per evitare lunghi tempi di attesa che si potrebbero verificare con pacchetti di dimensioni indefinite. Inoltre con pacchetti piccoli e di dimensioni fisse è più facile costruire hardware veloce.

Che cos'è una subnet mask in un indirizzo IP?

Una sequenza di bit utilizzata per estrarre la sottorete da un indirizzo. In pratica si somma (AND logico) in binario la subnet all'IP e rimane solamente la parte relativa alla sottorete.

E' possibile che si verifichino collisioni con il protocollo CSMA/CD nelle reti ethernet?

Si perché è impossibile evitare completamente collisioni anche se si può controllare lo stato del cavo. Basta che due stazioni inizino a trasmettere contemporaneamente su un canale libero che si verifica una collisione. CSMA/CD + algoritmo di backoff evitano, per quanto possibile, ulteriori collisioni.

Come è organizzata la rete pubblica telefonica?

Perché le rete cellulare divide una città in piccole celle?

Per poter riutilizzare un numero maggiore di canali.

Quante chiavi sono necessarie per realizzare una trasmissione sicura di una grossa quantità di dati tra due siti generici?

Tre chiavi, una pubblica, una privata e una simmetrica. La chiave simmetria consente codifiche più veloci, per cui è utilizzata per cifrare tutto il traffico tra i due siti. Le chiavi pubbliche e private, molto lente nel processo di cifratura e decifrazione, si utilizzano solo all'inizio per scambiarsi la chiave simmetrica.

E' più lunga una tabella di routing o una di switching?

Che cos'è un socket?

Un socket è un astrazione che rappresenta un canale, tipicamente utilizzata a livello di trasporto. Un socket è usualmente associato ad un indirizzo IP e a un numero di porta e può essere identificato da un descrittore. In genere un socket è associato ad un protocollo che determina le modalità del suo utilizzo

A che cosa serve una firma digitale?

A identificare in modo sicuro l'autore di un documento in formato elettronico.

E' sicuro un certificato digitale?

Non è sicuro al 100%. Il certificato ha la funzione di associare una persona fisica (o giuridica) ad una coppia di chiavi pubblica-privata. Il certificato è garantito poiché chi lo emette è un ente di cui tutti per ipotesi si fidano (se se... certo). Se un certificato è revocato, nell'intervallo di tempo tra la pubblicazione della revoca e la revoca stessa, esso potrebbe essere utilizzato per scopi discutibili.

Che cosa e' un CODEC? (qui la domanda è imprecisa, però passiamoci sopra :-)

E' un dispositivo hardware o che traduce segnali analogici in segnali digitali.
La domanda è imprecisa poiché si chiamano codec anche tutti i software che codificano una sorgente, multimediale ad esempio, in modo da trasmetterla o memorizzarla in un determinato formato. Es: flusso video codificato in MPEG-4.

Di cosa si occupa il livello IP del protocollo TCP/IP?

Di instradare opportunamente i pacchetti in rete. Attraverso il sistema di indirizzi IP, il collante di Internet, è possibile spedire pacchetti attraverso tutta la rete. l'intestazione IP che viene aggiunta ai dati da trasmettere contiene l'indirizzo del mittente, del destinatario, indicazioni di servizio sul tipo di contenuto, sulla frammentazione, un contatore che decrementa ad ogni passaggio da un router in modo da non propagarsi all'infinito in casi di topologie particolari o di errori di routing, più altre informazioni. Gli indirizzi IP vengono forniti dal server DNS ai processi che ne fanno richiesta.

Perché gli switch ATM non prendono decisioni di routing?

Con che topologia è organizzata una Token Ring?

perché il router utilizza le netmask binarie?

E' possibile integrare una rete ATM e una rete wireless in una sola rete locale?

A che livello lavora il protocollo ICMP?

perché UDP richiede una ACK dopo una trasmissione? (trabocchetto?)

E' possibile utilizzare il protocollo a chiave asimmetrica criptando con chiave privata?

Che cos'è una porta?

