Reti di Calcolatori

Giacomo Zanatta

AA 2017-2018

Indice

1 Introduzione

Una rete di calcolatori è un insieme di calcolatori o di dispositivi hardware, connessi tra loro mediante uno o più mezzi di comunicazione che hanno come scopo principale quello di condividere risorse. Due dispositivi si dicono connessi quando sono in grado di scambiare informazioni.

1.1 Applicazioni delle reti di calcolatori

1.1.1 Applicazioni aziendali

Una rete in ambito aziendale è utile perchè permette la condivisione di risorse, indipendentemente dalla posizione fisica dell'utente e della risorsa. Per risorsa in questo caso intendiamo programmi, periferiche (ad esempio stampanti, dispositivi di memorizzazione) e dati. Per le aziende può essere utile anche utilizzare delle VPN (Virtual Private Network), per unire più reti situate in punti diversi del mondo in un'unica rete interna all'azienda. È molto utilizzato il modello client/server, dove i dati sono memorizzati in macchine molto prestanti (server) e gli utenti (in questo caso gli impiegati) utilizzano macchine semplici (client) che permettono l'accesso ai dati situati nel server. Una rete è anche utilizzata come mezzo di comunicazione tra gli impiegati o qualsiasi altra persona. Gli utenti possono scambiarsi email, effettuare chiamate utilizzando software VoIP. È possibile accedere da remoto ai propri desktop (desktop sharing) o gestire anche i propri affari con un modello di e-commerce.

1.1.2 Applicazioni domestiche

In ambito domestico, una rete è utilizzata per connettersi al mondo, leggere quotidiani online, condividere contenuti multimediali (ad esempio utilizzando il protocollo P2P, dove non c'è una vera distinzione tra client e server ma ognuno può comunicare con chiunque), comunicare con altre persone utilizzando email o instant messaging. Un utente può studiare da casa (online teaching) o condividere i propri pensieri su un social network. Gruppi di persone possono cooperare per realizzare contenuti (ad esempio le Wiki). È possibile anche effettuare acquisti o accedere a servizi finanziari, pagare le bollette, partecipare ad aste on-line. È possibile usare una rete per intrattenersi, videogiocando online o guardando contenuti multimediali in streaming.

1.1.3 Utenti mobili

È possibile connettersi ad una rete utilizzando mezzi trasmissivi wireless. Le reti wireless sono utili in mobilità. I telefoni cellulari utilizzando delle reti senza fili per poter comunicare, scambiare SMS e anche accedere ad Internet mediante reti 3G e 4G. Si sta difofndendo anche l-m-commerce, dove per pagare un prodotto si utilizza il credito telefonico. Le reti di sensori sono fatte di nodi che raccolgono e consegnano in modo wireless il dato che hanno registrato dal mondo circostante, questo approccio è ampliamento utilizzate per l'IOT

(Internet Of Things). In commercio ci sono anche i wereable computer, come orologi, pacemaker ed iniettori di insulina.

1.1.4 Risvolti sociali

Opinioni espresse pubblicamente sui social network possono nuocere a qualcuno o non essere politicamente corrette. Inoltre su internet si può trovare facilmente materiale piratato o illegale, costringendo agli operatori di rete di bloccare contenuti o addirittura servizi come il P2P. Con neutralità della rete si intende che la comunicazione deve essere uguale per tutti indipendentemente dal contenuto, dalla sorgente e dal fornitore del contenuto. Per constrastare la pirateria online sono state creati sistemi automatici in grado di inviare avvisi a fornitori di servizi, agli utenti e agli operatori di rete sospetti di violazione di copyright (DMCA). La privacy online è un altro punto saliente. Ad esempio, i governi sorvegliano i cittadini, analizzando le mail per trovare informazioni a riguardo di comportamenti illeciti. Dei file chiamati cookie,memorizzati nei PC degli utenti, permettono alla aziende di tracciare le attività degli utenti, ma consentono anche di diffondere informazioni private dell'utente. Online è facilmente diventare vittime di phising o di virus. Per distinguare sistemi automatizzati da un utente sono stati sviluppati i CAPTCHA (variante del test di Touring).

1.2 Hardware di rete

Per progettare una rete è necessario tenere conto di queste due caratteristiche:

1. tecnologia di trasmissione
   (a) collegamenti broadcast, un solo canale di comunicazione condiviso da tutte le macchine nella rete. Ogni macchina riceve il messaggio. Nel messsaggio inviato è presente un campo indirizzo che identifica il ricevente. Solo la macchina specificata nel campo indirizzo processa e legge il messaggio, le altre macchine lo ignorano. In un collegamento broadcast è possibile, usando un indirizzo speciale, inviare il messaggio a tutti i dispositivi nella rete. Alcuni sistemi broadcast supportano l'invio di un messaggio ad un sottoinsieme delle macchine (multicast)
   (b) collegamenti punto a punto, connettono coppie di computer. I messaggi possono dover visitare più macchine intermedie per arrivare a destinazione. Se è presente un solo ricevente e un solo trasmittitore, la trasmissione punto a punto è chiamata unicast.
2. scala
   (a) PAN
   (b) LAN
   (c) MAN

(d) WAN

La connessione di due o più reti è chiamati internetwork. Internet è una internetwork.

1.2.1 PAN

Permettono ai dispositivi di comunicare nello spazio fisico a portata di una persona. Questi dispositivi possono essere, ad esempio, mouse, tastiera, smartwatch, auricolari. Una rete wireless a corto raggio è la rete Bluetooth, che adottano il paradigma master-slave: ad esempio, il pc è un master che comunica con i slave (tastiera, mouse), decidendo che indirizzi e frequenze usare, per quanto tempo comunicare, eccetera. Le reti PAN possono essere realizzate anche con tecnologie diverse dal bluetooth, come ad esempio gli RFID.

1.2.2 LAN

Una rete LAN è una rete privata che opera all'interno di un edificio o nelle sue vicinanze. Sono utilizzate per connetere PC e dispositivi per permettere la condivisione di risorse. Una LAN aziendale è chiamata enterprise network. Esistono anche LAN wireless: ogni macchina ha un ricevitore radio e un'antenna per comunicare con gli altri oppure con un AP (Access Point). Un AP distribuisce i pacchetti tra i dispositivi a lui collegati oppure tra i dispositivi e Internet. Se i computer sono vicini tra loro possono comunicare usando il protocollo P2P. Le LAN cablate utilizzano cavi di fibra ottica o di rame. Le LAN sono abbastanza piccole, quindi il tempo di trasmissione nel caso peggiore è limitato e noto a priori. Le LAN cablate viaggiano a 100 Mbps / 1 Gbps, hanno bassi tempi di ritardo e commettono pochi errori di trasmissione. Ogni computer si connette ad un dispositivo chiamato switch con una connessione punto a punto. Per costruire reti LAN grandi è possibile collegare tra loro più switch attraverso le porte. È possible anche suddividere una grande LAN in reti logiche più piccole, chiamate VLAN (virtual LAN).
Le reti broadcast wireless e cablate si possono dividere in statiche e dinamiche, a seconda del modo in cui è allocato il canale:

1. Allocazione statica: suddividere il tempo in intervalli discreti e usare un algoritmo round-robin. Una macchina può comunicare solo se è attivo il proprio turno. La capacità del canale viene sprecata se una macchina non ha nulla da trasmettere durante il proprio slot.

2. Allocazione dinamica: i metodi per questo tipo di allocazione possono essere centralizzati o non centralizzati.

   (a) Centralizzato: esiste una singola entità che stabilisce a chi spetta l'uso del mezzo.

   (b) Non centralizzato: non esiste un'entità centrale, ogni macchina decide se trasmettere o meno.

Una rete LAN domestica deve essere sicura, non molto costosa, facilmente espandibile, e semplice da usare.

1.2.3 MAN

Una rete MAN copre una intera città. Un esempio di rete MAN è la rete di TV via cavo, o la rete WiMax (IEEE 802.16)

1.2.4 WAN

Una WAN copre una nazione o un continente. Una rete WAN è composta da sottoreti (subnet) dove risiedono gli host. Una sottorete è composta da linee di trasmissione ed elementi di commutazione. Le linee di trasmissione permettono di spostare i bit tra le macchine. Gli elementi di commutazione (switch) sono delle macchine che collegano due o più linee di trasmissione. Un esempio di elemento di commutazione è il router. In una WAN gli host e la sottorete hanno proprietari e operatori diversi. I gestori di una sottorete sono i network provider. I router inoltre connettono usualmente reti diverse, ad esempio Ethernet e SONET. Sono necessari quindi dei dispositivi che uniscano questi tipi diversi di rete. Le WAN sono delle internetwork, ossia reti composite formate da più di una rete.
Ad una rete WAN può connettersi un singolo dispositivo oppure un'intera LAN. Una VPN (Virtual Private Network) permette di collegare più reti LAN distanti tra loro, dando l'idea di operare su una singola rete locale.
Una sottorete può anche essere utilizzata da diverse aziende: l'operatore della sottorete si chiama provider di servizi di rete, e gli uffici sono i suoi clienti. Un provider che permettere ai suoi clienti di accedere ad Internet è chiamato ISP e la sottorete si chiama rete ISP. Una rete WAN è composta da molte linee di trasmissione, ciascuna delle quali collega una coppia di router. È necessario quindi definire quale percorso devono fare i messaggi per arrivare a destinazione, mediante un algoritmo di routing, adottato dalla rete. Un algoritmo di inoltro invece è la strategia adottata localmente da un router per decidere dove inoltrare un pacchetto.
Le reti telefoniche e satellitari sono un esempio di reti WAN broadcast e wireless.

1.2.5 Internetwork

Una internetwork è un insieme di reti interconnesse. Internet è un esempio di internetwork, la quale utilizza le reti ISP per connettere reti aziendali, domestiche, e moltre altre reti. Una rete è composta dalla combinazione di una sottorete e dei suoi host. Due reti diverse possono essere collegate tra loro mediante un gateway.

1.3 Software di rete

1.3.1 Gerarchie di protocolli

La maggior parte delle reti è organizzata come una pila di livelli o strati. Ogni livello offre servizi ai livelli superiori, schermandoli dai dettagli implementativi (concetto definito come information hiding).
Un protocollo è un accordo tra le parti che comunicano sul modo in cui deve procedere comunicazione.
Le entità che stanno sullo stesso livello sono chiamati peer. I peer comunicano tra loro utilizzando il protocollo.
Ogni livello passa i dati al livello sottostante fino a raggiungere il livello 1, che si appoggia al supporto fisico su cui avviene la comunicazione.
Tra ogni livello è presente una interfaccia, che definisce le operazioni e i servizi che il livello inferiore offre al livello superiore.
L'insieme di livelli e protocolli si chiama architettura di rete. L'insieme dei protocolli utilizzati da un sistema è chiamato pila di procolli.

1.3.2 Progettazione dei livelli

Ci sono alcuni problemi sulla progettazione di livelli. È necessario che i protocolli garantiscono l'laffidabilità della rete. Ad esempio, è necessario fornire meccanismi per intercettare errori, oppure di fornire codici di correzione degli errori che permettono di ricostruire il messaggio in modo corretto.
Un altro problema consiste nel trovare un percorso valido attraverso la rete, utilizzando un algoritmo di routing.
Altri problemi sono: naming dei dispositivi connessi alla rete, scalabilità della rete, allocazione delle risorse (come dividere la banda?), flow control (come controllare il flusso per evitare congestioni?), sicurezza delle reti.

1.3.3 Servizi connectionless e connection oriented

1. servizi orientati alla connessione: l'utente deve stabilire una connessione, usarla e rilasciarla. Nella maggior parte dei casi l'ordine dei bit trasmessi è conservato. In alcuni casi trasmettitore, ricevente e la sottorete eseguono una negoziazione dei parametri da usare (es: massima dimensione di un messaggio, la qualità del servizio richiesta).

2. servizio connectionless: ogni messaggio è instradato in modo indipendente dai messaggi successivi.
   Ogni nodo intermedio deve ricevere completamente il pacchetto prima di inoltrarlo (store-and-forward). Non è garantito l'ordine di arrivo dei messaggi.

Oltre a questa distinzione, i servizi possono essere caratterizzati ulteriormente in affidabili e non affidabili:

1. servizi affidabili: servizi che non perdono mai dati. Utilizzato per trasferire file. Ci sono ulteriormente 2 distinzioni per questo tipo di servizi

orientati alla connessione: message sequence, dove i confini dei messaggi vengono preservati, e il byte stream, in cui la connessione è un semplice flusso di byte (quest'ultimo utilizzato per i film in streaming).
Un servizio affidabile non connesso viene chiamato datagram con confermas

2. servizi non affidabili: quando è possibile una perdita di dati. Utilizzato ad esempio per il VoIP, dove il ritardo è inaccettabile ma si può tollerare un po' di rumore. Un servizio senza connessione non affidabile viene chiamato servizio datagram.

1.3.4 Primitive di servizio

Un servizio è specificato da un insieme di primitive.. L'insieme delle primitive disponibili dipende dalla natura del servizio offerto (ad esempio se è connection oriented o no).

1.3.5 Relazione tra servizi e protocolli

Un servizio è un insieme di operazioni che un livello offre a quello superiore. Il servizio definisce QUALI operazioni, ma non COME vengono implementate.
Un protocollo invece è un insieme di regole che controllano il formato e il significato dei pacchetti o messaggi scambiati tra le entità pari all'interno di un livello.
Le entità usano i protocolli per implementare le loro definizioni dei servizi. Possono cambiare il protocollo ma non il servizio.

1.4 Modelli di riferimento

1.4.1 Modello OSI

Il modello OSI si fonda su una proposta dell'ISO (International Standard Organization) di standardizzare i protocollli impiegati nei livelli. Presenta 7 livelli:

1. LIVELLO FISICO: si occupa della trasmissione grezza dei dati sottoforma di bit.

2. LIVELLO DATA LINK: fa diventare una comunicazione grezza in una linea che appare priva di errori.Un sottolivello MAC si occupa di controllare l'accesso al mezzo trasmissivo.

3. LIVELLO DI RETE: controlla il funzionamento della sottorete. Controlla le congestioni e l'instradamento dei pacchetti.

4. LIVELLO DI TRASPORTO: accetta i dati dal livello superiore, li suddivide in unità più piccole, li passa al livello di rete e si assicura che i dati arrivino correttamente a destinazione.

5. LIVELLO DI SESSIONE: permette a utenti su computer diversi di stabilire una sessione. Una sessione offre: controllo del dialogo, gestione dei token, sincronizzazione.

6. LIVELLO DI PRESENTAZIONE: si occupa della sintassi e della semantica dell'informazione trasmessa. Gestisce delle strutture dati astratte con cui è possibile consentire la comunicazione tra computer che possiedono una diversa rappresentazione dei dati.

7. LIVELLO APPLICAZIONE: protocolli richiesti dagli utenti. Contiene il protocollo HTTP, FTP, SMTP..

1.4.2 Modello TCP/IP

1. LIVELLO LINK: descrive cosa devono fare i collegamenti per esaudire le necessità di questo livello internet senza connessione. È un interfaccia tra host e mezzo trasmissivo.

2. LIVELLO INTERNET:permette a degli host di inviare pacchetti su qualsiasi rete, e fare in modo che questi possano viaggiare in modo autonomo verso la destinazione. Protocollo IP

3. LIVELLO TRASPORTO: consente la comunicazione tra peer degli host sorgente e destinazione. Sono stati definiti 2 protocolli di trasporto end-to-end:

   (a) TCP: Trasmission Control Protocol, affidabile orientato alla connessione. Permette ad un flusso di byte di raggiungere la destinazione senza errori. Gestisce anche il controllo del flusso, per evitare congestioni.

