Reti di Calcolatori

Matteo Mazzaretto

2024

Indice

1 Tipi di cavo (2014)

Ci sono diversi tipi di cavo, fra i più utilizzati si trovano:

1. Unshielded Twisted Pair (UTP): coppia di fili annodati tra loro con il twist che serve a limitare l'interferenza reciproca che altrimenti sarebbe troppo elevata
   La sua applicazione più comune è il sistema telefonico, possono estendersi per diversi chilometri ma per distanze più lunghe sono necessari dei ripetitori
   Hanno un basso costo e un discreto livello di prestazioni, attualmente sono largamente utilizzati

2. Cavo coassiale: hanno una schermatura migliore dei cavi UTP e per questo sono molto usati per TV via cavo e le MAN (metropolitan area network)
   La loro larghezza di banda è all'incirca 1GHz
   Può estendersi per distanze più lunghe e consente velocità più elevate
   Fornisce ampiezza di banda ed eccellente immunità al rumore

3. Fibra ottica: non si ha più elettricità ma si trasporta la luce, grazie a un pezzetto di vetro interno che non deve assolutamente rompersi, però non subisce interferenze elettriche
   La connessione tra fibre può avere: connettori che perdono 10-20% di luce, allineatori meccanici coi quali si perde il 10% di luce, oppure per fusione con la quale si perde il 2% di luce
   L'ampiezza di banda raggiungibile va sicuramente oltre i 50Tbps ma si è chiusi dal limite pratico di 10Gbps
   C'è anche un tipo di fibra detto monomodale in cui la luce si propaga solo in linea retta, è più costosa ed utilizzata sopratutto sulle lunghe distanze

2 Satelliti (2015, 16, 18, 19, 20 21, 23, 24)

Esistono tre tipologie principali di satelliti:
GEO (geostazionari >35km), MEO (compreso fra 5km e 15km), LEO(<5km)
Nelle parti non comprese ci sono le "fascie di Van Allen" le quali assorbono la luce del Sole e causano problemi alle telecomunicazioni
Esse devono essere evitate tramite dei "buchi" altrimenti i satelliti si scioglierebbero all'istante
Più basso è il satellite più ne servono perché coprono un'area bassa ma i tempi di comunicazione sono ridotti rispetto a un satellite elevato

2.1 Satelliti GEO

2.1.1 Descrizione

Sono i satelliti più in alto del nostro mondo, sopra i 35km
Essi devono superare le due fasce di Van Allen per restare stazionari nell'orbita circolare dell'Equatore
Garantisce una copertura continua di vaste aree terrestri e un posizionamento stabile

2.1.2 Ambiti d'uso

Sono utilizzati come satelliti spia, meteo, televisione e internet satellitari, osservazioni della Terra

2.1.3 Pregi

1. Posizionamento stabile e fisso
   Un satellite GEO rimane costantemente sopra lo stesso punto della Terra, facilitando comunicazioni e trasmissioni continue

2. Copertura geografica ampia
   Ogni satellite può coprire fino a un terzo della superficie terrestre
   Con tre satelliti GEO opportunamente posizionati, è possibile garantire una copertura globale

3. Ideale per comunicazioni e broadcasting
   L'orbita GEO è ideale per applicazioni come la televisione satellitare, le trasmissioni radio e le telecomunicazioni a lunga distanza, grazie alla copertura costante e affidabile

4. Minor necessità di reti satellitari
   A differenza delle costellazioni LEO o MEO, che richiedono molti satelliti per fornire copertura continua, pochi satelliti GEO possono coprire vaste aree, riducendo i costi di lancio e manutenzione

5. Riduzione delle complessità di tracciamento
   Poiché i satelliti GEO appaiono "fissi" nel cielo, non è necessario un sistema complesso per tracciare il loro movimento, semplificando il design delle stazioni a terra

2.1.4 Difetti

C'è un limite di 180 satelliti per evitare interferenze tra le frequenze radio e sovrapposizioni delle orbite, inoltre richiedono tantissima energia prodotta comunque dai pannelli solari
Inoltre, utilizzando la banda Ku si è molto limitati dalla pioggia
Sono satelliti fermi nella nostra testa che stanno nell'orbita circolare dell'equatore il che vuol dire che sono meno efficaci alle alte latitudini (vicino ai poli)
Infine sono un vero disastro per sicurezza e privacy perché tutto può essere ascoltato da tutti (salva la crittografia adottata)

2.2 Satelliti MEO

2.2.1 Descrizione

Sono satelliti che stanno nell'orbita media, ed è stato il primo tipo di satellite lanciato dall'uomo, per la precisione lo Sputnik
Essi sono satelliti situati fra le due fasce di Van Allen
Si spostano lentamente lungo la longitudine impiegando circa 6 ore per compiere un giro intorno al pianeta causando la necessità del loro rintracciamento

2.2.2 Ambiti d'uso

Qui si trovano i satelliti utili per la geolocalizzazione, il cui servizio è attualmente del Dipartimento della Difesa USA

2.2.3 Pregi

Attualmente con la tecnologia A-GPS si migliora il GPS e si segnala dove sono presenti i satelliti (tramite le compagnie di rete telefonica) sfruttando l'effetto Doppler
Infatti a quest'altitudine si trovano i 24 satelliti GPS necessari