Che cos'è un frame?

Un frame è una definizione della struttura con cui vengono spediti i dati al livello datalink.

Cosa è il DNS?

Un servizio distribuito che permette di tradurre indirizzi logici in indirizzi IP e viceversa

Come è memorizzato un indirizzo IP?

Con un numero binario di 32 bit. La rappresentazione usuale è in 4 ottetti espressi in numeri decimali da 0 a 255.

In una comunicazione in Internet e' più' grande un frame o un pacchetto?

Un frame in quanto include il pacchetto.

Che cosa è la Scalabilità?

Esprime la capacità di una certa tecnologia di scalare, cioè di modificare le proprie caratteristiche di grandezza, potenza, capacità, ecc.. per adeguarsi alla domanda se la domanda cresce. Ad esempio una LAN ethernet è facilmente scalabile in ampiezza semplicemente aggiungendo uno o più switch.

Perché le applicazioni di rete utilizzano i Threads?

Perché sono generalmente costituite da più componenti che interagiscono e che è opportuno siano eseguite contemporaneamente., dunque attivando più processi. Il gestore dei processi si occupa del fatto che ciascuno di essi riceva un certo quantitativo di tempo di elaborazione dalla CPU.

Quale è l'interfaccia fornita al livello di trasporto

Tipicamente sono chiamate di sistema del sistema operativo.

Descrivere un protocollo di autenticazione in rete che non richiede lo scambio della password né in chiaro né criptata.

Che cos'è la lunghezza d'onda?

Considerando uno switch a 12 porte con solo 8 host connessi e la tabella di switch non configurata, qual è il numero minimo di messaggi che gli host devono spedire per configurare la tabella di switch?

Qual è la tecnica che si utilizza nel protocollo CSMA/CA per evitare le collisioni? Qual è il ruolo del messaggio di ACK?

Da casa con connessione via modem voglio verificare la presenza di un host tramite il comando "ping", descrivere la struttura dei messaggi ed i protocolli utilizzati ai veri livelli. Si tratta di un protocollo con o senza connessione?

Una piccola azienda con 5 dipendenti (6 postazioni di lavoro) deve progettare la sua rete locale collegata ad internet. Descrivere il progetto della piccola rete indicando le componenti hardware e software, il tipo di cablaggio ed il tipo di connessione in modo da:
- minimizzare i costi garantendo una banda interna di almeno 50 Mbps
- garantendo un alto livello di sicurezza
- garantire banda verso l'esterno di almeno 2 Mbps

Un esempio di rete locale ad alta sicurezza potrebbe essere costituito da:

- un router come interfaccia verso l'esterno
- un firewall che filtri tutto il traffico in entrata, basato ad esempio su un distribuzione unix tipo FreeBSD;
- uno switch a 8 porte che consenta collegamenti punto-punto con i 6 terminali client;
- Un file server con dischi in configurazione RAID che gestisca la condivisione e l'archiviazione dei file;
- Un ulteriore dispositivo di backup su nastro per salvataggi giornalieri o settimanali;
- Eventualmente una ulteriore macchina dedicata come database-server per gli applicativi aziendali.

Una applicazione comunica con SMTP per inviare posta elettronica via internet, attraverso un modem. Partendo dall'inizio indicare i nomi degli header e dei trailer necessari per spedire il pacchetto in rete. Se l'host del destinatario è possibile stabilire a priori quanti switch vengono attraversati dal messaggio?

Indicare i nomi degli header e trailer necessari per spedire un generico pacchetto in una rete Ethernet utilizzando il protocollo UDP. Cosa succede se si perde un pacchetto?

Una applicazione utilizza il protocollo POP per ricevere posta via modem. Indicare i nomi degli header e trailer ricevuti.

Utilizzando tecnologia per la telefonia cellulare di seconda generazione in una città di 2 milioni di abitanti, quante celle sono necessarie se si vuole servire non più di 10 utenti per canale?