   (b) UDP: User Datagram Protocol, inaffidabile senza connessione. È usato soprattutto per trasmissione di voce e filmati.

4. LIVELLO APPLICAZIONE: contiene tutti i protocolli di livello superiore. TELNET, FTP, SMTP, HTTP eccetera...

1.5 Esempi di reti

1.5.1 Internet

Internet è una raccolta di reti diverse che usano determinati protocolli e offrono servizi comuni.

1. ARPANET: Internet è nato come progetto militare. ARPANET è stata sviluppata verso la fine degli anni '60. Era composta da minicomputer chiamati IMP collegati da linee di trasmissione a 56 kbps. Ogni IMP doveva essere collegato ad almeno altri due IMP. La sottorete era basata su datagrammi: in caso di distruzione di alcune linee, i pacchetti facevano un'altra strada. Inizialmente, ARPANET collegava diverse università

degli USA. Verso gli anni '80 venne creato il DNS, poi evolutosi in un database distribuito.

2. NSFMET: permetteva la connessione dei dipartimenti di informatica e dei laboratori ad ARPANET, via dial-up e linee d'affitto.
   NSF costruì una rete di dorsale (backbone) per collegare i suoi 6 centri di ricerca.
   Dato l'enorme successo, venne creata ANSNET di tipo commerciale.

Architettura di Internet In Internet un computer si connette ad u ISP, il quale fornisce la connessione ad Internet.
Per connettersi all'ISP ci sono diversi modi: uno di questi è usare la linea telefonica, usando la DSL: il computer viene collegato ad un modem DSL che converte i pacchetti digitali in segnali analogici. Un dispositivo chiamato DSLAM converte i segnali analogici in pacchetti dall'altra parte della linea.
Un altro modo è usare il sistema della TV via cavo,
Il dispositivo situato in casa si chiama cable modem, quello all'altro capo invece CMTS (cable modem termination system).
Ora sta prendendo piede l'FTTH (fiber to the home).
Le reti ISP possno essere regionali, nazionali o internazionali. Le linee di trasmissione che collegano i vari ISP sono chiamate backbone (dorsali).

2 Il livello fisico

Definisce gli aspetti elettrici, di temporizzazione e le altre modalità con cui i bit vengono spediti sui canali di comunicazione.

2.1 Basi teoriche della comunicazione dati

Le informazioni possono essere trasmesse via cavo variando alcune proprietà fisiche (tensione).

2.1.1 Analisi di Fourier

Qualunque funzione periodica sufficientemente regolare g(t) con periodo T può essere ottenuta sommando un numero di funzioni seno e coseno:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_i \sin(2\pi n f t) + \sum_{n=1}^{\infty} b_i \cos(2\pi n f t) \tag{1}$$

f=1/T rappresenta la frequenza fondamentale
a_n e b_n rappresentano le ampiezze seno e coseno delle armoniche (termini) n-esime
c rappresenta una costante.
Se il periodo T è noto e le ampuezze sono definite, la funzione originale del tempo si ricava eseguendo le somme.

$$a_n = \frac{2}{T} \int_0^T g(t) \sin(2\pi n f t) dt \tag{2}$$

$$b_n = \frac{2}{T} \int_0^T g(t) \cos(2\pi n f t) dt \tag{3}$$

$$c = \frac{2}{T} \int_0^T g(t) dt \tag{4}$$

2.1.2 Segnali a banda limitata

I canali reali influiscono in modo non omogeneo sui segnali a diverse frequenze. Su un cavo, le ampiezze sono trasmesse senza modifiche fino ad una certa frequenza f_c (misurata in Hertz o in cicli al secondo) e attenuate per tutte le frequenze superiori. L'intervallo di frequenze trasmesse senza una forte attenuazione è chiamato banda (bandwith). La banda passante è compresa tra 0 e la frequenza dove la potenza è attenuata del 50%.
La banda passante è una proprietà fisica del mezzo di trasmissione e dipende dalla sua costruzione, lunghezza e spessire. Per ridurre l'ampiezza della banda è possibile inserire un filtro all'interno del circuito. Ad esempio i canali wireless 802.11 possono usare fino a 20Mhz di banda, per cui le interfacce radio filtrano la banda del segnale a questa dimensione.

Filtrare la banda può portare ad una maggior efficenza del sistema.
La larghezza di banda è la larghezza della banda delle frequenze.
I segnali che partono da 0 fino ad una frequenza massima si chiamano banda base (baseband).
I segnali che vengono traslati per occupare una gamma di frequenze più alte si chiamano banda passante (passband).
La banda analogica è una quantità in Hz, la banda digitale è il massimo tasso con cui un canale è in grado di trasportare dati, e si misura in bit al secondo.

2.1.3 Velocità massima di trasmissione di un canale

Nyquist dimostrò che se si trasmette un segnale arbitrario attraverso un filtro passa basso la cui ampiezza di banda è pari a B, il segnale filtrato può essere ricostruito completamente prendendo solo 2B campioni al secondo. Se il segnale è composto da V livelli discreti, il teorema di Nyquist afferma che

$$massimo\, tasso\, trasmissivo\ = 2B \log_2 V\ bit/s \tag{5}$$

Un canale a 3 kHz, per esempio, non è in grado di trasmettere segnali binari a velocità maggiore di 6000 bps.
Se sul canale è presente un rumore casuale, la situazione peggiora.
Il livello di rumore termico (rumore casuale provocato dal movimento delle molecole del sistema) si calcola facendo il rapporto tra la potenza del segnale e la potenza del rumore ed è chiamato SNR (signal-to-noise ratio). Il rapporto segnale rumore è pari a S/N (S = potenza del segnale, N = potenza del rumore). Di solito si cita la quantità $10\log_1 0$ S/N, misurata in decibel.
(Shannon) Il massimo tasso di invio dei dati (capacità) in bit/s su un canale rumoroso la cui ampiezza di banda è pari a B Hz e il cui rapporto segnale-rumore è S/N, è dato dal numero:

$$massimo\, numero\, di\, bit/s\ = B \log_2(1 + \frac{S}{N}) \tag{6}$$

che definisce la massima capacità di un canale fisico.

2.2 Mezzi di trasmissione vincolati

È possibile utilizzare diversi tipi di mezzi fisici per realizzare una trasmissione.

2.2.1 Supporti magnetici

Le informazioni vengono scritte su un supporto fisico e lo si trasporta alla destinazione. Più economico rispetto ad una rete.

2.2.2 Doppino

Il doppino (twisted pair) è composto da due conduttori di rame isolati, spessi circa 1mm, avvolti uno intorno all'altro in una forma elicoidale. I cavi vengono

intrecciati per evitare la formazione di antenne .
Un segnale è costruito da una differenza di potenziale tra i due cavi della coppia, come protezione per il rumore esterno (il quale, influenzando entrambi i cavi, mantiene inalterato il valore di questa differenza).
Un esempio di doppino è quello telefonico, usato per effettuare chiamate o accedere ad Internet mediante ADSL. Per distanze maggiori di qyakcge kilometro è necessario fare uso di ripetitori per amplificare il segnale. I doppini vengono usati per trasmettere segnali analogici e segnali digitali. L'ampiezza di banda dipende dal diametro del cavo e dalla distanza percorsa. Per tratti di pochi kilometri è possibile raggiungere velocità di circa qualche megabit al secondo. Oggi si utilizza il doppino Cat. 5, consiste di due cavi isolati e intrecciati tra loro. All'interno di una guaina sono presenti 4 di queste coppie.
Standard differenti di LAN possono usare i doppini in maniera diversa. Ethernet 100 Mbps uso solo due coppie, una per ogni direzione. Ethernet 1 Gbps usa tutte le coppie in entrambe le direzioni.
Collegamenti utilizzabili in entrambe le direzioni contemporaneamente sono chiamati full-duplex.
Colelgamenti in entrambi le direzioni ma che sfruttano una direzione alla volta sono chiamati half-duplex.
Collegamenti unidirezionali sono chiamati simplex.
Esistono anche altre categorie, come Cat. 6 o Cat. 7. Fino a Cat. 6 questi cablaggi sono identificati con UTP (unshielded twisted pair) e consistono solo di cavi e isolanti. Cat. 7 invece possiede una schermatura su ogni singolo doppino e anche attorno a tutto il cavo.

2.2.3 Cavo coassiale

Il cavo coassiale (coax) è più schermato del doppino, e quindi copre distanze più lunghe ed ha una velocità più elevata.
Esistono due tipi di cavi coax: il primo a 50 ohm è stato utilizzato per le trasmissione digitali, il secondo, a 75 ohm, per quelle analogiche e al tv via cavo.
Un cavo coax è composto da un nucleo conduttore coperto da un rivestimento isolante, circondato da un conduttore cilindrico realizzato con una calza di conduttori sottili, avvolto da una guaina protrettiva di plastica.
Ha una grande ampiezza di banda e resiste fortemente al rumore. La banda disponibile dipende dalla qualità e dalla lunghezza del cavo (i cavi moderni hanno un'ampiezza di banda pari a qualche GHz).

2.2.4 Linee elettriche

Sono usate per comunicazioni a basso tasso di invio o bit-rate.
Il segnale dati è sovrapposto al segnale elettrico a bassa frequenza. Il segnale elettrico viene inviato a 50-60 Hz e il mezzo trasmissivo attenua le frequenze più late richieste dalle trasmissioni dati. Soffre molto del rumore generato dai dispositivi elettrici accesi.

2.2.5 Fibre ottiche

Le fibre ottiche sono utilizzate per lel trasmissioni a lunga distanza nelle dorsali di rete, le reti LAN ad alta velocità e l'accesso ad Internet ad alta velocità come FttH.
Un sistema di trasmissione ottico è formato da 3 componenti: la sorgente luminosa, il mezzo trasmissivo e il rilevaore. Il mezzo trasmissivo è una fibra di vetro. Il rilevatore, quando il mezzo è colpito dalla luce, genera un impulso elettrico.
Non c'è dispersione della luce, in quanto quando un raggio luminoso passa da un materiale all'altro si rigrange sul confine tra i due materiali. A causa della riflessione totale, la luce rimane intrappolata.
La fibra può contenere molti raggi, che rimbalzano ad angoli diversi (ogni raggio ha una modalità diversa).
Una fibra multimodale presenta più raggi a diverse modalità.
Una fibra monomodale, più costosa ma più veloce, permette alla luce di non rimbalzare (in quanto il diametro della fibra viene ridotto).

Trasmissione della luce attraverso la fibra. L'attenuazione della luce attraverso il vetro dipende dalla sua lunghezza d'onda, definita come il rapporto tra la potenza del segnale di ingresso e quello di uscita.
Le lunghezze d'onda più comuni sono 3: la banda a 0,85 micron ha il fattore di attenuazione più forte, e viene usata per brevi distanze. La banda a 1,30 micron ha una buona attenuazione come anche la banda a 1,55 micron.
La dispersione cromatica è il fenomeno in cui gli impulsi luminosi trasmessi nella fibra si espandono nella lunghezza d'onda durante la propagazione. Creando impulsi di una certa forma è possibile annullare quasi tutti gli effetti della dispersione e inviare impulsi per migliaia di chilometri. senza modifiche sensibili (sotiloni).

Cavi in fibra ottica. Al centro di un cavo in fibra ottica si trova il nucleo (core) di vetro attraverso il quale viene propagata la luce. Nelle multimodali ha un diametro di 50 micron, in quelle monomodali dagli 8 ai 10 micron.
Il nucleo è circondato da un rivestimento di vetro (cladding) con un basso indice di riflazione. Poi c'è una fodera di plastica che protegge il tutto. Le fibre sono raggruppate in fasci, protetti da una guaina.
Le fibre si possono collegare in 3 modi: possono terminare in connettori (connettori perdono circa il 10-20% della luce), possono essere attaccate meccanicamente (-10% della luce) oppure fusi (piccola attenuazione del segnale). Le riflessioni avvengono sul punto di giuntura, e l'energia riflessa può interferire con il segnale.
I tipi di sorgenti luminose sono 2: i LED o i laser a semiconduttore.

Confronto tra fibre ottiche e cavi in rame. Le fibre ottiche sono molto vantaggiose: hanno maggiore ampiezza di banda e i ripetitori possono essere installati dopo 50 km (mentre per i cavi di rame ogni 5 km). La fibra è anche

sottile e leggera, ed è difficile intercettare i dati trasportati (sono più sicure dei cavi di rame). Però è facilmente danneggiabile, le interfacce costano di più di quelle di rame, e la comunicazione bidirezionale richiede due fibre o due bande di frequenza.

2.3 Trasmissioni wireless

2.3.1 Lo spettro elettromagnetico

Quando gli elettroni si spostano creano onde elettromagnetiche. Il numero di oscillazioni al secondo di un'onda è chiamato frequenza (f) ed è misurato in Hz. La distanza tra due massimi o minimi consecutivi è chiamata lunghezza d'onda ed è indicata dalla lettera λ.
Nel vuoto le onde elettromagnetiche indipendentemente dalla frequenza viaggiano alla stessa velocità chiamata velocità della luce pari a $c = 3 * 10^8 m/s$. Nei cavi in rame e nelle fibre ottiche tale velocità scende a 2/3 ed è dipendente dalla frequenza. La relazione tra f, λ e c (nel vuoto) è:

$$\lambda f = c \tag{7}$$

La quantità di informazione che un'onda elettromagnetica può trasportare dipende dall'energia ricevuta ed è proporzionale alla sua banda.
Esistono diverse tecniche di suddivisione della banda:

1. spettro distribuito a frequenza variabile: il trasmettitore cambia frequenza centinaia di volte al secondo. Utilizzata in ambito militare per garantire sicurezza (trasmissioni difficili da rilevare e difficili da disturbare).
   È utile in zone dello spettro molto affollate, e viene usata anche per Bluetooth.

2. spettro distribuito a sequenza diretta: usa una sequenza codificata per distribuire il segnale su una banda di frequenza molto più ampia ed è efficente nel permettere a più segnali di condividere le stesse bande di frequenza.
   Ad ogni segnale può essere assegnato un diverso codice mediante CDMA, metodo usato dalle reti 3G e GPS.

3. UWD (ultra wideband): trasmette dati tramite una serie di immpulsi rapidi in posizioni diverse. Il segnale viene disperso su una banda di frequenza molto ampia.

2.3.2 Trasmissioni radio

Le onde in radio frequenza RF sono semplici da generare e attraversano gli edifici. Le onde sono omnidirezionali, si propagano quindi verso tutte le direzioni. Alle frequenze più basse le onde radio attraversano bene gli ostacoli. La potenza diminuisce allontanandosi dalla sorgente (path loss).
Alle frequenze più alte le onde viaggiano in linea retta e rimbalzano contro gli

ostacoli, e vengono assorbite dagli eventi atmosferici.
Le onde radio sono soggette ad interferenze elettriche.
Nelle bande VLF, LF e MF le onde radio seguono il terreno, si possono ricevere fino a 100 km di distanza dalla sorgente e attraversano gli edifici.
Nelle bande HF e VHF le onde terrestri tendono ad essere assorbite dal pianeta, ma le onde che raggiungono la ionosfera sono riflesse.

2.3.3 Trasmissione a microonde

Le microonde non attraversano bene gli edifici. Alcune onde inoltre si possono infrangere sugli strati pù bassi dell'atmosfera e arrivano un po' dopo le onde dirette. Questo fenomeno è chiamato multipath fading e può annullare il segnale.
Le microonde sono anche abbastanza economiche. Le bande a circa 4 Ghz sono facilemnte assorbibili dall'acqua.