2.2.4 Difetti

Il cosmo è pieno di satelliti di tipo MEO e questi sono nient'altro che rottami spaziali che inquinano il cosmo e rischiano continuamente di scontrarsi fra di loro creando sempre più microframmenti rischiando l'effetto domino

2.3 Satelliti LEO

2.3.1 Descrizione

Utilizzato per l'Internet satellitare e il telefono satellitare, ideato col progetto Iridium (sistema di 77 satelliti diventati 66) per coprire l'intera superficie terrestre
Ha la comodità di non dover superare alcuna fascia di Van Allen per essere lanciato nello spazio creando così meno difficoltà nella realizzazione e nella progettazione
Si ha un tempo di rivoluzione breve (dai 90 minuti alle 2 ore)

2.3.2 Ambiti d'uso

Attualmente fa parte dello Tsunami Warning System
Forniscono connessioni Internet a banda larga, permettono di osservare la Terra, sono utilizzati per scopi militari, di sicurezza e di ricerca scientifica (studi sull'atmosfera)

2.3.3 Pregi

Il tempo di latenza è molto breve, i costi di lancio e costruzione sono ridotti rispetto ai satelliti più elevati
Si ha un'alta risoluzione per ottenere immagini più dettagliate
Sono facili da aggiornare, nel senso che le costellazioni di satelliti possono essere integrate o sostiuite rapidamente
Le stazioni terrestri non hanno bisogno di molta energia, il ritardo nelle comunicazioni è di pochi millisecondi

2.3.4 Difetti

Avendo una durata operativa molto bassa, ora sono presenti tantissimi detriti spaziali che rischiano di scombussolare l'intero sistema dei satelliti causando un effetto domino

Inoltre hanno una copertura limitata e dei costi di manutenzione elevati (nel senso che sono necessari lanci frequenti)

3 Bit o baud rate

3.1 Descrizione

Sono metriche di misurazione dell'informazione passata ogni secondo e permettono di calcolare la larghezza di banda
Bit rate: è il doppio del baud rate, è il numero di bit che si possono trasmettere contemporaneamente con ogni impulso
Baud rate: si trasmette un impulso usando 4 frequenze con l'alfabeto composto da 4 simboli con ognuno dal peso di 2 bits

3.2 Ambiti d'uso

Utilizzato per calcolare le larghezze di banda di diversi sistemi e confrontarli, trasferimento di file, comunicazioni digitali, media streaming, sistemi di trasmissione digitale con modulazione complessa

3.3 Pregi

3.3.1 Bit

Indicatore di qualità:
più alto è il bit rate, maggiore è la qualità dei dati trasmessi (ad esempio, immagini meno compresse nei video)
Scalabilità:
adattabile in base alle capacità del canale (esempio: streaming adattivo)
Misura diretta:
facile da interpretare come velocità di trasmissione

3.3.2 Baud

Misura dell'efficienza spettrale:
indica quanto efficacemente la banda di frequenza è utilizzata
Rilevanza per il canale fisico:
permette di ottimizzare la trasmissione per canali con larghezza di banda limitata

3.4 Difetti

3.4.1 Bit

Non tiene conto dell'efficienza del canale:
un bit rate elevato può consumare molta larghezza di banda anche se il canale non è utilizzato in modo efficiente
Dipende dalla codifica
un bit rate elevato non sempre significa qualità migliore; dipende dall'efficienza del codice usato
Suscettibilità agli errori:

a velocità più alte, i dati possono essere più vulnerabili al rumore e alle interferenze

3.4.2 Baud

Non direttamente legato alla velocità dei dati:
il baud rate da solo non indica quanti bit vengono effettivamente trasmessi (esempio: un simbolo può rappresentare più bit)
Dipendenza dalla modulazione:
richiede informazioni aggiuntive sulla tecnica di modulazione per essere interpretato correttamente
Più difficile da misurare:
in sistemi avanzati, calcolare il baud rate richiede una conoscenza precisa dei dettagli del sistema

4 Serie di Fourier

La trasformata di Fourier è un'operazione matematica che permette di rappresentare un segnale (tipicamente una funzione nel dominio del tempo o dello spazio) come una somma di funzioni sinusoidali (onde di diversa frequenza)
In altre parole, la trasformata di Fourier consente di passare al dominio della frequenza, rivelando le componenti di frequenza che compongono il segnale
La trasformata di Fourier scompone un segnale in una serie di onde sinusoidali di diverse frequenze, ampiezze e fasi
Questo è particolarmente utile perché:
Analisi di segnali:
Permette di analizzare un segnale in termini di frequenze, utile ad esempio in elaborazione del segnale (audio, video, immagini), comunicazioni, acustica, fisica, e in molte altre aree
Filtraggio: Consente di isolare o rimuovere frequenze specifiche (ad esempio, per ridurre il rumore in un segnale)
Compressione: Le trasformate di Fourier sono utilizzate in tecniche di compressione dei dati, come nel formato MP3 per l'audio o JPEG per le immagini
La trasformata di Fourier è uno strumento potente per analizzare la struttura di frequenza di un segnale e viene utilizzato in numerosi campi come la fisica, l'ingegneria, le telecomunicazioni e l'elaborazione dei segnali