I canali sono pochi, in un sistema di seconda generazione sono 2500.
Per ogni canale ci devono essere al massimo 10 utenti.
Statisticamente, ogni utente utilizza il cellulare per il 5% del proprio tempo.
Celle adiacenti non possono utilizzare gli stessi canali per evitare interferenze nelle zone di sovrapposizione del segnale. Per tale motivo si stima il riutilizzo del

canale dividendo il numero di celle per un fattore 7.
(X celle / 7) * 2500 canali * 10 utenti = 2.000.000 utenti * 5%
X = 28 (mi sembrano pochine... boh..)

Un'azienda deve progettare un collegamento ad una rete geografica scegliendo tre tecnologia frame relay e linee dedicate. Si ipotizzi un costo mensile di 2000 euro per ogni linea dedicata, mentre i costi mensili relativi alla tecnologia frame relay sono specificati tra parentesi nel seguito. Se l'azienda ha due uffici principali e due filiali tutti collegati tra loro con i seguenti requisiti:
- a) la comunicazione tra i due uffici principali A1 e A2 deve essere di 300 kbps
- b) le filiali devono essere connesse tre loro e agli uffici principali ad almeno 100 kbps.
Qual è la soluzione che minimizza i costi, tenendo conto delle seguenti disponibilità riguardo alla soluzione frame relay.
- i PVC disponibili sono di 56 kbps (100), 128 kbps (200), 256 kbps (150), 348 kbps (300), 512 kbps (400), 1 Mbps (500)
- le velocità delle porte disponibili sono: 56 kbps (200), 128 kbps (400), 256 kbps (600), 348 kbps (800), 512 kbps (1000), 756 kbps (1200), 1 Mbps (1400)
- le linee dedicate per collegarsiai POP sono da 56 kbps (100), 256 kbps (150), 512 kbps (200), 1 Mbps (250), 1,5 Mbps (300)

Ufficio principale 1.
Servono 2 PVC da 128 e uno da 348. TOTALE = 700 euro
Il totale della banda è 128 + 128 + 348 = 604 kbps. Si stima un utilizzo medio del 70%, per cui 70% di 604 = 422,8 ovvero serve una porta da 512 kbps da 1000 euro. Infine le tre linee sono da 256, 256 e 512 per un totale di 150 + 150 + 200 = 500 euro. La spesa complessiva è di 700 + 1000 + 500 = 2200 euro.
Ufficio principale 2.
Uguale all'uno, meno il costo della linea da 348 kbps e del PVC.
2200 – 300 – 200 = 1800 euro
Filiale 1
Serve un solo PVC da euro 200 verso la filiale 2 e una sola linea da 150 euro, le altre sono già previste nei casi precedenti. Serve inoltre una porta da 348 kbps a 800 euro, poiché il traffico stimato è il 70% di (128 kbps x 3) = 268,8.
200 + 150 + 800 = 1150 euro
Filiale 2
Uguale alla uno, meno il costo della linea e del PVC: solo 800 euro, regalato!!
TOTALE FINALE
2200 + 1800 + 1150 + 800 = 5950 euro mensili... e asti cazzi!

Una applicazione comunica con il protocollo SMTP per inviare posta elettronica via internet. L'hostess risiede su una rete Ethernet collegata a internet. Partendo dall'inizio indicare i nomi degli header e dei trailer necessari per spedire il pacchetto in rete.Se l'host del destinatario è sulla stessa rete locale è possibilestabilire a priori quanti router vengono attraversati ?

Livello applicazione: protocollo SMTP
Livello trasporto: protocollo TCP SMTP + **TCP**
Livello network: protocollo IP SMTP + TCP + **IP**
Livello datalink: protocollo Ethernet
DL Trailer Ethernet + SMTP + TCP + IP + **DL Header Ethernet**

Se il server SMTP è sulla stessa rete, quindi non si attraversa nessun router. Se il server SMTP è ad esempio sui server del proprio ISP, non si può sapere a priori quanti siano i router da attraversare. Con un traceroute si possono invece scoprire. Es: **traceroute smtp.eutelia.it**