Politiche dello spettro elettromagnetico. I governi nazionali assegnano lo spettro per le radio AM e FM, per le TV e i telefoni.
Il problema sorge sui fornitori di servizi, e sono stati utlizzati 3 algoritmi per spartire le frequenze: beauty contest (ogni fornintore doveva motivare il valore della proposta), lotteria, vendita all'asta.
Un altro approccio è quello di non assegnare le frequenze, e regolare la potenza dei dispositivi. Alcune bande di frequenza chiamate ISM sono utilizzate senza licenze, e vengono usate per telecomandi, telefoni senza fili eccetera.

2.3.4 Trasmissione a infrarossi

A corto raggio si utilizzano i raggi infrarossi non vincolati. È un sistema direzionale, economico e facile da realizzare. Non attraversano i muri delle stanze, quindi è possibile utilizzarle per i telecomandi delle TV. Sono più sicuri delle onde radio, non richiedono una licenza.

2.3.5 Trasmissione a onde luminose

Laser montati sui tetti permettono di realizzare una LAN tra due edifici. Questo tipo di sistema è unidirezionale. Non richiede licenze.
Una trasmissione dati può essere realizzata codificando le informazioni come successioni di accensione e spegnimento dei LED a una velocità non percepibile ad un occhio umano.

2.4 Comunicazioni satellitari

Un satellite di comunicazione è un grande ripetitore di microonde collocato nel cielo. Contiene transponder (ricetrasmettitori satellitari), i quali ascoltano ognuno una parte dello spettro, amplificano il segnale e lo ritrasmettono su un'altra frequenza. I raggi puntati posono essere larghi o stretti (bent pipe).
È possibile anche manipolare o ridirigere i flussi di dati all'interno della banda, per poter ridurre il rumore.

2.4.1 Satelliti geostazionari

I satelliti geostazionari, GEO, sono collocati su orbite alte. L'allocazione degli slot orbitali è gestita dall'ITU. I GEO sono molto pesanti, e sono alimentati ad energia solare. Possiedono motori a razzo per permetterne l'allineamento (station keeping). L'ITU assegna anche le bande di frequenza, in quanto arrivate al sottosuole potrebbero interferire con le onde esistenti.
Ogni satellite ha più antenne e trasponder: possono avvenire contemporaneamte più trasmissioni nei due sensi.
Esistono anche microstazioni chamate VSAT, che possiedono antenne piccole e consumano 1 watt di potenza, usate dalle TV satellitari. È necessario installare hub terrestri che trasmettono il traffico attraverso le stazioni VSAT.
Questi satelliti sono mezzi di trasmissione broadcast e quindi è necessario adottare sistemi di crittografia per garantire una sicurezza della comunicazione. Il costo della trasmissione di un messaggio è indipendente dalla distanza attraversata.

2.4.2 Satelliti su orbite medie

Ad altitudini tra le due fasce di Van Alien si trovano i satelliti MEO. Impiegano 6 ore per girare intorno alla Terra, e devono essere seguiti mentre si spostano. Coprono un'area più piccola e sono raggiungibili per mezzo di trasmettitori meno potenti. Un esempio sono i 30 satelliti GPS che operano a circa 20.000 km.

2.4.3 Satelliti su orbite basse

Satelliti LEO. Si spostano rapidamente e sono quindi necessari numerosi satelliti di questo tipo. Ci sono 2 tipi di satelliti LEO:

1. Iridium: quando un satellite spariva dalla vista, ne appariva un altro. Si trovano ad un'altitudine di 750 kmk. È presente un satellite ogni 32 gradi di latitudine.
   Sei collane di satelliti coprono la terra, la comunicazione tra clienti distanti avviene nello spazio: ogni satellite comunica con quello suo limitrofo.

2. Globalstar: 48 satelliti LEO, utilizza un modello bent-pipe (informazioni trasmesse sulla terra subito).

3. Cubesat: piccoli satelliti da 10cm di lato.

2.4.4 Satelliti o fibra ottica?

I satelliti vengono preferiti per scopi militari e vengono usati dove le infrastrutture terrestri non son ancora ben sviluppate, ed anche per i programmi televisivi in broadcast.

2.5 Modulazione digitale e multiplexing

Il processo di conversione tra bit e segnali che li rappresentano prendono il nome di modulazione digitale.

2.5.1 Trasmissione in banda base

Si usa una tensione positiva per rappresentare un 1 e una negativa per rappresentare lo zero (NRZ). In questo modo, il segnale segue l'andamento dei dati.
Il ricevente converte in bit il segnale, campionandolo a intervalli regolari di tempo e decodificandolo assegnando i campioni ai simboli più vicini.

Efficenza di banda. Per sfruttare meglio la banda è possibile utilizzare più di due livelli di segnale.
Il bit rate equivale al symbol rate (tasso con cui il segnale cambia) moltiplicato per il numero di bit in ogni simbolo.
Alcuni dei livelli di segnale sono usati come protezione contro gli errori e semplificano la progettazione.

Clock recovery È necessario che il ricevente conosca quando un simbolo termina. Con NRZ, diventa difficile distinguire i bit.
Come soluzione è possibile spedire al destinatario un segnale di clock separato (spreco di risorse), oppure mandare il segnale di cock in XOR con i dati (Manchester encoding). Questo secondo approccio richiede l'invio del doppio dei dati.
Ci sono anche altri modi per codificare: possiamo codificare 1 come transazione e 0 come una situazione stazionaria (NRZI). Ma lunghe sequenze di 0 possono creare problemi.
Il codice 4B/5B associa ad ogni sequenza di 4 bit una sequenza di 5 bit, scelta in modo tale da non avere più di tre 0 consecutivi (overhead del 25%).
Un altro approccio è lo scrambling, ossia far sembrare i dati come generati casualmente. Uno scrambler applica una XOR tra i dati e una sequenza pseudocasuale. IL ricevente applicherà una XOR ai bit con la stessa sequenza pseudocasuale. Non aggiunge overhead, e i segnali generati tendono ad essere bianchi (energia distribuita su tutte le componenti di frequenza). Non garantisce che non ci saranno lunghe sequenze di bit ripetuti.

Segnali bilanciati I segnali sono bilanciati se hanno una tensione negativa pari a quella positiva (media pari a 0). Il bilanciamento aiuta il clock recovery.
Per formulare un codice bilanciato si usano 2 livelli di tensione per rappresentare 1 (+1V e -1V) e 0V per rappresentare lo 0. Per trasmettere un 1 viene alternato +1V e +1V (codifica bipolare).
Un esempio di codice bilanciato è la codifica di linea 8B/10B, che mappa 8 bit su 10 bit di output (20% overhead).

2.5.2 Trasmissione in banda passante

Per spedire un messaggio spesso si usano gamme di frequenze che non iniziano con lo 0, in quanto esistono vincoli legislativi e per evitare interferenze.
Possiamo prendere una segnale in banda base che occupa da 0 o B Hz e traslarlo fino ad occupare una banda passante da S a S+B Hz, senza cambiare il quantitativo di informazione che può trasportare. Per elaborare il segnale possiamo traslarlo in banda base in modo da avere una più semplice decodifica dei ati.
La modulazione digitale è ottenuta modulando un segnale portante che risiede in banda passante.

1. ASK (Amplitude shift keying): due diverse ampiezze rappresentano 0 e 1. È possibile usare più di 2 livelli per rappresentare più simboli.
2. FSK (Frequency shift keying): è possibile usare due o più frequenze
3. PSK (Phase shift keying): è possibile usare due o più fasi. Ad esempio: BPSK, l'onda portante è traslata di 0 o 180 gradi. QPSK, 4 traslazioni: 45, 135, 225, 315 gradi.

Per trasmettere più bit per simbolo è possibile combinare questi approcci ed usare più livelli. È possibile rappresentare le combinazioni di ampiezza e di fase in un diagramma a costellazioni. Esempi di diagramma a costellazioni: QAM-16 (16 combinazioni di ampiezza e fase per trasmettere 4 bit per simbolo), QAM-64 (64 combinazioni di ampiezza e fase per trasmettere 16 bit per simbolo).
È necessario porre attenzione all'assegnazione dei bit ai simboli, per evitare errori generati dal rumore. Si usa la codifica di Gray, ossia i simboli adiacenti differiscono di un solo bit.

2.5.3 Multiplexing a divisione di frequenza

Per permettere a molti segnali di condividere uno stesso canale trasmissivo sono nate le tecniche di multiplexing.
FDM (Frequency Division Multiplexing) sfrutta la trasmissione in banda passante per condividere un canale: lo spettro viene diviso in bande di frequenza di cui ogni utente ha un uso esclusivo.
L'eccesso di allocazione prende il nome di banda di guardia (guard band) e permette di tenere i canali ben separati tra loro. Un picco ai bordi del canale viene trattato come rumore nel canale adiacente.
FDM è usato ad alto livello nelle reti telefoniche e cellulari, wireless e satellitari.
Per dati digitali viene usato OFDM (Ortogonal frequency division multiplexing), che divide la banda del canale in molte sottoportanti che inviano dati in maniera indipendente. Ogni sottoportante si estende in quelle adiacenti: la risposta in frequenza in corrispondenza del centro delle sottoportanti adiacenti è 0, quindi può essere campionata senza interferenza nella frequenza centrale dai vicini. È necessario un tempo di guardia per ripetere un sottoinsieme dei simboli trasmessi, per ottenere la risposta in frequenza richiesta.

2.5.4 Multiplexing a divisione di tempo

Un'alternativa è TDM (Time Division Multiplexing): gli utenti trasmettono a turno secondo una politica round-robin, prendendo possesso della banda completa. I flussi di bit inviati devono essere sincronizzati nel tempo: per questo vengono usati dei piccoli intervalli (tempi di guardia) per permettere aggiustamenti.
Un altro esempio è STDM, noto come packet switching.

2.5.5 Multiplexing a divisione di codice

CDM (Code Division Multiplexing): è una forma di comunicazione a spettro distribuito in cui un segnale a banda stretta viene sparso su una banda di frequenza più ampia. Le trasmissioni simultanee vengono separate usando la teoria dei codici. CDMA (code division multiple access) è in grado di estrarre il segnale e rifiutare il resto come rumore casuale.
Il funzionamento di CDMA è semplice: il tempo di trasmissione di ogni bit è suddiviso in m intervalli, chiamati chip. Ad ogni stazione viene assegnato un chip sequence (sequenza di chip). Per trasmettere un bit con un valore 1 una stazione invia la sua sequenza di chip, per trasmettere uno 0 la sua negazione.
Esempio: chiamano S il vettore di m chip della stazione s, e $\overline{S}$ la sua negazione.
Tutte le sequenze di chip sono ortogonali a coppie, ossia il prodotto interno normalizzato di ogni coppia distinta di sequenze di chip S e T è zero. Questa sequenza di chip viene generata usando il codice di Walsh.
Quando due stazioni trasmettono contemporaneamente le loro sequenze bipolari si sommano linearmente.
Per recuperare la sequenza di bit generata da una certa stazione, il ricevente deve innanzitutto conoscere in anticipo la sequenza di chip di quella stazione e calcolare il prodotto interno normalizzato tra la sequenza di chip ricevuta e quella della stazione mittente.

2.6 La rete telefonica pubblica commutata

Per poter comunicare con tutto il mondo è possibile usare sistemi di telecomunicazione esistenti. Ad esenpio, la PSTN (public switched telephone network)

2.6.1 Struttura del sistema telefonico

Inizialmente, veniva usata una rete interamente connessa: per poter comunicare con n destinatari, il mittente doveva tirare n cavi, uno per ogni destinatario.
Bell risolvì questo problema, creando uffici di commutazione. La società stendeva cavi dalle case alla commutazione. Per effettuare una chiamata, si chiamava l'ufficio dell'azienda telefonica e un operatore creava un ponte tra il mittente e il destinatario. Per collegare più città venivano usate centraline di secondo livello.
Le connessioni tramite doppine tra ogni telefono e la centrale sono chiamate local loop.
Se i due interlocutori sono collegati alla stessa centrale locale, il meccanismo di

commutazione crea una connessione elettrica diretta, che rimane attiva fino al termine della chiamata.
Se invece sono situati in 2 differenti centrali locali, si attua una chiamata interurbana. Ogni centrale ha diverse linee in uscita che conducono a uno o più centri di commutazione chiamati centrali interurbane. Queste linee sono chiamate linee di connessione interurbana. Se la centrale locale e quella del chiamato hanno una linee di connessione diretta verso la stessa centrale interurbana, è in quest'ultima che si può stabilire una connessione.
Le centrali interurbane comunicano tra loro mediante intertool trunk, linee a banda larga. Esistono meccanismi di instradamento flessibili e non gerarchici (in precedenza era gerarchico).
In passato la trasmissione era analogica, ora tutte le linee e i commutatori sono digitali, solo l'ultimo miglio è ancora analogico.
La tramissione digitale è preferibile, perchè basta poter distinguere uno 0 da un 1 invece che riprodurre in modo accurato una forma d'onda.

2.6.2 Politiche telefoniche

Dal 1995 ogni società può offrire ai propri clienti un singolo pacchetto integrato, comprendente TV via cavo, telefonia e servizi d'informazione. È imposta l'implementazione di portabilità del numero locale.

2.6.3 Collegamenti locali: modem, ADSL, fibre

Il collegamento locale è l'ultimo miglio.

Modem telefonici. Per spedire dei bit questi devono essere convertiti in segnali analogici.
i Un modem (modulatore demodulatore) converte un flusso di bit in analogico. Può essere interno od esterno ad un computer. Un modem si colloca tra tra il computer e il sistema telefonico.
Un modem telefonico permette di inviare bit tra due computer su una linea telefonica. Per ridurre gli errori, gli standard impolgono alcuni simboli per la correzione degli errori, ad esempio TCM (Trellis Coded Modulation).
Lo standard V.32 usa una costellazione a 32 punti per condividere 4 bit di dati, e 1 bit di controllo per ogni simbolo. Esistono anche V.90 e V.92.

Linee DSL Gli xDSL sono offerte che promettono più banda della connessione telefonica. Un esempio è l'ADSL.
La linea in ingresso viene collegata a un commutatore che non presenta il filtro usato nelle comunicazioni vocali. Questo permette una maggiore velocità di trasmissione perchè rende disponibile l'intera capacità del collegamento locale.
La capacità del collegamento locale dipende anche dalla lunghezza, il diametro dei cavi e la sua qualità.
I servizi xDSL devono funzionare su doppini Cat.3 esistenti, non devono influenzare i dispostivi telefonici, ed è molto più veloce della connessione a 56kbps.

Hanno un costo mensile indipendentemente dal tempo di utilizzo.
Per trasmettere dati su questi canali viene usata la tecnica OFDM, chiamata in questo contesto DMT (discrete multitone). Il canale viene usato per il POTS (il servizio telefonico), i canali da 1 a 5 funzionano come guardia (non vengono utilizzati per evitare interferenze), 1 canale è usato per controllare il canale in upstream, uno per quello in downstream, mentre i rimanenti 248 sono utilizzati per trasmettere i dati degli utenti.
Per evitare interferenze, 32 canali vengono usati per la trasmissione e i rimanenti per la ricezione. Da questo fatto deriva il termine ADSL (Asymmetric DSL).
Una configurazione ADSL si effettua nel seguente modo: un tecnico installa nell'edificio del cliente un NID (Network Interface Device). Accanto al NID c'è uno splitter, filtro analogico che divide i dati della banda da 0 a 4000 Hz, usata da POTS da quella dei dati. I dati sono instradati verso un modem ADSL.
Lo svantaggio è che è necessario un intervento di un tecnico per installare il NID e lo splitter.