5 QPSK (2015)

5.1 Descrizione

QPSK vuol dire "Quadrature phase shift keying) e indica lo spostamento di fase delle onde con la chiave con 4 intervalli simmetrici: 45°, 135°, 225°, 315°
Ogni stato rappresenta un simbolo, consentendo la trasmissione di 2 bit per simbolo
Ciò rende il QPSK il doppio più efficiente rispetto alla modulazione BPSK (Binary Phase Shift Keying) in termini di bit trasmessi per baud

5.2 Ambiti d'uso

Si usa per modulare il segnale digitale in modo da far funzionare correttamente l'infrastruttura telefonica tra cui reti mobili (3G, 4G), sistemi satellitari per comunicazioni bidirezionali, nella televisione digitale e nel Wi-Fi

5.3 Pregi

Efficienza spettrale: Raddoppia il numero di bit trasmessi rispetto a tecniche più semplici come BPSK
Robustezza: È meno suscettibile al rumore rispetto a modulazioni con più simboli, come QAM-16
Facilità di implementazione grazie alla semplicità dei circuiti richiesti

5.4 Difetti

Più aumentano i simboli più sono simili causando problemi nelle telecomunicazioni
Ci sono limitazioni in ambienti rumorosi senza tecniche avanzate di correzione degli errori
Efficienza limitata, sicuramente inferiore alla QAM

6 QAM (2019, 20, 22, 23)

6.1 Descrizione

Ci sono diversi tipi di QAM:
Col QAM-16 si combinano più tipi di modulazione (4 ampiezze e 4 fasi per un totale di 16 combinazioni) in modo che se qualcosa viene attenuato o disperso il sistema è più robusto permettendo la trasmissione di 4 bit per simbolo
Poi esiste anche il QAM-64 il quale permette di arrivare a un bitrate sestuplo rispetto ai baud (6 bit per simbollo) e 3 volte quello dei QPSK

6.2 Ambiti d'uso

Usato principalmete per telecomunicazioni e reti dati come DSL, ADSL, Reti wireless, tecnologie 4G e 5G, per la televisione digitale e il broadcasting, per le comunicazioni satellitari, per il modem e la trasmissione dati su fibra ottica

6.3 Pregi

Può trasmettere più bit per simbolo rispetto ad altre tecniche di modulazione aumentando capacità del canale senza aumentare la larghezza di banda
Maggiore velocità di trasmissione
Flessibilità (esistono molte varianti)
Compatibilità con diverse tecnologie
Supporto per applicazioni moderne (streaming video, gaming online e in generale per alta velocità)

6.4 Difetti

Richiede canali di alta qualità e un hardware complesso
Limitazioni dei QAM rettangolari: Sebbene più semplici da generare, non sono ottimali come i QAM circolari, che però sono più difficili da implementare in pratica e per questo si preferisce i QAM rettangolari

7 ADSL (2024)

7.1 Descrizione

L'Asymmetric DSL (ADSL) è un tipo di DSL (Digital Subscriber Line) le quali sono nate per via della crescente necessità di maggiore capacità di download come streaming video e contenuti multimediali
L'ADSL sfrutta la rete telefonica esistente, rimuovendo i tradizionali filtri limitati a 4 kHz e ampliando lo spettro di frequenza fino a 1,1 MHz
Per evitare interferenze tra il segnale telefonico e quello internet, viene introdotto lo splitter, un filtro economico che separa le due bande (voce e dati)

7.2 Ambiti d'uso

Usata come sistema di connessione per abitazioni private, piccole e medie imprese, appartamenti e condomini

7.3 Pregi

Si può spezzare la banda in 256 sottocanali da 4312.5Hz (1 voce, 5 vuoti, 32 upload, resto download) e indipendenti, ovvero ogni canale viene trattato come una connessione telefonica a sè stante e c'è controllo costante sulla qualità della trasmissione → ogni canale può essere rallentato/accelerato indipendetemente
Inoltre si ha un costo contenuto e un'accessibilità diffusa

7.4 Difetti

La velocità e la qualità della connessione ADSL diminuiscono significativamente con l'aumentare della distanza dell'abitazione o dell'ufficio dalla centrale telefonica
Ad esempio, a distanze superiori a 4-5 km dalla centrale, la velocità può ridursi drasticamente o la connessione potrebbe diventare instabile
Oltretutto un altro suo difetto è l'asimmetria, in quanto la banda disponibile per il download è molto maggiore rispetto a quella per l'upload limitando le applicazioni che richiedono connessione bilanciata
Infine oggi è ormai superata da tecnologie più moderne e veloci come fibra ottica, 5G, VDSL

8 TDM Multiplexing (2016)

8.1 Descrizione

Il Time Division Multiplexing (TDM) è una tecnica di multiplazione che consente la condivisione di un unico canale di trasmissione tra più segnali
Invece di separare i segnali attraverso frequenze diverse (come avviene nel Frequency Division Multiplexing, FDM), il TDM utilizza intervalli temporali distinti per trasmettere i segnali

8.2 Ambiti d'uso

Ampiamente utilizzato nelle telecomunicazioni (trasmissione di segnali vocali e dati su reti digitali), reti di trasmissione dati (Ethernet e WAN), sistemi satellitari, sistemi di trasmissione televisiva (segnali multipli su un singolo canale)

8.3 Pregi

Permette di avere un'elevatissima flessibilità, un'ottima efficienza spettrale in quanto si usa un'unica banda e una buona compatibilità (dalle linee telefoniche ai sistemi satellitari)

8.4 Difetti

Più i canali aumentano più ognuno avrà a disposizione meno capacità e quindi sarà più lento
Sincronizzazione complessa precisa tra trasmettitore e ricevitore
Sensibilità al ritardo, il quale se accumulato influenza negativamente sulla qualità dei servizi in tempo reale come la voce o il video

9 Handoff (2023)

9.1 Handoff 1G

Nella prima generazione di trasmissione dati attraverso la rete di telefonia mobile, analogica, uno degli standard principali era l'AMPS (Advanced Mobile Phone System) per gli USA
L'handoff era una tecnica che occorreva quando il segnale era debole per ricollegarsi ad un segnale migliore
In questa situazione lo switching office (la stazione base di ogni cella) chiede alle celle vicino quanta potenza ricevono dal cellulare ed esso viene assegnato alla cella con potenza più alta
Ci sono due tipi:

1. **hard handoff**: la vecchia stazione rilascia il cellulare prima che la nuova lo riagganci causando un ritardo di circa 0,3 secondi

2. **soft handoff**: la nuova cella acquisisce il cellulare prima che la vecchia cella lo lasci, eliminando le interruzioni ma il cellulare deve collegarsi a due frequenze contemporaneamente aumentando costi e consumo energetico

9.2 Handoff 2G

Mentre nell'handoff 1G se ne occupa il control switch, nel nuovo standard D-AMPS (evoluzione dell'AMPS e retrocompatibile) inizia l'idea delle "tacchette" presente nei telefoni attuali
Con questo sistema si rappresenta la potenza del segnale permettendo di monitorare costantemente la qualità della connessione
Questo approccio è noto come MAHO (Mobile Assisted Hand Off) permettendo un carico aggiuntivo minimo poiché le misurazioni vengono effettuate durante i tempi morti del TDM

10 Modulazione delta (2016, 17, 18, 19, 20, 22, 23)

10.1 Descrizione

La modulazione delta è una tecnica di codifica a basso consumo utilizzata per comprimere segnali analogici in modo semplice ed efficiente
Il principio base è quello di campionare il segnale a intervalli regolari e confrontare ogni campione con il valore precedente
Se il segnale cresce, si registra un 1; se diminuisce, si registra uno 0
Questa rappresentazione descrive l'andamento del segnale, ma non ne conserva la forma precisa

10.2 Ambiti d'uso

Usato per le compressioni delle trasmissioni in digitale (come ad esempio per il 2G), nelle trasmissioni audio in dispositivi che non richiedono una qualità elevata, sistemi di acquisizione dati, nei dispositivi a bassa potenza, comunicazioni wireless a bassa velocità

10.3 Pregi

Efficienza di compressione, basso consumo energetico e velocità di elaborazione

10.4 Difetti

Si ha una perdita di qualità in quanto non conserva informazioni dettagliate sulla forma dell'onda originale
Inoltre si ha dipendenza dalla velocità di campionamento, se troppo lento può introdurre errori significativi nella ricostruzione del segnale

11 CDMA (Code Division Multiple Access) (2016, 18)

11.1 Descrizione

Il CDMA (Code Division Multiple Access) è una tecnologia di comunicazione wireless che consente a più utenti di condividere la stessa banda di frequenza simultaneamente
Ogni utente è identificato da un codice univoco (codice di spreading), che permette di distinguere i segnali sovrapposti sfruttando la teoria della codifica
CDMA lavora sullo spazio multidimensionale in cui i codici generano degli "assi" per garantire la separazione tra utenti

11.2 Ambiti d'uso

È stata utilizzata nelle reti cellulari di seconda generazione (2G) e terza generazione (3G) dove è alla base dello standard W-CDMA, usato per comunicazioni mobili con velocità superiori

11.3 Pregi

Efficienza nell'uso della banda (più utenti condividono lo stesso spettro), gestione intelligente del traffico, robustezza contro le interferenze e utilizzo flessibile dello spettro

11.4 Difetti

Presenta difetti legati alla gestione della potenza (le variazioni della distanza tra l'utente e la stazione base comportano che gli utenti più lontani debbano aumentare la loro potenza di trasmissione, causando così una maggiore interferenza e aumentando il consumo energetico), all'interferenza tra utenti (se i codici non sono abbastanza distinti o se vi sono errori nei codici, può verificarsi un'interferenza tra i segnali), alla complessità dell'hardware (i dispositivi e le stazioni base sono complesse e costose da progettare)

12 Bit o byte stuffing (2017, 18, 19, 20, 22, 23, 24)

Nel campo delle reti l'escaping è una tecnica fondamentale per garantire che i dati trasmessi siano interpretati correttamente
Due tecniche principali sono il byte stuffing e il bit stuffing

12.1 Byte stuffing

12.1.1 Descrizione

Il byte stuffing consiste nell'aggiungere caratteri speciali di escape per distinguere i dati effettivi da caratteri riservati o delimitatori (FLAG) che indicano l'inizio o la fine del pacchetto

Nell'header dati si indica di cosa si tratta
Nel payload si caricano i dati necessari per il messaggio
Nel trailer, uguale all'header, ci sono i dati per identificare la chiusura del pacchetto
FLAG finale: segna la fine del frame
Se nel payload compare un carattere uguale al FLAG o un carattere di escape, viene preceduto da un ulteriore carattere di escape per evitarne l'interpretazione errata