FTTH - Fiber to to home Questa tecnologia permette una velocità di accesso fino a 100 Mbps. L'ultimo miglio in fibra è passivo, non è necessario utilizzare apparati attivi per amplificare o elaborare il segnale.
Dato che le fibre provenienti dalle case sono unite tra loro (ad esempio, una fibra parte dalla centrale e arriva a 100 abitazioni), vengono utilizzati dei splitter (separatori ottici) che dividono il segnale proveniente dalla centale locale alle varie abitazioni. Questa architettura si chiama PON (passive optical network): si una sola lunghezza d'onda per tutte le abitazioni per la trasmissione in upstream e un'altra per la trasmissione in downstream.
È necessario però definire un protocollo di comunicazione: non è possibile che gli utenti inviino un messaggio nello stesso momento, perchè potrebbero collidere, e non possono ascoltare a vicenda le proprie trasmissioni (quindi non possono controllare il canale prima di effettuare la trasmissione. È necessaria una sincronizzazione tra apparato locale e centrale.

2.6.4 Trunk e multiplexing

Un trunk è un segmento principale di una rete telefonica e permette di collegare tra loro i centri di commutazione. Differiscono dall'ultimo miglio sia dalla velocità (offrono una maggiore velocità), sia dalla dimensione (trasportano tantissime chiamate simultaneamente). Inoltre la parte interna della rete trasporta informazioni digitali e non analogiche, quindi è necessaria una conversione alla centale locale per trasmettere sui trunk a lunga distanza.

Digitalizzazione di segnali vocali I segnali analogici sono digitalizzati da un codec, dispositivi che estra 8000 SWAG campioni al secondo. Questa tecnica è chiamata PCM (Pulse Code Modulation).All'altro capo viene ricreato un segnale analogico dai campioni quantizzati.

I livelli di quantizzazione sono distanziati tra loro in maniera non uniforme secondo una scala logaritmica per evitare errori.

Time division multiplexing vedi libro...

2.6.5 Commutazione

Commutazione di circuito Quando una chiamata passa attraverso una centrale di commutazione, viene stabilita una connessione fisica tra la linea di provenienza della chiamata e una linea di uscita.
Inizialmente, un operatore creava la connessione. Ora c'è una macchina.
È necessario configurare un percorso da un punto all'altro prima di iniziare a trasmettere i dati.

Commutazione di pacchetto È un'alternativa alla commutazione di circuito. I pacchetti vengono inviati non appena sono disponibili. Non c'è un percorso stabilito in anticipo, quindi i pacchetti possono anche arrivare in ordine disordinato e se un commutatore si blocca è possibile aggirarlo. È necessario fissare un limite superiore alla dimensione dei pacchetti, per evitare una monopolizzazione del sistema.
Non c'è prenotazione di banda, quindi può accadere un ritardo di accomodamento e congestione della rete se molti pacchetti vengono spediti nello stesso momento. È più efficente in quanto non viene sprecata banda.

2.7 Il sistema telefonico mobile

Il sistema telefonico è usato per comunicazioni a grande distanza, sia vocali che dati. Si sono successe 3 generazioni:

1. 1G: voce analogica
2. 2G: voce digitale
3. 3G: voce e dati digitali

Attualmente c'è la generazione 4G. Il primo sistema mobile è stato sviluppato negli USA, e funzionava per tutto il territorio statunitense.
Ora gli USA usano due sistemi digitali mobili, incompatibili tra loro. In USA i telefoni cellulari sono mischiati ai telefoni fissi, e i possessori di telefoni cellulari pagano le chiamate in arrivo.
In Europa, sebbene inizialmente ogni stato aveva un proprio sistema analogico cellulare, ora c'è un unico sistema digitale. Questo ha permesso una diffusione più grande rispetto agli Stati Uniti. In Europa c'è un ampio uso delle schede prepagate, e i telefoni cellulari non sono mischiati ai telefoni fissi (è semplice capire se il chiamante sta chiamando da un telefono fisso oppure da un cellulare).

2.7.1 Prima generazione (1G): voce analogica

Nel 1946 venne creato il primo sistema telefonico per auto. Veniva usato un sistema push-to-talk.
Negli anni '60, si iniziò ad utilizzare IMTS: un trasmettitore ad alta potenza veniva installato in una zona elevata e venivano usate 2 frequenze: una per la trasmissione ed una per la ricezione. Gli utenti non potevano ascoltarsi.

AMPS - advanced mobile phone system Sistema inventato da Bell Labs nel 1982. In Inghilterra e in Italia veniva chiamatao TACS, e in Giappone LCS-LI. AMPS è stato si è ritirato nel 2008.
Nei sistemi mobili un'area geografica viene divisa in celle. In AMPS le celle sono grandi 10-20 km. Ogni cella utilizza delle frequenze non usate da quelle vicine.
Usando questo sistema ci sono stati molti miglioramenti: vengono gestite più chiamate contemporaneamente in una zona più ristretta rispetto ai sistemi precendenti, e le celle sono più piccole (quindi vengono usati trasmettitori e dispositivi più piccoli ed economici).
Le celle hanno tutte la stessa dimnesioni e sono organizzate in gruppi di 7, e ogni lettera indica un gruppo di frequenze. C'è un'area cuscinetto attorno ad ogni cella, per separare le frequenze.
Se il sistema si satura, è possibile usare microcelle più piccole per aumentare il riuso di frequenze, oppure usare microcelle temporanee utilizzando torri portatili.
Al centro di ogni cella c'è una stazione base. Questa stazione comunica con tutti i telefoni nella cella. La stazione è composta da un computer e da un trasmettitore/ricevitore collegato all'antenna.
Le stazioni base sono collegate ad un dispositivo chiamato MSC (mobile switch center). Possono esserci più MSC che comunicano tra loro mediante una rete a commutazione di pacchetto.
Ogni telefono è collegato in una specifica cella. Quando si allontana dalla cella, la stazione trasferisce la gestione dell'apparecchio alla cella che riceve il segnale più forte. Questo processo è chiamato handoff.

Canali AMPS usa FDM. Usa 832 canali full duplex, ognuno costituito da canali simplex (FDD, Frequency Division Duplex). I canali sono divisi in 4 categorie:

1. controllo per gestire il sistema
2. paging per avvisare gli utenti mobili di chiamate in arrivo
3. accesso per impostare la chiamata e l'assegnazione del canale
4. dati per vece, fax o dati.

Gestione delle chiamate Ogni telefono mobile possiede un numero seriale (32 bit) e un numer.o telefonico di 10 cifre, registrato nella memoria.
Il numero telefonico è composto da prefisso (3 cifre) e il numero vero e proprio (7 cifre).
All'accensione il telefono cerca il segnale più potente e trasmette a questo i 2 numeri sottoforma di pacchetto digitale, più volte e con un codice di correzione degli errori. La stazione base aggiorna l'MSC, che registra la presenza del cliente, e informa l'MSC principale del cliente.
I telefoni inattivi rimangono in ascolto sul canale di trasferimento per rilevare eventuali messaggi inviati a loro.

2.7.2 Seconda generazione (2G)

Con questa generazione abbiamo un guadagno di capacità trasmissiva grazie alla digitalizzazione e compressione della voce. È possibile inviare sms.

GSM GSM (Global System for Mobile communications) è diventato lo standard europeo per il 2G. Mantiene l'handoff e la struttura a celle.
Il terminale mobile GSM è diviso in dispositivo e chip chiamato SIM. La SIM permette al telefono di funzionare correttamente ed è usata anche come supporto di memorizzazione. La SIM scambia dati con la rete per permettere l'identificazione.
Il telefono parla con la stazione base mediante una air interface.
Le stazioni base sono collegate a un BSC che gestisce le risorse radio delle celle e gli handoff.
Il BSC è collegato ad un MSC che instrada le chiamate e si connette alla PSTN.
Un database chiamato VLR permette all'MSC di sapere dove sono i dispositivi.
HLR invece permette di instradare le chiamate in arrivo verso le giuste posizioni.

2.7.3 Terza generazione (3G)

2.8 Televisione via cavo

2.8.1 Televisione ad antenna collettiva

2.8.2 Internet via cavo

2.8.3 Allocazione dello spettro

2.8.4 Cable modem

2.8.5 ADSL o connessione via cavo?

3 Il livello data link

3.1 Progettazione del livello data link

Permette di:

1. fornire un'interfaccia di servizio per il livello di rete
2. gestire gli errori di trasmissione
3. gestire il flusso di dati

Data Link incapsula i pacchetti del livello di rete in frame. Ogni frame contiene una intestazione, una sezione per contenere il pacchetto ed una sequenza di chiusura.

3.1.1 Servizi forniti al livello di rete

Il livello data link offre questi servizi al livello rete:

1. servizio senza conferma senza connessione: sorgente invia dei frame indipendenti alla destinazione, senza conferma dell'avvenuta ricezione. Usato quando la frequenza degli errori di trasmissione è molto basso (Ethernet).
2. servizio con conferma senza connessione: ciascun frame è inviato individualmente ma ne viene data conferma di ricezione. Usato sulle connessione Wi-Fi.
3. servizio con conferma orientato alla connessione: viene stabilita una connessione prima di iniziare a trasferire i dati. Garantito l'ordine dei pacchetti, usato su canali satellitari. Il trasferimento avviene in 3 fasi: stabilire connessione, trasmissione, rilascio connessione.

3.1.2 Suddivisione in frame

Data Link suddivide il flusso di bit in una serie di frame. Per ogni frame calcola un checksum (inserito poi all'interno del frame). Per verificare che non ci sono stati errori, il destinatario ricalcola il checksum e lo controlla con quello inviato. Per facilitare al destinatario la suddivisione in frame ci sono 4 metodi:

1. conteggio dei byte: un campo dell'intestazione usato per specificare il numero di byte nel frame. Il problema è che il campo può essere compromesso da un errore di trasmissione.
2. flag byte con byte stuffing: inseriti byte speciale all'inizio e alla fine di ogni frame, chiamati flag byte. Se il flag byte compare nei dati, si usa un byte di escape prima di ogni occorrenza accidentale del flag byte.
3. flag bit con bit stuffing: simile al byte stuffing ma a livello di bit: ogni frame inizia e finisce con una sequenza di bit specifica, ogni 5 bit 1 consecutivi viene inserito uno 0. Usato da USB.

4. violazioni della codifica del livello fisico: si possono usare segnali riservati per indicare l'inizio e la fine di un frame usando un code violation.

3.1.3 Controllo degli errori

Il protocollo richiede che la destinazione invii sulla rete dei frame di controllo contenenti un ACK. Viene anche introdotto un timer: quando la sorgente invia un pacchetto, fa partire un timer. Se la sorgente non riceve l'ACK entro la scadenza del timer, vuol dire che la il frame è andato perso e verrà reinviato.
Ogni frame ha un numero di sequenza.

3.1.4 Controllo di flusso

Il controllo del flusso viene attuato mediante feedback (destinazione manda permesso alla sorgente di inviare altri dati) o tramite limitazione del tasso di invio.

3.2 Rilevazione e correzione degli errori

Per poter combattere gli errori di trasmissione, vengono usate 2 strategie:

1. includere informazioni ridondanti per permettere al destinatario di dedurre i dati spediti (codici a correzione di errore)
2. includere informazioni per permettere al destinatario di capire se i dati contengono errori, e richiedere una nuova trasmissione (codici a rilevazione d'errore).

Nella fibra ottica (canale affidabile) è meglio usare i secondi.
Su canali ad alto tasso di errore (wifi ad esempio) è meglio usare i primi.

3.2.1 Codici a correzione di errore

1. codice di Hamming
2. codice convoluzionale binaria
3. codice di Reed-Solomon
4. codice a controllo a bassa priorità

Un frame consiste di m+r bit, dove m sono il numero di bit di dati e r il numero di bit di controllo.
In un codice a blocco, gli r bit di controllo sono calcolati in funzione degli m bit di dati.
In un codice sistematico, gli m bit di dati sono trasmessi insieme a quelli di controllo.
In un codice lineare gli r bit di controllo sono una funzione lineare degli m bit

di dati quali lo XOR o la somma modulo 2.
Il codice di un frame lo identifichiamo con codice(n,m).
Un'unità di n bit che contiene sia dati che controllo è chiamato codeword di n bit.
Date 2 sequenze, il numero di bit corrispondenti diversi nelle 2 sequenze è detto disanza di Hamming. Se 2 parole di codice sono a distanza Hamming d una dall'altra, saranno necessari d erori su singoli bit per convertire una sequenza nell'altra.
Per trovare d errori è necessaria una codifica con distanza d+1.
Per correggere d errori, è necessaria una codifica con distanza 2d+1
Se abbiamo m bit di messaggio, è possibile fissare un limite inferiore al numero di bit di controllo usando la disuguaglianza:

$$(m + r + 1) <= 2^r \tag{8}$$

In Hamming, i bit della parola di codice vengono numerati. I bit che sono una potenza di 2 vengono usati come bit di controllo, i restanti sono gli m bit di dati.
Ogni bit di controllo forza la somma modulo 2 o parità di alcuni bit di dati (incluso se stesso) ad essere pari (o dispari).
Un bit può essere incluso in più calcoli di bit di controllo.
UN bit di dati è controllato solo dai bit di controllo presenti nella sua espansione in somma di potenze di 2.
Il destinatario ricalcola i bit di controllo, includendo i valori di quelli appena ricevuti: i bit ottenuti prendono il nome di check result. Se tutti i bit del check result sono 0, allora la parola è valida.
L'insieme dei risultati di controllo forma la sindrome d'errore.
I codici di Hamming sono utilizzati nei dispositivi di memorizzazione.
Il codice convoluzionale non fissa a priori una dimensione del messaggio, l'output dipende dai di input correnti e da quelli precedenti. Il numero di bit precedenti su cui si basa la codifica è chiamato lunghezza dei vincoli del codice.
Vengono utilizzati nelle reti GSM, e nelle comunicazioni satellitari.
I codici di Reed Solomon operano a gruppi di m simboli di bit, e si basano sul fatto che un polinomio di grado n è univocamente determinato da n+1 punti. Questi codici infatti sono definiti come polinomi che operano su campi finiti. Con simboli di m bit le parole sono lunghe $2^m - 1$. Se poniamo m = 8 abbiamo che i simboli sono byte, e una parola è lunga 255 byte. Vengono usati nelle DSL, nei CD e nei DVD.Sono anche usati in combinazione con altri codici.
Il codice LDPC (low-density parity check) definisce che ogni bit di output è formato solo da una frazione dei bit in input. Le parole ricevute vengono decodificate con un algoritmo di approsimazione.

3.2.2 Codici a rilevazione di errore

1. Parità: un bit di parità viene aggiunto in coda ai dati, in modo tale che il numero di 1 nella parola sia dispari o pari. Con un singolo bit di parità, abbiamo un codice con distanza 2, ed è in grado di rilevare errori su singoli

bit.
Per poter rilevare anche errori a burst viene usata una tecnica chiamata interleaving. Se consideriamo ogni blocco da inviare come una matricec n*m, con questa tecnica possiamo calcolare il bit di parità per ognuna delle n colonne e trasmettiamo i bit come m righe. Come ultima riga abbiamo i bit di parità.

2. checksum: usato per indicare un gruppo di bit di controllo associati al messaggio.

3. : CRC (Cyclic Redundancy Check, o codifica polinomiale): sequenze di bit vengono viste come dei polinomi a coefficienti, che possono assumere solo i valori 0 e 1.
   La sorgente e la destinazione devono mettersi d'accorso su un polinomio generatore, G(x). G(x) deve avere i bit di ordine più alto e più basso pari a 1.
   Per calcolare il checksum di un frame di m bit (visto come un polinomio M(x)), questo frame deve essere più lungo del polinomio generatore. L'algoritmo per calcolare il checksum è il seguente:

   (a) se r è il grado di G(x), aggiungiamo r bit con valore 0 dopo la parte di ordine più basso del frame, così che contenga m + r bit (polinomio $x^R M(x)$).