12.1.2 Ambiti d'uso

Il byte stuffing è utilizzato per codificare pacchetti dati nei protocolli a frame, come nelle comunicazioni seriali o nei protocolli di livello data link (esempio: PPP)

12.1.3 Pregi

Metodo semplice e intuitivo per gestire il problema dei caratteri riservati
Il primo metodo adottato per realizzare l'escaping risultando storico e consolidato in molte applicazioni

12.1.4 Difetti

Il problema potenziale è che ci possono essere molte più flag/escape del necessario, in quanto ogni carattere originale dopo lo stuffing è preceduto da un escape, e se già ci sono degli escape nel messaggi originale in quello finale ce ne saranno molti di più rendendo lunga la decodifica del messaggio
Oltretutto usa grandezze fisse il che lo rende inefficiente in contesti che richiedono maggiore flessibilità

12.2 Bit stuffing

12.2.1 Descrizione

Il bit stuffing è una tecnica più sofisticata che lavora a livello di bit anziché di byte
In questa tecnica, viene aggiunto un bit 0 ogni volta che nel flusso di dati appaiono cinque bit consecutivi impostati a 1
Questo serve a evitare che il ricevitore interpreti erroneamente una sequenza di bit come un FLAG

12.2.2 Ambiti d'uso

Il bit stuffing è ampiamente utilizzato in protocolli di comunicazione ad alta efficienza, come HDLC (High-Level Data Link Control), reti CAN, e altre tecnologie di trasmissione dati in cui è essenziale ottimizzare la trasmissione rispetto al byte stuffing

12.2.3 Pregi

Risolve il problema della grandezza fissa usando i bit e risolve il problema degli escaping multipli

Con la tecnica dello 0 dopo cinque 1 si ha un solo livello di escaping consentendo una più veloce decodifica

12.2.4 Difetti

1. Aumento della lunghezza del frame in quanto vengono aggiunti bit supplementari causando un aumento della lunghezza totale del frame, riducendo l'efficienza della trasmissione, specialmente in sistemi con messaggi lunghi

2. Maggiore complessità del decoder
   Il dispositivo ricevente deve avere la capacità di rilevare e rimuovere i bit aggiunti

3. Se un errore di trasmissione altera i bit "stuffati" o la sequenza originale, il ricevitore potrebbe interpretare erroneamente i dati, perdendo la sincronizzazione con il flusso di bit

4. Maggiore complessità del debugging:
   Durante il debug della comunicazione, i bit aggiunti rendono più complessa l'analisi del flusso dati, richiedendo strumenti in grado di gestire e interpretare correttamente il bit stuffing

13 Error control

13.1 Descrizione

L'error control è composto da error detection, che si occupa di accorgersi se il frame ha subito errori e nel caso ritrasmettendo dati, ed error correction, che corregge autonomamente i frame errati utilizzando tecniche che permettono di identificare e ripristinare i dati alterati

13.2 Ambiti d'uso

Ampiamente utilizzato in tutte le aree della comunicazione dati, dalle reti di telecomunicazione ai sistemi di archiviazione, in quanto è indispensabile per garantire la qualità e l'integrità delle informazioni

13.3 Pregi

Affidabilità: consente di rilevare e, in molti casi, correggere errori, migliorando l'affidabilità delle trasmissioni
Flessibilità: la capacità di rilevare o correggere errori varia in base alla tecnica utilizzata, adattandosi alle esigenze del sistema
Metriche di qualità: l'efficacia dell'error control è misurata attraverso la distanza di Hamming, ovvero il numero minimo di bit che differenziano due messaggi validi
Una maggiore distanza di Hamming indica una maggiore capacità di rilevare e correggere errori

13.4 Difetti

Purtroppo, sempre a causa della distanza variabile, non esistono tecniche di error control che permettono di correggere al 100% gli errori
Inoltre, prevede spesso una forte complessità computazionale e un overhead a causa dell'aggiunta dei bit di controllo

14 Stop and wait

14.1 Descrizione

Stop and wait è uno dei protocolli half-duplex (canale singolo) in cui tra ricevente e mittente si condivide un singolo canale e le comunicazioni avvengono in modo alternato
Il mittente trasmette un blocco dati (frame) e attende un segnale di conferma (acknowledgment) segnalandoci che si può inviare un altro messaggio
Se il ricevente rileva errori nel frame ricevuto, invia un messaggio di richiesta di ritrasmissione (NAK, negative acknowledgment)
Se il mittente non riceve nessun ACK entro un tempo prestabilito (timeout), ritrasmette il frame
Per evitare duplicazioni nel caso di ritrasmissioni, ogni frame include un identificatore (di solito un bit, 0 o 1) che permette di distinguere i dati già ricevuti da quelli nuovi

14.2 Ambiti d'uso

Viene utilizzato principalmente per gestire il flow control in situazioni dove è cruciale garantire l'affidabilità come nei collegamenti a bassa velocità o in ambienti con elevate probabilità di errore
Attualmente trova applicazione in contesti semplici

14.3 Pregi

Semplicità: l'implementazione è molto semplice, rendendolo ideale per applicazioni basilari o sistemi con risorse limitate
Robustezza: garantisce l'integrità dei dati grazie al meccanismo di ritrasmissione e alla conferma esplicita (ACK)
Compatibilità: funziona su canali half-duplex, dove la comunicazione simultanea non è possibile, riducendo i requisiti hardware