   (b) dividiamo la sequenza di $x^R M(x)$ per la sequenza di G(x), usando la divisione modulo 2.

   (c) sottraiamo il resto (che contiene massimo r bit) dalla sequenza di $x^R M(x)$ usando la sottrazione modulo 2. Il risultato è il frame di checksum T(x).

   Ci sono polinomi diventati standard internazionali, come quello di Ethernet, che permette di rilevare tutti gli errori di burst di lunghezza pari o minore a 32 bit.

3.3 Protocolli data link elementari

I processi del livello fisico e alcuni del livello data link vengono eseguiti su una NIC (scheda di rete) oppure sulla CPU sottoforma di device driver. Quando il livello data link accetta un pacchetto, lo incapsula in un frame aggiungendo un'intestazione (header) e una coda (trailer). Quando un frame arriva a destinazione, l'hardware ne calcola il checksum.
Una dichiarazione comune di un protocollo è composta da 5 strutture dati:

1. boolean

2. seq_nr, numero intero usato per numerare i frame

3. packet, unità di informazione che viene scambiata fra il livello di rete e quello data link

4. frame, composto da 4 campi: kind (indica se ci sono dati nel frame), seq (numeri di sequenza), ack (acknowledgement) (questi primi 3 sono definiti come frame header in quanto di controllo), e info (i dati da trasferire).

5. frame_kind

Alcune funzioni di libreria sono le seguenti:

void wait_for_event(event_type *event)	aspetta che accada un evento
void from_network_layer(packet *p)	prende un pacchetto dal liv. rete
void to_network_layer(packet *p)	porta il pacchetto arrivato al liv. rete
void from_physical_layer(frame *r)	prende un frame dal liv. fisico e lo copia in r
void to_physical_layer(frame *s)	passa il frame al liv. fisico
void start_timer(seq_nr k)	fa partire l'orologio, e abilita l'evento di timeout
void stop_timer(seq_nr k)	ferma l'orologio, e disabilita l'evento di timeout
void start_ack_timer(void)	fa partire il timer ausiliario, e abilita ack_timeout
void stop_ack_timer(void)	stoppa il timer ausiliario, e disabilita ack_timeout
void enable_network_layer(void)	abilita il livello di rete a scatenare eventi net_layer_ready
void disable_network_layer(void)	disabilita il livello di rete a scatenare eventi net_layer_ready

3.3.1 Un protocollo simplex utopistico

Questo protocollo permette la trasmissione dei dati in una sola direzione. Viene assunto che il canale sia privo di errori, e che la destinazione possa elaborare l'input a velocità infinita. La sorgente invia i dati alla velocità massima.
Non è necessario specifica ACK e MAX_SEQ perchè può arrivare solo un frame intatto (frame_arrival).

Listing 1: simplex utopistico

```
void sender1(void){
        frame s;
        packet buffer;

        while(true){
                from_network_layer(&buffer);
                s.info = buffer;
                to_physical_layer(&s);
        }
}

void receiver1(void){
        frame r;
        event_type event;

        while(true){
```

```
                wait_for_event(&event);
                from_physical_layer(&r);
                to_network_layer(&r.info);
        }
}
```

3.3.2 Un protocollo simplex stop-and-wait per un canale privo di errori

Come gestire il traffico? Il destinatario deve mandare feedback al mittente. Dopo aver passato il pacchetto al liv. network, il destinatario invia un pacchetto dummy al mittente. Il mittente è obbligato ad aspettare finchè non riceve il pacchetto dummy di ACK.

Listing 2: simplex stop-and-wait senza errori

```
void sender1(void){
        frame s;
        packet buffer;
        event_type event;
        while(true){
                from_network_layer(&buffer);
                s.info = buffer;
                to_physical_layer(&s);
                wait_for_event(&event);
        }
}

void receiver1(void){
        frame r,s;
        event_type event;

        while(true){
                wait_for_event(&event);
                from_physical_layer(&r);
                to_network_layer(&r.info);
                to_physical_layer(&s);
        }
}
```

3.3.3 Protocollo simplex stop-and-wait per un canale soggetto a rumore

In questo caso possono verificarsi errori: il pacchetto può venire danneggiato o addirittura perso.
Come procedere? Viene aggiunto un timer, e un metodo per permettere alla

destinazione di distinguere i frame che vede per la prima volta.
Se il frame m viene perso o danneggiato, viene inviato l'ACK corrispondente al pacchetto precedente.

Listing 3: simplex stop-and-wait con canale con errori

```
#define MAX_SEQ 1

void sender3(void){
        seq_nr next_frame_to_send;

        frame s;
        packet buffer;
        event_type event;

        next_frame_to_send = 0;
        from_network_layer(&buffer);

        while(true){
                s.info = buffer;
                s.seq = next_frame_to_send;
                to_physical_layer(&s);
                start_timer(s.seq);
                wait_for_event(&event);
                if(event == frame_arrival){
                        from_physical_layer(&s);
                        if(s.ack == next_frame_to_send){
                                stop_timer(s.ack);
                                from_nextwork_layer(&buffer);
                                inc(next_frame_to_send);
                        }
                }
        }
}

void receiver3(void){
        seq_nr frame_expected;
        frame r,s;
        event_type event;

        while(true){
                wait_for_event(&event);
                if(event == frame_arrival){
                        from_physical_layer(&r);
                        if(r.seq == frame_expected){
                                to_network_layer(&r.info);
                                inc(frame_expected);
```

```
                        }
                        s.ack = 1 - frame_expected;
                        to_physical_layer(&s);
                }
        }
}
```

3.4 Protocolli a finestra scorrevole

I protocolli precedenti erano simplex(i dati venivano trasmessi solo in una direzione).
Sarebbe meglio trasmettere in duplex (entrambe le direzioni).
Ci sono diversi modi per farlo: o si usano 2 canali separati, uno per l'andata (dati) e uno per ritorno (ack) (ma in questo modo la banda del canale di ritorno risulterebbe sprecata), oppure usare un unico canale per entrambe le direzioni.
È possibile fare questo usando una tecnica chiamata piggybacking (ritardare gli ack in uscita ed agganciarli al successo frame di dati trasmesso).
Se il pacchetto da inviare arriva rapidamente, allora viene fatt o piggybacking, sennò l'ack viene inviato da solo.
Particolari protocolli sono i protocolli a finestra scorrevole. In ogni istante la sorgente memorizza un insieme di numeri di sequenza, che corrispondono ai frame che è autorizzata a inviare. I frame che possono essere inviati si trovano sulla finestra di invio. La destinazione tiene traccia della finestra di ricezione (frame che è autorizzata a ricevere). Queste finestre possono avere dimensione fissa oppure variabile.
Quando arriva un nuovo pacchetto dal livello di rete, gli viene assegnato il numero di sequenza successivo e la finestra viene incrementata di 1. Quando arriva un ACK, viene incrementato di 1 il limite inferiore della finestra.
È necessario mantenere un buffer della stessa dimensione della finestra per mantenere in memoria eventuali frame persi o danneggiati durante la trasmissione e cha vanno spediti di nuovo.
In ricezione, se arriva un frame con un numero di sequenza non compreso nella finestra, questo frame viene scartato.
Se la dimensione della finestra è 1, i frame arrivano sempre nella giusta sequenza.

3.4.1 Un protocollo a finestra scorrevole a 1 bit

Questo protocollo utilizza il metodo stop-and-wait. La sorgente invia un frame e poi aspetta di ricevere l'ACK prima di inviare il successivo.

Listing 4: protocollo a finestra scorrevole a 1 bit

```
#define MAX_SEQ 1 /*la finestra ha dimensione 1*/

void protocol4(void){
```

```
        seq_nr next_frame_to_send;
        seq_nr frame_expected;

        frame r, s;
        packet buffer;
        event_type event;

        next_frame_to_send = 0;
        frame_expected = 0;
        from_network_layer(&buffer);
        s.info = buffer;
        s.seq = next_frame_to_send;
        s.ack = 1 - frame_expected; /* ack in piggybacking*/
        to_physical_layer(&s);
        start_timer(s.seq);

        while(true){
                wait_for_event(&event);
                if(event == frame_arrival){
                        from_physical_layer(&r);
                        if(r.seq == frame_expected){
                                to_network_layer(&r.info);
                                inc(frame_expected);
                        }
                        if(r.ack == next_frame_to_send){
                                stop_timer(r.ack);
                                from_nextwork_layer(&buffer);
                                inc(next_frame_to_send);
                        }
                }
                s.info  = buffer;
                s.seq = next_frame_to_send;
                s.ack = 1 - frame_expected;
                to_physical_layer(&s);
                start_timer(s.seq);
        }
}
```

3.4.2 Un protocollo che usa go-back-n

Per permettere alla sorgente di non aspettare l'ACK, è possibile mandare un numero w di frame maggiore di 1. Gli ACK arriveranno per i frame precedenti prima che la finestra si riempi.
Per calcolare l'opportuno w, si calcola la bandwith-delay product (banda (bit/s) del canale * tempo di transito in una direzione). Dividendo questa grandezzza per il numero di bit per frame si ottiene il numero di frame (BD). w deve essere

pari a 2BD + 1.
Per piccole finestre, a volte la sorgente rimarrà bloccata e quindi l'utilizzazione sarà inferiore al 100%.
La tecnica che consiste nel tenere più frame in viaggio viene chiamata pipeling.
Per ripristinare gli errori in presenza di pipeling sono previsti due approcci. Il primo è go-back-n: la destinazione scarta tutti i frame successivi all'errore, senza mandare l'ACK per questi frame scartati (finestra di ricezione di dimensione 1). (vedi libro per l'implementazione, pag. 222-223)
La sorgente può trasmettere fino a MAX_SEQ senza dover aspettare un ACK. Il livello di rete scatena un evento network_layer_ready quando c'è un pacchetto da inviare. Quando arriva l'ACK per il frame n, anche i frame precedenti hanno l'ACK (cumulative acknowledgement).

3.4.3 Un protocollo che usa selective-repeat

L'altra strategia è chiamata selective-repeat (pag.226/227 per l'implementazione).
Sorgente e destinazione mantengono una finestra di numeri di sequenza accettabili. La finestra sorgente ha dimensione variabile, da 0 a max, mentre la destinazione ha un buffer di dimensione fissa pari a max. La destinazione ha un buffer riservato per ogni numero di sequenza all'interno della sua finestra. Ad ogni buffer è associato un bit (arrrival) che identifica quando il buffer è pieno o vuoto. Quando arriva un frame viene controllato che il numero di sequenza si trovi all'interno della finestra.
Il frame, prima di essere passato al livello rete, viene trattenuto finchè tutti i frame con numeri di sequenza inferiori siano stati ricevuti e passati al liv. network (per garantire l'ordine).
La ricezione non è sequenziale. Questo comporta a dei problemi, ad esempio l'invio di una sequenza di frame già ricevuta.
Per risolvere questo problema, dobbiamo essere sicuri che quando la destinazione ha portato avanti la sua finestra non ci siano sovrapposizioni con la finestra della sorgente. Per risolvere questo problema, si pone come dimensione massima della finestra (MAX_SEQ+1)/2.
Per evitare che il protocollo si blocchi quando la finestra della sorgente si sarà riempita, viene fatto partire un timer ausiliario dopo l'arrivo di una sequenza di frame. Se scade il timer, viene inviato un ACK di ritorno.
Se la destinazione sospetta un errore, viene inviato un NAK (negative ACK), necessario per rispedire il frame.

3.5 Esempi di protocolli data link

Analizziamo ora protocolli data link su collegamenti punto a punto di Internet. Questo tipo di protocolli è chiamato PPP (Point to Point Protocol).

3.5.1 Pacchetti su SONET

SONET è il protocollo di liv. fisico usato nei collegamenti in fibra ottica delle WAN.
È necessario disporre di meccanismi di framing che distinguano i pacchetti occasionali dal flusso di bit continuo in cui vengono trasportati.
Il protocollo PPP ha 3 caratteristiche:

1. un metodo di framing, che permette di delimitare la fine e l'inizio di un frame.
2. protocollo per gestire la connessione, ad esempio il test della linea o le opzioni di collegamento, e gestire la disconnessione (LCP, Link Control Protocol).
3. modalità per negoziare le opzioni relative al livello di rete, in modo indipendente dall'implementazione.

Il formato del frame PPP assomiglia a quello HDLC.
PPP è orientato ai byte e usa il byte stuffing, fornisce trasmissioni affidabili anche nel caso di canali soggetti a rumore.
Formato frame PP:

1. flag byte standard HDLC (0x7E)
2. Address, impostato a 11111111.
3. Control, default 00000011 (frame senza numero).
4. Protocol, per comunicare quale tipo di pacchetto è contenuto nel campo payload.
5. Payload, lunghezza variabile.
6. Checksum, 2 o 4 byte. (CRC)
7. Flag di chiusura.

Il collegamento PPP deve essere stabilito e configurato. Le fasi di attivazione sono:

1. DEAD, liv. fisico non esiste connessione.
2. ESTABILISH, stabilita connessione ottica.
3. AUTHENTICATE, sorgente e destinazione possono verificare le proprie identità.
4. NETWORK, fase di configurazione del liv. rete
5. OPEN, trasmissione di pacchetti IP in frame PPP su linea SONET.
6. TERMINATE, fine trasmissione.

3.5.2 ADSL

L'ADSL utilizza diversi protocolli. Questi protocolli si basano su OFDM (multiplazione a divisione di frequenza ortogonali).
Viene utilizzato PPP. A metà tra l'ADSL e PPP troviamo ATM, un livello data link che si basa su celle di informazione a lunghezza fissa. Non è necessario, come in SONET, che le celle vengano inviate secondo un flusso continuo e sincrono di bit, ma solo quando bisogna necessariamente comunicare.
ATM è orientato alla connessione; ogni cella possiede un identificatore di circuito virtuale, che viene usato per indirizzare la cella lungo il percorso di una connessione già stabilita. Per spedire dei dati è necessario associarli a una sequenza di celle. Il livello AAL5 si occupa di segmentare e riassemblare i dati. AAL5 al posto di un'intestazione è dotato di un trailer contenente la lunghezza e un CRC di 4 byte. Un frame AAL5 può contenere byte di padding per rendere la lunghezza multiplo di 48 byte.
Per la correzione degli errori oltre a CRC viene aggiunta alla codifica del liv. fisico di ADSL una codifica Reed-Solomon ed un ulteriore CRC.

4 Il sottolivello MAC

Il sottolivello MAC è la parte inferiore del liv. data link e riguarda soprattutto i canali broadcast.
Le reti wireless si servono per la connessione di un canale ad accesso multiplo (broadcast), le WAN invece preferiscono le connessione punto a punto.

4.1 Problema dell'allocazione del canale

Come allocare un canale di trasmissione?

4.1.1 Allocazione statica del canale

Per allocare staticamente un canale, possiamo dividere la sua capacità usando FDM. Se ci sono N utenti, la larghezza di banda è divisa equamente in N parti. Non ci sono interferenze tra gli utenti (es stazione radio FM).
Se ci sono meno di N utenti, si spreca parte dello spettro. Se ci sono più di N utenti, alcuni non potranno comunicare.
Calcoliamo il ritardo medio T relativo alla spedizione di un frame su un canale con capacità C bps. Assumiamo che il tasso medio degli arrivi casuali sia λ frame/s e che ogni frame abbia lunghezza variabile, con una media di 1/u bit. Il tasso di servizio del canale è uC.

$$T = \frac{1}{uC - \lambda} \tag{9}$$

Dividiamo il canale in N sottocanali indipendenti, ognuno di capacità C/N bps. Il tasso medio d'ingresso sarà λ/N. Ricalcoliamo T:

$$T = \frac{1}{u(C/N) - (\lambda/N)} = \frac{N}{uC - \lambda} = NT \tag{10}$$

4.1.2 Ipotesi per l'allocazione statica di canali dinamici

Ci sono 5 premesse da fare:

1. Traffico indipendente: l'arrivo di ogni frame è indipendente dagli altri arrivi
2. Canale singolo: la comunicazione avviene in un solo canale.
3. Collisioni osservabili: possono verificarsi collisioni se 2 frame vengono trasmessi simultaneamente.
4. Tempo continuo o diviso in intervalli.
5. Rilevamento di portante o non rilevamento di portante.