14.4 Difetti

Lentezza: poiché non è possibile inviare un nuovo frame prima di ricevere l'ACK del precedente, il protocollo introduce notevoli ritardi, soprattutto su canali con alta latenza
Bassa efficienza: utilizza male la larghezza di banda disponibile, dato che il canale rimane inattivo durante l'attesa degli ACK
Limiti in contesti moderni: non è adatto a sistemi ad alta velocità o reti con grandi volumi di dati, dove protocolli più avanzati (come sliding window) risultano preferibili

15 Go back n (2015, 20, 24)

15.1 Descrizione

Go back N è un tipo di protocollo di trasmissione basato sulla tecnica delle Sliding Windows,che consente l'aumento del grado di parallelismo (pipelining)
In questo tipo di protocollo il mittente può inviare fino a N frame consecutivi senza ACK ma il ricevente utilizza una finestra di dimensione 1 accettando i frame nell'ordine corretto
Se un frame arriva fuori sequenza viene scartato
In caso di errore o mancato ACK per un frame, il mittente ritrasmette tutti i frame a partire da quello non confermato, da qui il nome "Go-Back-N"
Questo protocollo è particolarmente efficace quando il prodotto bandwidth*round-trip-delay è elevato e la probabilità di errore è bassa

15.2 Ambiti d'uso

Ampiamente utilizzato nello strato data-link delle reti per gestire flusso di dati tra mittente e ricevente garantendo affidabilità nella trasmissione
Adatto dove la perdita o la corruzione dei dati è relativamente rara

15.3 Pregi

Efficienza migliorata rispetto a protocolli come lo Stop-and-Wait, poiché consente l'invio continuo di più frame senza attendere conferme immediate
Implementazione semplice, dato che richiede solo la ritrasmissione dei frame non confermati
Affidabilità garantita: ritrasmettendo tutti i frame a partire dall'errore, si evita qualsiasi dubbio sullo stato dei dati ricevuti
Controllo del flusso integrato: il mittente non sovraccarica il ricevitore, rispettando i limiti della finestra

15.4 Difetti

Overhead significativo in caso di errore: se un frame viene perso o corrotto, tutti i frame successivi devono essere ritrasmessi, anche se già correttamente ricevuti, causando un uso inefficiente del canale
Memoria e buffer aggiuntivi: il mittente deve mantenere una copia di tutti i frame non ancora confermati, aumentando il carico sul sistema
Non adatto a reti con alti tassi di errore, dove le frequenti ritrasmissioni possono saturare il canale e ridurre l'efficienza complessiva
Ritardo aumentato: i frame corretti che seguono un errore non possono essere elaborati finché il frame errato non viene ritrasmesso e riconosciuto

16 Selective Repeat (2022)

16.1 Descrizione

Selective Repeat è protocollo di trasmissione basato sulle Sliding Windows, progettato per gestire in modo efficiente la comunicazione tra mittente e ricevente

sopratutto in presenza di errori
In questo caso specifico la taglia delle sliding window per chi riceve è di una taglia maggiore rispetto ai Go back N (1) richiedendo però un buffer di taglia la sua apertura
Consente al ricevitore di accettare e memorizzare i frame ricevuti fuori ordine in un buffer
Permette al mittente di ritrasmettere solo i frame specifici che risultano persi o corrotti, riducendo l'overhead associato alla ritrasmissione di interi blocchi di dati

16.2 Ambiti d'uso

Viene utilizzato per le reti ad alta latenza e larghezza di banda elevata (comunicazioni satellitari e transoceaniche), nelle reti wireless e per i trasferimenti di dati critici in cui l'efficienza e l'affidabilità sono essenziali

16.3 Pregi

Alta efficienza: consente di ottimizzare l'uso della larghezza di banda, riducendo le ritrasmissioni inutili
Gestione dei frame fuori ordine: i frame ricevuti in anticipo o in ordine errato non vengono scartati, ma conservati in un buffer per il successivo riordino
Adatto a reti con alti tassi di errore: migliora le prestazioni rispetto al Go-Back-N in ambienti rumorosi, dove gli errori sono frequenti
Flessibilità: ideale per sistemi con requisiti di precisione e integrità dei dati

16.4 Difetti

Complessità maggiore: il ricevitore deve gestire un buffer sofisticato per i frame fuori ordine, aumentando il costo e la difficoltà di implementazione
Overhead elevato: a causa della necessità di buffer ampi e della gestione delle conferme per ogni singolo frame, l'overhead operativo è più alto rispetto ad altri protocolli
Problemi di sincronizzazione: la gestione delle finestre di trasmissione e ricezione può risultare complessa, specialmente in presenza di ritardi variabili o errori di sincronizzazione
Buffering elevato: la necessità di memorizzare i frame fuori ordine richiede più memoria, specialmente in reti ad alta velocità o con grandi dimensioni di finestra

17 HDLC

17.1 Descrizione

Protocollo concreto ideato inizialmente dall'IBM
I suoi frames sono delimitati tramite bit stuffing e sono composti da:

1. Data: è il payload
2. Checksum: calcolata usando CRC, una tecnica di error detection che sfrutta l'aritmetica polinomiale

3. Address: serve per la componente di indirizzamento
4. Control: flow control tramite sliding window <= 3 bit. Può essere:
   (a) Information: composto da Seq (n° controllo), next (ack in piggybacking) e P/F, un bit che indica P (Poll, si chiede al ricevente di iniziare la trasmissione) o F (Final, la trasmissione viene conclusa)
   (b) Supervisory: supervisione flusso di dati con campo Type
      i. Type 0: ACK quando il flusso è sbilanciato
      ii. Type 1:NAK, vanno ritrasmessi tutti i frame a partire da quello indicato
      iii. Type 2: Receiver not ready
      iv. Type 3: classico NAK
   (c) Unnumbered: è usato per ulteriori comandi di controllo:
      i. DISC (DISConnect): la macchina sta uscendo dalla rete in maniera definitiva
      ii. SNRM (Set Normal Response Mode): la nuova macchina entrata nella rete è meno importante
      iii. SABM (Set Asynchronous Balanced Mode): la nuova macchina entrata nella rete ha gli stessi diritti
      iv. FRMR (Frame Reject):il frame appena arrivato ha una sequenza di controllo non corretta/sconosciuta
      v. UA (Unnumbered ACK): ACK non numerato (la sliding window è una)

17.2 Ambiti d'uso

Attualmente viene usato per modem/fax, reti di vario tipo e molti circuit bancari

17.3 Pregi

Affidabilità nella trasmissione:
HDLC utilizza meccanismi di rilevamento e correzione degli errori tramite checksum (Cyclic Redundancy Check, CRC), riducendo significativamente il rischio di errori nella trasmissione
Versatilità:
supporta configurazioni punto-punto e multipunto, rendendolo adatto a diverse architetture di rete
Controllo di flusso efficiente:
implementa tecniche di acknowledgment e gestione della finestra scorrevole per garantire una trasmissione fluida ed evitare congestioni
Semplicità delle operazioni:
le tre modalità di funzionamento (Normal Response Mode, Asynchronous Balanced Mode, e Asynchronous Response Mode) permettono flessibilità e semplicità nell'implementazione
Efficienza nella trasmissione continua:
HDLC utilizza frame strutturati con overhead minimo, ottimizzando la trasmissione di dati su collegamenti con capacità elevate

17.4 Difetti

Complessità di implementazione:
nonostante la standardizzazione, HDLC richiede un'implementazione relativamente complessa per gestire tutte le sue funzioni (controllo di flusso, rilevamento errori, configurazioni multipunto)
Overhead di controllo:
anche se il protocollo è efficiente, l'uso di campi di controllo, intestazioni e sequenze di frame introduce un overhead che può influire negativamente su collegamenti a bassa velocità
Non ottimale per reti moderne:
è stato progettato per linee seriali e reti tradizionali; potrebbe non essere ideale per reti moderne basate su Ethernet o reti wireless, dove altri protocolli sono più efficienti
Limiti nella gestione degli errori:
sebbene HDLC rilevi errori, non sempre riesce a correggerli
In caso di errore, il frame deve essere ritrasmesso, aumentando il ritardo

18 PPP

18.1 Descrizione

Le connessioni Internet possono essere dedicate punto a punto (point-to-point)
In Internet si usa il protocollo PPP (point-to-point protocol)
Questo tipo di protocollo dà un metodo di framing per impacchettare dati che può essere LCP o NCP:
LCP (Link Control Protocol): si occupa del controllo delflusso per attivare le connessione, test, negoziazione e chiusura
NCP (Network Control Protocol): è il metodo per negoziare con lo strato superiore Network
PPP usa byte stuffing nonostante sia leggermente meno efficiente perché è una tecnica di encoding più veloce rispetto al bit stuffing, e nella base di Internet anche la minima velocità in più fa la differenza
Ha diversi campi:

1. FLAG: delimitatore frame
2. Address: non viene mai usato, valore costante 11111111 (può essere tolto del tutto)
3. Control: non si usa, valore costante 00000011 (può essere tolto del tutto)
4. Protocol: si specifica il protocollo implementato (bit 0 per NCP, bit 1 per LCP)
5. Checksum: calcolato usando CRC e fa solo error detection
6. Payload: dati il cui significato dipende dal protocollo implementato

18.2 Ambiti d'uso

Lo strato fondamentale di Internet, su di esso si basano tutti i protocolli "avanzati" e permette un rapido invio di messaggi con un error detection in aritmetica polinomiale

18.3 Pregi

Grazie al byte stuffing è molto veloce e permette le connessioni punto a punto negli strati base di Internet

18.4 Difetti

Purtroppo usando il byte stuffing dipende da delle grandezze fisse e non per l'appunto dai singoli bit come avviene nel bit stuffing

19 Aloha (2014, 17, 18, 19, 21, 23)

19.1 Descrizione

Aloha è un tipo di protocollo multiaccesso, ovvero quei sistemi di comunicazione multipla in cui c'è un unico canale condiviso da molti (contention)
Ogni protocollo di questo tipo ha la station model (entità che trasmettono) e le collision (quando 2 frame si sovrappongono c'è una collisione e sono inutilizzabile rendendo inutile CDMA)
Questo protocollo sfrutta le probabilità, infatti, nell'eventualità di una collisione, il tempo di ritrasmissione è deciso dalle probabilità
La probabilità che k frames siano generati in un certo intervallo di tempo è di tipo Poisson e viene studiata con la sua distribuzione
Grazie a questa si ottiene che con Aloha "classico" si ottiene un 18,4% di banda che ha il pregio di non dipendere dal numero di trasmissioni contemporanee
Invece, con lo slotted Aloha (in cui la trasmissione è permessa solo all'inizio di uno slot) si arriva a un 36,8% di banda
Questo tipo di protocollo non ha il carrier sense (la stazione non può analizzare il canale finché non lo usa)