4.2 Protocolli ad accesso multiplo

4.2.1 ALOHA

Hawai, anni 70. Per connettere gli utenti delle varie isole al computer principale, vennero usate onde radio a corto raggio, dove ogni terminale utilizzava la stessa frequenza di upstream per spedire i frame al computer locale.

ALOHA pure Dopo che ogni stazione ha spedito il frame, il computer locale lo rispedisce in broadcast a tutte le stazioni. Una stazione trasmittente può ascoltare la trasmissione del coordinatore (hub) per controllare se il frame è arrivato a destinazione.
Se il frame è andato perso, il trasmettitore attende un tempo casuale prima di rispedirlo. Casuale perchè se più frame vengono rispediti nello stesso istante, alla prossima collisione cambieranno il loro tempo d'attesa e non collideranno.
I sistemi dove più utenti condividono un canale in cui possono generarsi conflitti si chiamano sistemi a contesa.
Tutti i frame utilizzati su ALOHA hanno la stessa lunghezza per massimizzare la capacità di trasporto del sistema. Se due frame occupano contemporaneamente il canale vengono danneggiati.
In ALOHA puro una stazione non ascolta il canale prima di cominciare a trasmettere. La probabilità che k frame siano generati durante un dato tempo di frame è data dalla distribuzione di Poisson:

$$Pr[k] = \frac{G^k e^{-G}}{k!} \tag{11}$$

Un frame non entrerà in collisione se nessun altro frame sarà trasmesso nello stesso intervallo temporale.
La probabilità di generare zero frame è e^{-G}. In un intervallo di due frame time (intervallo di tempo per trasmettere un frame di lunghezza standard e fissa), il numero medio di frame generati è pari a 2G. S = Ge^{-2G}.
La capacità di trasporto massima si ha con G = 0,5 e con S=$\frac{1}{2e}$. Si spera di utilizzare al massimo il 18% del canale.

ALOHA slotted Per duplicare la capacità di ALOHA, viene diviso il tempo in slot (intervalli discreti), ognuno corrispondente ad un frame. Gli utenti devono concordarsi sui limiti degli intervalli.
È possibile utilizzare una stazione che si occupa di emettere un segnale all'inizio di ogni intervallo.
La probabilità che non ci sia altro traffico durante lo stesso intervallo occupato dal frame è pari a $e * -G$. Quindi S=Ge^{-G}.
ALOHA ha il massimo con G=1, di cui la capacità di trasporto S è pari a $\frac{1}{e}$ (circa 36%).
La probabilità di una collisione sarà 1-e^{-G}.
La probabilità che una trasmissione richieda esattamente k tentativi (quindi k-1

collisioni) sarà:

$$P[k] = e^{-G}(1 - e^{-G})^{k-1} \tag{12}$$

Il numero atteso di trasmissioni E sarà pari a:

$$E = \sum_{k=1}^{\infty} kP_k = e^{G} \tag{13}$$

Piccole variazioni del carico del canale possono ridurre le sue prestazioni.

4.2.2 Protocolli ad accesso multiplo con rilevamento della portante

Abbiamo detto che con ALOHA slotted il massimo utilizzo del canale è di 1/e. Per fare meglio possiamo usare protocolli con rilevamento della portante (trasmissione), che permettono di controllare il canale per vedere se è occupato.

CSMA persistente e non persistente

1. CSMA 1-persistente: quando una stazione deve trasmettere, ascolta il canale. Se il canale è libero trasmette, se è occupato aspetta finchè non si libera. Problema quando ci sono 2 stazioni che attendono, oppure se inviano simultaneamente. Si chiama 1 perchè la stazione trasmette con probabilità 1 quando il canale è libero.
   Il ritardo di propagazione incide sulle collisioni.
   Questo protocollo ha prestazioni migliori di ALOHA puro.

2. CSMA non persistente: stazione attende un intervallo di tempo casuale prima di trasmettere se il canale non è libero. Se è libero invece trasmette. (allunga i ritardi).

3. CSMA p-persistente: si applica ai canali divisi ad intervalli. Ogni stazione controlla il canale. Se è libero, trasmette subito con probabilità p, e rimanda la trasmissione all'intervallo successivo con probabilità q = 1-p. Se anche il prossimo intervallo è libero, si itera il procedimento. Se lo slot non è libero, la stazione attende un tempo casuale.

CSMA con rilevamento delle collisioni Un miglioramente consiste nel rilevare le collisioni, e interrompere la trasmissione anzichè portarla a termine. Si risparmia tempo e banda.
CSMA/CS (CSMA with Collision Detection). L'HW della stazione ascolta il canale durante la trasmissione. Se il segnale letto è diverso da quello inviato, si è verificata una collisione.Implica che il segnale non debba essere molto piccolo rispetto a quello inviato, e deve essere scelta una corretta modulazione.
Il tempo minimo per rilevare una collisione è pari al tempo impiegato dal segnale per propagarsi da una stazione all'altra.

4.2.3 Protocolli senza collisione

Con CSMA/CD non ci sono collisioni se una stazione ha acquisito il canale. Possono però verificarsi in fase di contesa del canale. Le collisioni riducono l'ampiezza di banda, e rendono il tempo di trasmissione di un frame variabile.
Supponiamo che ci siano N stazioni, ognuna associata ad un indirizzo (da 0 a N-1).

Protocollo a mappa di bit Ogni periodo di contesa è composta da N slot. Se la stazione N deve inviare un frame, trasmette un bit 1 durante l'intervallo N-1. Ogni slot è associato ad una stazione.
Una volta trascorsi tutti gli N slot del periodo di contesa, ogni stazione sa chi deve trasmettere e si procede in ordine.
Protocolli di questo tipo si chiamano protocolli a prenotazione.
La media di attesa di accesso agli slot è N. A basso carico, l'efficenza è pari a d/(d+N), dove d è la quantità di dati per frame, e N è il numero di bit per il controllo (N per frame).
Con un carico elevato, d/(d+1).
Il ritardo medio per un frame è pari a (N-1)d+N + tempo di accomodamento dentro la stazione.

Protocolli token passing Viene passato un breve messaggio chiamato token (gettone) da una stazione alla successiva in un ordine predefinito. Il token rappresenta il permesso per inviare dati: chi ha il frame può comunicare.
Per stabilire l'ordine delle stazioni è usata la topologia della rete: le stazioni sono collegate a formare un anello, che può essere anche virtuale.

Protocolli binary countdown Per i protocolli precedenti, è necessario 1 bit di controllo per stazione. Sono poco adatti con reti grandi.
Il protocollo binary countdown cerca di risolvere questo problema: vengono usati indirizzi binari per ogni stazione, e un canale combina le trasmissioni. Una stazione che vuole usare il canale, comunica in broadcast il proprio indirizzo bit per bit partendo da quello più significativo. I bit che occupano la stessa posizione negli indirizzi di stazioni diverse vengono spediti contemporaneamente. Si applica quindi una regola di arbitraffio: la stazione rinuncia non appena si accorge che una posizione di bit di ordine elevato che nel proprio indirizzo è uguale a 0 è stata cambiata in 1.
Le stazioni con un indirizzo più alto hanno più priorità.
L'efficenza del canale è pari a d/(d+$log_2 N$).

4.2.4 Protocolli a contesa limitata

Con carico leggere la contesa è preferibile. Con ampio carico, invece, è preferibile usare metodi senza collisioni.
I protocolli a contesa sono simmetrici, ossia ogni stazione tenta di acquisire il canale con una probabilitè p uguale per tutte. Se assegnamo ad ogni stazione

una differente probabilità, le prestazioni potrebbero aumentare.
Con un protocollo simmetrico, se ci sono k stazioni, la probabilità che una stazione durante uno slot è la probabilità che una stazione trasmetta con probabilità p e che tutte le k-1 stazioni non lo faccino. Il valore ottimo di p è 1/K. Quindi: (pr[successo con p ottimo]):

$$Pr = ((\frac{k-1}{k})^{k-1} \tag{14}$$

Se il numero di stazioni è basso, le possibilità di successo sono buone, ma più stazioni ci sono, più si tende a 1/e.

Protocollo adaptive tree walk Immaginiamo le stazioni come le foglie di una struttura ad albero. Nel primo slot che segue una trasmissione senza collisioni (slot 0), tutte le stazioni possono comunicare. Se una ci riesce ok. Se avvengono collisioni, durante il prossimo intervallo possono comunicare solo le stazioni sotto il nodo 2. Se ci riescono, allora il prossimo intervallo sarà riservato alle stazioni sotto il nodo 3. E così via.

4.2.5 Protocolli per LAN wireless

Le reti wireless non sono in grado di inviduare una collisione mentre sta avvenendo. Una volta accaduti, si rilelvano con ACK. Per progettare protocolli per LAN wireless, bisogna tenere conto del problema del terminale nascosto (una stazione non è in grado di rilevare i concorrenti per il mezzo di trasmissione a causa della distanza), e del terminale esposto.
Per le LAN wireless si utilizza il protocollo MACA (multiple access collision detection).
L'idea base è: trasmettitore chiede al ricevente di trasmettere un piccolo frame (A invia a B un RTS (request to send), B invia CTS (clear to send), A ricevuto CTS inizia la trasmissione). Le stazioni che si trovano nelle vicinanze che rilevano questa trasmissione evitano di trasmettere dati.
Le stazioni che rilevano RTS sono vicine ad A, e stanno zitte.
Se due stazoni invece decidono di inviare un pacchetto RTS contemporaneamente, si verificherà un errore, e i pacchetti andranno persi. Se le 2 stazioni non ricevono il CTS entro un certo periodo di tempo, allora aspetteranno un tempo casuale prima di ritrasmettere il pacchetto RTS.

4.3 Ethernet

Esistono 2 tipi di Ethernet:

1. Ethernet classica: risolve il problema dell'accesso multiplo usando le tecniche studiate qui di seguito (tassi di trasmissione tra i 3 e 10 Mbps)

2. Ethernet commutata: dispositivi (commutatori) utilizzati per connettere diversi computer (100, 1000 e 10.000 Mbps).

4.3.1 Livello fisico di Ethernet classica

Uno standard di Ethernet a 10 Mbps venne proposto nel 1978 (Standard DIX). Nel 1983 divenne IEEE 802.3. La prima archiettura era la Thick Ethernet: un unico cavo permetteva di collegare dei computer tra loro.
Successivamente, venne sviluppata Thin Ethernet, più flessibile ed utilizzava collettori BNC. Era più economica, ma limitata a 185 metri per segmento. Per collegare più segmenti, vengono utilizzati dei repeater, dispositivi di livello fisico che riceve, amplifica e ritrasmette il segnale in entrambe le direzioni.
Le informazioni sono spedite con codifica Manchester. Un Ethernet può contenere divevrsi segmenti di cavi e diversi repeater, ma non ci possono essere due transceiver a più di 2,5 Km, per poter permettere al protocollo MAC di lavorare in modo corretto.

4.3.2 Protocollo sottolivello MAC di Ethernet classica

Il formato dei frame è il seguente:

1. Preambolo (8 byte), composto da 7 byte pari a 0101010, e l'ultimo uguale a 0101011 (gli ultimi 2 bit sono chiamati delimitatore di inizio frame). Manchester con questa codifica genera un'onda quadra in grado di permettere al clock del ricevente di sincronizzarsi con quello del trasmittente.

2. Indirizzo destinazione (6 byte), se il primo bit è un 1 identifica un gruppo. Se l'indirizzo è composto da tutti 1 allora è un indirizzo di broadcast.

3. Indirizzo d'origine (6 byte),

4. Type (Lenght se IEEE 802.3) (2 byte), Ethernet utilizza Type per comunicare che cosa fare con il frame (specifica . 802.3 utilizza questo campo per indicare la lunghezza del frame.

5. Dati (0...1500 byte), limitato perchè un transceiver aveva bisogno di salvare il frame in RAM.

6. Pad (0...46 byte)

7. Checksum (4 byte), CRC a 32 bit.

Ethernet chiede che i frame siano lunghi almeno 64 byte. Se i dati sono minori di 46 byte, viene usato il campo Pad per compensare.

CSMA/CD con backoff esponenziale binario Ethernet classica usa CSMA/CD 1-persistente.
Per determinare l'intervallo di tempo casuale di attesa prima della ritrasmissione dopo una collisione, il tempo viene diviso in intervalli discreti la cui lunghezza è uguale al tempo di propagazione di andata e di ritorno sul mezzo di trasmissione nel caso peggiore.

Dopo una collisione la stazione attende casualmente 1 o 0 slot prima di ritrasmettere. Se due stazioni scelgono lo stesso numero avverrà una nuova collisione e si sceglierà tra 0, 1, 2 o 3 slot. Se avviene una terza collisione il numero prossimo di intervalli è compreso tra 0 e $2^3 - 1$. Dopo 16 collisioni di seguito viene dato un errore.
Questo algoritmo è chiamato backoff esponenziale binario, e permette di adattarsi dinamicamente al numero di stazioni che tentano di trasmettere. Se non ci sono collisioni si suppone che la comunicazione sia andata a buon fine (non viene fornita una conferma di ricezione).
Usata per mezzi a basso tasso d'errore (cavi di rame o fibra ottica). Per mezzi wireless viene usato un ACK.

4.3.3 Prestazioni di Ethernet

Supponiamo una probabilità costante di ritrasmissione ad ogni slot. Se ogni stazione trasmette in un intervallo con contesa con probabilità p, allora la probabilità A che qualche stazione acquisista il controllo del canale in quell'intervallo è:

$$A = kp(1-p)^{k-1} \tag{15}$$

Il numero medio di slot per contesa è:

$$A = \sum_{i=0}^{\infty} jA(1-A)^{j-1} = \frac{1}{A} \tag{16}$$

Se il frame medio impiega P secondi per essere trasmesso, quando molte stazioni hanno frame da inviare si ha:

$$Efficenza = \frac{P}{P + 2\pi/A} \tag{17}$$

Più il cavo è lungo, più tempo si ha di contesa. L'efficenza può essere vista anche con un'altra formula: F = lunghezza di frame, B = banda di rete, L = lunghezza del cavo, c = velocità di propagazione del segnale in codizioni ottime di e slot di contesa per frame.

$$Efficenza = \frac{1}{1 + 2BLe/cF} \tag{18}$$

Quindi aumentando la banda della rete o la distanza, l'efficenza diminuisce.

4.3.4 Ethernet commutata

Per gestire il carico crescente, viene usato uno switch (commutatore) che contiene una scheda HW di collegamento tra le intefacce di rete o backpane che connette tutte le porte. Lo switch è in grado di capire a che porta inoltrare un frame. In uno switch inoltre ogni porta ha un proprio dominio di collisione separato.

Lo switch deve avere un buffer, in cui possa accodare un frame in ingresso se c'è giù un frame in uscita nella porta scelta.
La maggior parte delle interfacce di rete supporta la modalità promisqua, in cui un computer raccoglie tutti i frame, non solo quelli interessati. Uno switch evita questo inconveniente e migliora la sicurezza.
Alcune porte nello switch vengono usate come concentratori, in cui è possibile collegare degli hub.

4.3.5 Fast Ethernet

Fast Ethernet (802.3u) fu approvato dall'IEEE nel 1995. Vengono mantenuti tutti i vecchi formati di frame per calcoli, interfacce e regole procedurali. Ci sono diverse cablature di fast Ethernet:

1. 100Base-T4, doppino, lunghezza max segmento: 100m, UTP di cat. 3
2. 100Base-TX, doppino, lunghezza max segmento: 100m, Full Duplex a 100 Mbps (UTP cat. 5)
3. 100Base-FX, fibra ottica, lunghezza max segmento: 2000m, Full Duplex a 100 Mbps (distanze elevate).

4.3.6 Gigabit Ethernet

802.3ab. Come fast Ethernet, le comunicazioni sono punto a punto. Gigabit Ethernet supporta due modalità operative: full duplex e half duplex. Si ha full duplex quando c'è uno switch centrale collegato ai computer. Non si verifica contesa, e non si usa CSMA/CD. La modalità half duplex si usa quando i computer sono collegati ad un hub e non a uno switch. Sono possibili collisioni, quindi è richiesto il protocollo CSMA/CD.
Per migliorare questo standard, sono state aggiunte due funzionalità che consentono di avere una lunghezza massima del cavo fino a 200 metri:

1. carrier extension, per aggiungere dati di riempimento dopo il frame normale.
2. frame bursting, permette a un trasmittente di inviare una sequenza concatenata di più frame in una singola trasmissione

1. 1000Base-SX, fibra ottica, lunghezza max segmento: 550m, fibra multimodale
2. 1000Base-LX, fibra ottica, lunghezza max segmento: 5000m, fibra mono o multimediale
3. 1000Base-CX, 2 coppie STP, lunghezza max segmento: 25m, doppino schermato
4. 1000Base-T, 4 coppie UTP, lunghezza max segmento: 100m, UTP standard cat. 5

Gigabit Ethernet implementa il controllo del flusso, per evitare l'esaurimento del buffer. Il controllo di flusso è implementato spedendo dei frame speciali di pausa.

4.3.7 10-gigabit Ethernet

Viene usata all'interno dei datacenter e nelle centrali di commutazione, per collegare router di fascia alta, switch e server. I collegamenti a lunga distanza (che collegano centrali che gestiscono intere MAN) usano fibra ottica, quelli a breve cavi di rame o fibra. 10-gigabit Ethernet supporta solo full-duplex.
Le versioni di 10-gigabit Ethernet inviano un flusso sequenziale di dati prodotto mischiando i bit e poi applicando una codifica 64B/66B.

1. 10GBase-SR: fibra ottica, lunghezza max segmento: 300m, fibra multimodale.
2. 10GBase-LR: fibra ottica, lunghezza max segmento: 10km, fibra monomodale.
3. 10GBase-ER: fibra ottica, lunghezza max segmento: 40km, fibra monomodale.
4. 10GBase-CX4: 4 coppie di biassiali, lunghezza max segmento: 15m, rame biassale.
5. 10GBase-T: 4 coppie di UTP, 100m, UTP di Cat. 6a.

4.4 Commutazione a livello data link

è possibile unire le LAN per crearne una più grande usando dei bridge (o switch).

4.4.1 Vari utilizzi dei bridge

Perchè usare i bridge?
Per dividere una LAN logica in più LAN fisiche,vper poter avere reti più grandi, per poter unire i computer di un ufficio. I bridge ideali dovrebbero essere trasparenti.

4.4.2 Bridge con apprendimento

Ogni bridge opera in modalità promiscua (accetta ogni frame trasmesso dalle stazioni collegate ad ognuna delle sue porte). Il bridge ha il compito di decidere se inoltrare o scartare ogni frame, e su che porta farlo uscire.
Un modo per fare questo, è tenere su una tabella hash dentro il bridge tutte le possibili destinazioni e le porte ad esse associate.
Al primo collegamento del bridge, tutte le porte sono vuote. I bridge devono usare un algoritmo di flooding per trovare le varie destinazioni: ogni frame in entrata per una destinazione sconosciuta viene fatto passare su tutte le porte su cui il bridge è connesso (ad eccezione della porta entrante). Se una destinazione

è nota, il frame viene indirizzato subito, e non inoltrato a tutte le porte.
I bridge usano l'algoritmo di backward learning.
Per gestire topologie dinamiche, ogni volta che un elemento viene aggiunto alla tabella viene anche calcolato il tempo di arrivo del frame, che viene aggiornato ogni volta che arriva un frame la cui sorgente è già in tabella.
Un processo interno al bridge inoltre scandisce la tabella di hash ed elimina tutti gli elementi più vecchi di qualche minuto.
L'algoritmo di routing utilizzato è il seguente:

1. scarta il frame se la porta per raggiungere la destinazione è la stessa della porta sorgente.

2. inoltra il frame sulla porta di destinazione se la porta per raggiungere il frame non è la stessa della porta di destinazione.

3. utilizza il flooding ed inoltra il frame a tutte le porte tranne la porta sorgente se la porta di destinazione è sconosciuta.

Questo algoritmo è implementato con chip VLSI, che gestiscono la tabella in pochi millisecondi.
Inoltre è possibile iniziare la decisione di inoltro del frame appena arriva l'indirizzo MAC: questo riduce la latenza (cut-through switching).

4.4.3 Bridge con spanning tree

Possono esserci collegamenti ridondanti tra i bridge, che creano cicli. Questo per assicurarsi che se un collegamento va giù, la rete non verrebbe divisa in 2.
Il problema però sono i cicli, viene quindi usato un algoritmo per ricavare un albero di copertura minima in grado di raggiungere ogni bridge.
Alcuni collegamenti quindi possono venire ignorati per poter permettere di costruire una topologia virtuale esente da cicli.
è possibile vedere la topologia di questo tipo di rete come un grafo. Questo grafo può essere ridotto ad uno spanning tree. Usando uno spanning tree c'è sempre un collegamento tra ogni coppia di stazioni.
Per generare lo spanning tree viene usato un algoritmo distribuito: ogni bridge trasmette un messaggio di configurazione da tutte le sue porte ai suoi vicini, ed elabora i messaggi che riceve dai suoi vicini. Per scegliere il bridge radice, viene sceto quello con l'identificatore MAC più basso. Gli indirizzi MAC vengono spediti nel messaggio di configurazione. Per trovare i percorsi minimi, i bridge includono la loro distanza dalla radice nei messaggi di configurazione. Ogni bridge ricorda il percorso più breve individuato verso la radice e spegnendo le porte che non fanno parte del tragitto più breve. L'algoritmo dello Spanning Tree è stato standardizzato come IEEE 802.1D.

4.4.4 Repeater, hub, switch, router e gateway

1. Repeater: si trovano nel livello fisico, sono dispositivi analogici che gestiscono i segnali sui cavi a cui sono collegati. Un segnale che appare sul

cavo è ripulito dal rumore, amplificato ed inoltrato sull'altro cavo.
Comprendono solo i simboli che codificano i bit in volt.

2. Hub: un hub ha diverse linee di input collegate elettronicamente. I frame che arrivano su una di queste linee vengono spediti attraverso tutte le altre. Due frame che arrivano contemporanemente collidono. Tutte le linee operano alla stessa velocità.
   Gli hub non amplificano il segnale in ingresso.

3. Bridge: i Bridge operano a livello data link, collega 2 o più LAN e ogni porta ha un proprio dominio di collisione. Il bridge può spedire più frame contemporaneamente. è necessario un buffer all'interno del bridge.

4. Switch: gli Switch sono bridge moderni,

5. Router: un Router opera ad un livello più alto. Quando un pacchetto raggiunge un router, vengono rimosse la sua intestazione e la sua coda, e il pacchetto contenuto nel payload viene passato al software di instradamento.

6. Gateway: un Gateway connette due computer che usano protocolli di trasporto orientati alle connessioni differenti. Un gateway a livello applicazione comprende il formato e il contenuto dei dati e possono tradurre i messaggi da un formato ad un altro.

4.4.5 Virtual LAN

5 Il livello di rete

Questo livello si occupa del trasporto dei pacchetti lungo tutto il percorso della rete. È il livello più basso che si occupa della trasmissione punto a punto.
Il livello di rete deve conoscere la topologia della rete di comunicazione, e scegliere i percorsi appropriati.

5.1 Problematiche nella progettazione del livello di rete

5.1.1 Commutazione di pacchetto store-and-forward

In questo livello i componenti principale sono le apparecchiature ISP e i dispositivi degli utenti. Un host che vuole trasmettere invia un pacchetto nel router più vicino, oppure mediante un collegamento punto a punto con l'operatore di telecomunicazionei. Il pacchetto viene memorizzato finchè non è completamente arrivato. A questo punto, dopo aver verificato il checksum, viene inviato al router successivo della rete e così via fino a destinazione (meccanismo store-and-forward).

5.1.2 Servizi forniti al livello di trasporto

I servizi del livello rete vengono progettati tenendo conto:

1. che non devono essere legati alla tecnologia dei router
2. che il livello di trasporto non deve conoscere dettagli tipo numero, tipo, topologia dei router
3. che gli indirizzi di rete dovrebbero utilizzare uno schema di numerazione uniforme.

Il livello di trasporto offre servizi orientati alla connessione e servizi connectionless.

5.1.3 Implementazione del servizio non orientato alla connessione

In questo contesto i pacchetti sono chiamati datagram e la rete rete datagram.
Il livello di rete si occupa di suddividere il pacchetto ricevuto dal livello di trasporto in n parti, e inviare un pacchetto dopo l'altro ad un router usando un protocollo punto-a-punto (PPP).
Ogni router possiede una tabella interna, che indica dove devono essere inviati i pacchetti diretti a ogni possibile destinazione. Ogni voce è composta da una coppia di valori (destinazione, linea da usare).
Vengono usate solo linee dirette.
I router controllano questa tabella per decidere dove inviare il messaggio.
I router implementano algoritmi di routing, che gestiscono le tabelle e prendono decisioni di instradamento.
Un esempio di protocollo connectionless più diffuso è il protocollo IP.

5.1.4 Implementazione del servizio orientato alla connessione

In questo caso una rete è a circuito virtuale. Si stabilisce un percorso all'inizio della connessione, e quel percorso viene usato per tutti i pacchetti di quella connessione. Il circuito virtuale viene rilasciato al momento del rilascio della connessione.
Ogni pacchetto contiene un identificatore che permette di indicare il circuito virtuale di appartenenza.
Un esempio è MPLS, trasparente agli utenti ma utilizzato dagli ISP per garantire la QOS.

5.1.5 Confronto tra reti a circuito virtuale e reti datagram

I circuiti virtuali rihiedono un tempo e risorse per la fase di configurazione, ma poi risulta facile capire dove instradare i pacchetti (basta leggere l'identificatore di circuito per trovare la prossima destinazione). In una rete datagram non viene richiesta una configurazione (meno tempo e meno risorse sprecate), ma è più difficile trovare la destinazione.
Inoltre gli indirizzi di reti datagram sono più lunghi quindi per piccoli pacchetti datagram c'è molto overhead.
Reti a circuito virtuale utilizzano meno memoria dei router, in quanto nelle tabelle basta memorizzare una sola voce per circuito virtuale, mentre per le reti datagram viene memorizzata una voce per ogni destinazione.
I circuiti virtuali garantiscono QOS e permettono di evitare congestioni all'interno della rete (le risorse possono essere rilasciate in anticipo e sono sempre disponibili se si è stabilita una connessione). Con le reti datagram tutto questo risulta difficile.
I circuiti virtuali però hanno un problema di vulnerabilità. Se un router ha un problema HW o SW tutti i circuiti virtuali che passano da lui devono essere terminati.
Le reti datagram permettono di bilanciare il carico e il traffico della rete.

5.2 Algoritmi di routing

Un algoritmo di routing è implementato in un processo di livello di rete e permettono di scegliere lungo quale linea in uscita vanno inoltrati i pacchetti in arrivo.
È bene distinguere tra

1. forwarding: processo che gestisce un pacchetto in arrivo, cercando in una tabella la linea di trasmissione più adatta.

2. routing: processo che riempie e aggiorna le tabelle di routing.

Se la rete è datagram, allora la scelta della linea viene eseguita per ogni pacchetto in arrivo. Se è un circuito virtuale, le decisioni vengono prese allo stabilirsi della

connessione.
Gli algoritmi di routing si dividono in:

1. Algoritmi non adattivi: non basano le proprie decisioni su misure o stime del traffico e della topologia corrente. Il percorso tra I e J, generici router, viene calcolato in anticipo (routing statico).

2. Algoritmi adattivi: modificano le decisioni in base a diversi fattori (topologia, traffico) e si adattano alla rete con il tempo(routing dinamico)

5.2.1 Principio di ottimalità

Il principio di ottimalità afferma che se il router J si trova sul percorso ottimale tra I e K, allora il percorso ottimale tra J e K segue la stessa sequenza di router.
La serie di percorsi ottimali che collegano tutte le sorgenti ad una data destinazione forma una struttura ad albero, dove il nodo principale è la destinazione (sink tree), dove la distanza è calcolata in base al numero di salti.
UN DAG è un grafo diretto aciclico, che contiene tutti i percorsi minimi (è una unione di tutti i possibili sink tree di un nodo.

5.2.2 Algoritmo di cammino minimo

Per scegliere un percorso tra una coppia di router, l'algoritmo deve trovare il cammino minimo che collega i due nodi del grafo.
L'algoritmo di Dijkstra trova un percorso minimo tra una sorgente e tutte le destinazioni della rete.

5.2.3 Flooding

Flooding (inondazione) è una tecnica che consiste di inviare un pacchetto a tutte le linee in uscita, tranne a quella da cui proviene.
Ovviamente questa tecnica genera un numero grandissimo di pacchetti, quindi è necessario usare tecniche avanzate per migliorarla.
È possibile utilizzare un contatore di salti, in modo tale che quando questo contatore raggiunge lo zero il pacchetto viene scartato. Il valore del contatore viene settato alla lunghezza del percorso tra sorgente e destinazione (oppure al diametro della rete) e viene decrementato ad ogni hop.
I router potrebbero ricevere pacchetti duplicati, quindi viene inserito un contatore di sequenza all'interno di ogni pacchetto. I router accettano solo pacchetti con una sequenza più alta da quella destinazione.
Il flooding garantisce che effettivamente un pacchetto venga inviato e ricevuto, in quanto trova sempre una strada. È usato per connessioni broadcast, in quanto un pacchetto viene consegnato a tutti i nodi della rete.
È un aloritmo robusto, e sceglie sempre il percorso migliore.

5.2.4 Routing basato su vettore delle distanze

Ogni router conserva una tabella, che definisce la distanza minima conosciuta per ogni destinazione e il collegamento che conduce a quella destinazione.
Le tabelle vengono aggiornate scambiando informazioni con i router vicini. È l'algoritmo di Bellman-Ford.
Una voce della tabella identifica un router all'interno della rete ed è composta da 2 parti: linea di trasmissione da usare, stima del tempo o della distanza associata a quella destinazione.
Per trovare il ritardo di propagazione tra 2 router vengono usati particolari pacchetti chiamati ECHO, contenenti data e ora di trasmissione.

Il problema del conteggio all'infinito L'assestamento dei percorsi verso la configurazione dei cammini ottimi è chiamato convergenza.
Il routing basato su vettori delle distanze converge molto lentamente, ed è possibili avere ritardi infiniti.
Il funzionamento di questo algoritmo di routing si basa sullo scambio dei vettori con i router vicini.
È meglio rappresentare l'infinito come valore corrispondente al percorso più lungo all'interno della rete.
Quando X dice a Y che ha un percorso che punta da qualche parte, Y non può sapere se fa parte di quel percorso.
Può avvenire un count to infinity quando viene cambiata la topologia della rete.

5.2.5 Routing basato sullo stato dei collegamenti

L'idea base di questo tipo di routing è la seguente:

1. scoprire i propri vicini e i relativi indirizzi di rete
2. misurare la distanza o la metrica di costo di ogni vicino
3. costruire un pacchetto contenente tutte le informazioni raccolte
4. inviare tale pacchetto a tutti gli altri router e ricevere i loro pacchetti
5. elaborare il percorso più breve verso tutti gli altri router

Scoperta dei vicini Il router cerca i vicini inviando un pacchetto HELLO su ogni linea punto a punto.
Un router riponde al pacchetto HELLO con il proprio nome (globalmente unico).
Una LAN broadcast in questo caso viene modellata inserendo un designated router che permette di collegare sottoreti della LAN tra loro.

Misurazione del costo dei collegamenti Per calcolare i cammini minimi su usa l'algoritmo link-state-routing. Ogni collegamento deve avere un costo. Per favorire i cammini con collegamenti corti, nel costo viene inserito anche il ritardo, calcolato inviando speciali pacchetti chiamati ECHO (misurando (tempo andata + tempo ritorno) / 2).

Costruzione dei pacchetti che contengono lo stato dei collegamenti Nel pacchetto viene salvato (in ordine): identità del trasmettitore, numero del pacchetto, Age del pacchetto, lista dei vicini.
I pacchetti che contengono le informazioni sullo stato dei colelgamenti vengono costruti periodicamente oppure all'avvenire di un evento significativo (ad esempio si interrompe una linea o un vicino si spegne)

Distribuzione dei pacchetti che contengono lo stato dei collegamenti Per distribuire questi pacchetti viene usato il flooding. Ogni pacchetto ha un numero di sequenza, incrementato per ogni nuovo pacchetto inviato.
I router tengono traccia delle coppie (router, numero sequenza) e confronta questi dati con quelli arrivati da un pacchetto: se il numero di sequenza è maggiore, allora il pacchetto viene floodato. Se è minore o uguale, viene scartato.
Alcuni difetti: i numeri di sequenza ripetitivi possono generare confusione (infatti vengono usati numeri di 32 bit),quando un router si blocca perde traccia dei suoi numeri di sequenza, possono verificarsi errori di trasmissione sul numero di sequenza.
L'età di un pacchetto viene decrementata di 1 ogni secondo. Quando raggiunge lo 0, le informazioni di quel router vengono scartate, il campo Age viene anche decrementato durante il flooding per evitare inondazioni di pacchetti.
Tutti i pacchetti che contengono informazioni sullo stato non vengono subito accodati per la trasmissione, ma parcheggiati in una zona d'attesa per un breve periodo. Se durante questo periodo arrivano altri pacchetti il router confronta i numeri di sequenza e tiene solo il pacchetto con il numero più alto. Tutti i pacchetti contenente informazioni sullo stato ricevono un ACK.

Calcolo dei nuovi percorsi Dopo aver ricevuto tutti i pacchetti di stato, i router creano il proprio grafo della rete. Ogni router esegue Dijsktra sul suo grafo per trovare i cammini minimi per raggiungere ogni router.
I risultati vengono salvati sulle tabelle di routing.
Il link state routing richiede più memoria e tempo di calcolo rispetto al distance vector routing. Con n router ognuno con k vicini, per memorizzare k dati in input serve una memoria di n*k.
Non presenta convergenza lenta. Utilizzato dalle reti reali.
Due esempi di protocolli link state sono IS-ISS e OSPF, il quale quest'ultimo fornisce un metodo di flooding per gli aggiornamenti sullo stato dei collegamenti, in modo da raggiungere uno stato stabile. Il problema di questi tipi di algoritmi è che sono influenzabili da problemi hardware e guasti dei router.

5.2.6 Routing gerarchico

La dimensione delle tabelle cresce proporzionalmente con la dimensione della rete, e consuma CPU e risorse. Se in memoria non ci stanno più entry. il routing avviene gerarchicamente.

I router sono divisi in regioni: ogni router conosce i router della sua regione e per comunicare con router al di fuori di questa comunica con un router "capo" della regione.
Il numero ottimale di livelli per una rete di N router è uguale a ln(N), per un totale di e*ln(N) voci per router.

5.2.7 Routing broadcast

La trasmissione contemporanea di un pacchetto a tutte le destinazioni è chiamata broadcasting.
Esistono diverse implementazioni:

1. invio tramite flooding: spreco di banda inutile, ogni sorgente deve conoscere tutte le destinazioni.

2. multidestination routing: ogni pacchetto contiene una lista delle destinazioni o una mappa di bit che indica le destinazioni desiderate.

Tratteremo del multidestination routing. Un router quando riceve un pacchetto controlla le destinazioni per trovare l'insieme delle linee di trasmissione richieste. Genera una nuova copia del pacchetto per ogni linea di output e include in ogni pacchetto solo quelle destinazioni che si trovano su quella linea (l'insieme delle destinazioni viene diviso tra le linee di trasmissione). Il flooding non si adatta bene alle linee punto a punto, ma potrebbe essere preso in considerazione nel caso della comunicazione broadcast.
Un altro esempio è il reverse path forwarding: quando il router riceve un pacchetto broadcast, verifica se è giunto attraverso la linea che normalmente è utilizzata per inviare pacchetti alla sorgente della trasmissione broadcast.
Se si, allora forse è la prima volta che quel pacchetto arriva in quanto ha scelto la strada migliore, e quindi vengono inoltrate le copie attraverso tutte le linee esclusa quella di input.
Se no, il pacchetto viene scartato, perchè può essere un duplicato.
Il vantaggio del reverse path forwarding è che è semplice da implementare ed efficente. È simile al flooding (trasmette in una direzione solo una volta), e richiede che i router sappiano solo come raggiungere tutte le destinazione e non è necessario memorizzare i numeri di sequenza o la lista di tutte le destinazioni del pacchetto.
Un altro algoritmo fa uso del sink tree del router che ha iniziato la trasmissione. Uno spanning tree è un sottoinsieme di tutti i router ma non contiene cicli. Se ogni router sa quali sue linee appartengono allo spanning tree, allora può copiare un pacchetto broadcast in arrivo su tutte le linee dello spanning tree, esclusa quella in ingresso.
Utilizza eccellentemente la banda, e genera il minor numero di pacchetti possibile.
Il problema è che ogni router deve conoscere uno spanning tree, e non sempre questa informazione è disponibile.

5.2.8 Routing multicast

Questo tipo di routing permette l'invio di un messaggio ad un gruppo di router. Richiede un metodo per creare e distruggere i gruppi, e identificare i router appartenenti ai gruppi.
Gli schemi multicast sono costruiti sulla base di quelli broadcast, e se il gruppo è denso basta tagliare le connessioni con i router che non fanno parte del gruppo. Per ridurre lo spanning tree si può operare in 3 modi:

1. ogni router costruisce il sink tree completo e rimuove i collegamenti verso router non facenti parte del gruppo (usato se i router conosco la topologia completa e se si adotta il link state routing).Viene usato il protocollo MOSPF (Multicast OSPF)

2. se si usa il routing con il vettore delle distanze, allora si usa il reverse path forwarding. Ogni volta che un router non facente parte del grupoo riceve un pacchetto multicast, risponde con un pacchetto PRUNE (che vuol dire "non inviarmi più messaggi!"). LO spanning tree viene ridotto in modo ricorsivo. Un protocollo è il DVMRP

3. core-based tree: viene scelta una radice per tutti i router, e costruiscono l'albero inviando pacchetti da ogni membro alla radice. Per inviare un pacchetto su un gruppo, un router invia un pacchetto al core (radice) che lo inoltra a tutto l'albero. Può essere inefficente, in base alla posizione del router sorgente nell'albero.
   Un vantaggio di usare un albero condiviso è il costo di memorizzazione, molto basso. È necessario possedere un solo albero per gruppo. I router non appartenenti al gruppo non devono svolgere nulla.
   Un protocollo è il protocollo PIM.

5.2.9 Routing anycast

Un pacchetto viene consegnato al membro più vicino del gruppo.
Sull'anycast ci interessa il messaggio e non il nodo sorgente, viene usato come parte del DNS.

5.2.10 Routing per host mobili

Gli host mobili hanno una home location fissa che non cambia (LAN di appartenenza), e possiedono un indirizzo utilizzabile per determinare la home location. Il routing per host mobili ha come obiettivo quello di inviare pacchetti ai host mobili utilizzando il loro home address ovunque si trovino.
È possibile usare un modello di adattamento che modifica i percorsi ogni volta che l'host mobile si sposta e di conseguenza la topologia cambia.
Oppure è possibile fornire mobilità sopra il livello rete (cambiando indirizzo di rete se gli host si muovono in una nuova postazione internet).
L'host mobile deve indicare a un host nella LAN di appartenenza dove si trova.

Questo host della LAN si chiama home agent, e agisce per nome dell'host mobile.
Quando l'host agent sa dove si trova l'host mobile, può inviare a lui i pacchetti.
Ovviamente quando un host mobile cambia rete, deve ottenere un nuovo indirizzo definito come un care of address. Questo permette all'host agent di risalire alla posizione. Viene effettuato un routing triangolare, eseguendo un meccanismo di tunnelling.
Alcuni schemi usano un agente esterno,remoto, ma non è necessario nei sistemi più recenti in quanto gli host mobili agiscono come propri agenti esterni. La locazione temporanea dell'host mobile è disponibile solo a pochi eletti (dispositivo mobile, home agent, mittenti) e in questo modo non bisogna ricalcolare i percorsi.

5.2.11 Routing nelle reti ad hoc

E se i router sono mobili?
Ogni nodo comunica in modo wireless ed agisce sia da host che da router.
La topologia può cambiare in qualsiasi momento, e i percorsi possono cambiare senza preavviso.
Viene utilizzato l'algoritmo AODV, che tiene conto della banda limitata e della scarsa durata delle batterie dei dispositivi che operano all'interno di questo ambiente.

Identificazione dei percorsi AODV è un algoritmo a richiesta, ossia determina il percorso migliore ogni volta quando c'è effettivamente bisogno di inviare pacchetti al destinatario.
Due nodi della rete sono collegati se possono comunicare direttamente usando la loro radio.
Ogni nodo può comunicare con tutti quelli dentro la sua copertura.
Per individuare un nodo I, viene inviato un pacchetto ROUTE REQUEST usando il flooding. Quando il nodo I riceve il pacchetto, invia un ROUTE REPLY seguendo il percorso inverso. Ogni nodo intermedio deve memorizzare il suo predecessore, e un contatore dei salti, incrementato ogni volta che riceve una risposta (questo per capire quanto i nodi siano distanti dalla destinazione). Viene usato il campo time to live, decrementato ad ogni salto. Se raggiunge lo 0, il pacchetto viene scartato. Si inizia partendo con time to live pari a 1, e se non si ha risposta il valore viene incrementato e si riprova.

Aggiornamento di un percorso La topologia può cambiare spontaneamente. Ongi nodo periodicamente trasmette in broadcast un pacchetto HELLO, ed ognuno dei suoi vicini deve rispondere. Se un vicino non risponde, vuol dire che si è spostato, e non può essere raggiunto. Questo metodo permette di eliminare i percorsi che non sono più validi. A questo punto possono usare il meccanismo di scoperta per scopire nuovi percorsi validi.
Per garantire una rapida convergenza, i percorsi includono un numero di sequenza controllato dalla destinazione. Questo numero funziona come un orolo-

gio logico, la destinazione lo incrementa ogni volta che invia un nuovo pacchetto ROUTE REPLY. La richiesta sarà trasmessa in broadcast fino a un percorso con un numero di sequenza più alto. I nodi intermedi memorizzano solo i percorsi che hanno un numero di sequenza più alto, o il minor numero di salti per il numero di sequenza corrente. Memorizzano solo i percorsi che sono in uso, e questo porta ad un miglioramento di banda e durata della batteria.
Scoperta e manutenzione dei percorsi vengono condivisi quando questi si sovrappongono per risparmiare risorse.
Se si implementa uno schema GPSR (greedy perimetral stateless routing), se tutti i nodi conoscono la loro posizione geografica l'inoltro ad una destinazione può procedere senza calcolo del percorso andando nella direzione giusta.

5.3 Algoritmi per il controllo della congestione

Una congestione è un evento non voluto che causa degrado delle prestazioni, perdita di pacchetti e ritardi. Questo può avvenire quando sono presenti troppi pacchetti all'interno della rete. Il livello rete ha il compito di risolvere queste congestioni.
Per ridurre i problemi di congestione è possibile agire sul carico, riducendo i pacchetti inviati dal livello trasporto.
Quando il numero di pacchetti inviati in rete dagli host è al di sotto della sua capacità di carico, il numero di pacchetti consegnati è proporzionale al numero di inviati. Quando il carico si avvicina alla capacità di carico, alcuni pacchetti vengono persi e si verifica un problema di traffico, e la rete si congestiona. I pacchetti persi consumano parte della capacità di rete.
È possibile che si verifichi un collasso da congestione, nel quale le prestazioni crollano vertiginosamente.
Se la memoria non è sufficente, alcuni pacchetti verranno persi.
Una tecnica per risolvere problemi di congestione consiste nel diminuire il carico o costruire una rete più veloce.
Il controllo della congestione riguarda tutti gli host e tutti i router, e significa garantire che la rete sia in grado di trasportare il traffico immesso.
Il controllo di flusso rigurda solo il traffico tra un singolo trasmittente e un dato ricevente, e cerca di evitare che una sorgente veloce trasmetta una quantità di dati maggiore di quella che il ricevente è in grado di assorbire.

5.3.1 Approcci al controllo della congestione

La presenza di una congestione indica che il carico è maggiore di quello che può essere gestito da una parte del sistema. Esistono due soluzioni: aumentare le risorse o diminuire il carico.
Un modo per evitare una congestione è quello di costruire una rete che si adatti al traffico sopportato. Se si verifica una congestione è possibile aggiungere dinamicamente le risorse (es. deviando il traffico su router di riserva o utilizzare linee dedicate) o acquistando più banda.

Questo metodo è chiamato provisioning.
I percorsi possono essere personalizzati in modo da tenere conto dei cambiamenti che avvengono durante la giornata, in base all'analisi del traffico, modificando i loro pesi in determinate situazioni.
Questo metodo è chiamato traffic-aware routing.
Il controllo di ammissione invece permette di diminuire il traffico in quelle situazioni in cui non è possibile aumentare la capacità della rete. In una rete a circuito virtuale si può rifiutare una connessione se la sua attivazione causa una congestione.
Quando è imminente la congestione la rete può fornire un feedback alle sorgenti causanti la congestione, richiedendo una pausa di trasmissione o il rallentamento.
Le difficoltà sono: identificare la nascita di una congestione, informare la sorgente di rallentare il traffico.
Per il primo problema i router possono monitorare il carico medio, il ritardo di accomodamento o la perdita di pacchetti. Se tali numeri crescono, sta avvenendo una congestione.
Per il secondo problema, è necessario inviare un feedback alle sorgenti. Fornire un feedback tempestivo non è un problema banale, e i router inviano più messaggi quando la rete è congestionata.
Il load shedding permette di eliminare il carico in eccesso, e una buona politica per scegliere quali pacchetti scartare può aiutare a prevenire il collasso.

5.3.2 Traffic-aware routing

5.3.3 Controllo di ammissione

5.3.4 Limitazione del traffico

5.3.5 Load shedding

5.4 Qualità del servizio

5.4.1 Requisiti delle applicazioni

5.4.2 Traffic shaping