19.2 Ambiti d'uso

Reti wireless a bassa complessità:
è stato utilizzato nelle reti satellitari e nelle prime reti mobili, dove la semplicità era una priorità
Reti di sensori:
può essere applicato in reti di sensori distribuiti, dove i nodi trasmettono dati solo sporadicamente
Reti RFID:
utilizzato per la comunicazione tra tag RFID e lettori, dove le collisioni sono gestite in modo autonomo
Sistemi di comunicazione a bassa velocità:
ideale per applicazioni a basso traffico e ridotta necessità di coordinamento

19.3 Pregi

Semplicità di implementazione:
il protocollo non richiede una gestione complessa o una sincronizzazione rigorosa tra i nodi
Distribuzione decentralizzata:
ogni dispositivo agisce in modo autonomo, rendendo il sistema flessibile e adatto a reti distribuite
Adattabilità:
può essere facilmente implementato in sistemi con traffico intermittente o poco intenso
Robustezza:
in reti con pochi nodi o basso traffico, ALOHA funziona bene, garantendo una trasmissione rapida dei dati

19.4 Difetti

Efficienza bassa:
Nel Pure ALOHA, l'efficienza massima teorica è del 18% (1/2e), a causa delle collisioni frequenti
Nello Slotted ALOHA, l'efficienza migliora ma si ferma a circa il 37%
Gestione delle collisioni:
non esiste un meccanismo preventivo per evitare collisioni; ciò comporta ritrasmissioni e perdita di tempo e risorse
Non adatto a traffico elevato:
quando il numero di utenti cresce, il tasso di collisioni aumenta esponenzialmente, rendendo il protocollo inefficace
Latenza alta nei casi peggiori:
con molte collisioni, i tempi di ritrasmissione possono aumentare significativamente, generando latenza

20 CSMA (2017, 18, 20)

20.1 Descrizione

CSMA (Carrier Multiple Access Protocol) è un protocollo multiaccesso più complesso ispirato da Aloha
Prima di trasmettere si controlla se non ci sia già una trasmissione e, se essa è presente, controlla il canale e appena si libera trasmette il messaggio
Ci sono diverse varianti di CSMA, che migliorano il protocollo in base al modo in cui le collisioni vengono gestite:
CSMA/CD (Collision Detection):
utilizzato nelle reti Ethernet cablate, rileva le collisioni durante la trasmissione e interrompe immediatamente la trasmissione
CSMA/CA (Collision Avoidance):
utilizzato nelle reti wireless (come Wi-Fi), cerca di evitare le collisioni implementando un sistema di attesa (backoff) e segnalazioni di conferma (acknowledgments)
CSMA senza controllo delle collisioni
il dispositivo trasmette solo se il canale è libero, ma non reagisce alle collisioni

20.2 Ambiti d'uso

Ethernet (CSMA/CD):
reti Ethernet cablate delle prime generazioni (ad esempio reti 10BASE5 e 10BASE2), dove più dispositivi condividevano lo stesso mezzo trasmissivo
Wi-Fi (CSMA/CA):
reti wireless, come IEEE 802.11, dove le collisioni sono difficili da rilevare ma possono essere mitigate con strategie di evitamento
Sistemi wireless a bassa potenza:
ad esempio in reti di sensori o reti IoT (Internet of Things), dove i dispositivi comunicano su un canale condiviso
Reti satellitari o radio:
utilizzato nei sistemi dove il mezzo trasmissivo è condiviso da molteplici dispositivi e le risorse radio sono limitate

20.3 Pregi

Semplicità:
CSMA è relativamente semplice da implementare e si adatta bene a reti a basso traffico o con poche stazioni attive
Efficienza in reti leggere:
Con pochi dispositivi attivi, la probabilità di collisione è bassa, e il protocollo garantisce una trasmissione efficace
Flessibilità:
è adatto sia a reti cablate (CSMA/CD) sia a reti wireless (CSMA/CA), con modifiche per adattarsi alle caratteristiche specifiche del mezzo trasmissivo
Uso decentralizzato:
Non richiede un coordinatore centrale, rendendolo adatto a reti distribuite
Adattabilità dinamica:
il meccanismo di rilevazione o evitamento di collisioni consente al protocollo di reagire in tempo reale ai cambiamenti nel traffico della rete

20.4 Difetti

Problemi con traffico elevato:
all'aumentare del numero di dispositivi, aumenta la probabilità di collisioni, riducendo drasticamente l'efficienza
Collisioni inevitabili:
anche con il carrier sensing, le collisioni possono avvenire, specialmente nei sistemi con alti tempi di propagazione del segnale (ad esempio reti wireless)
Degrado delle prestazioni:
Quando la rete è congestionata, CSMA può portare a ritrasmissioni frequenti, riducendo l'efficienza complessiva e aumentando i ritardi

21 CSMA non persistent (2022)

21.1 Descrizione

Il CSMA non persistente è un tipo di CSMA (protocollo multiaccesso) in cui, quando un dispositivo rileva che il canale è occupato, non continua a monitorarlo

costantemente
Invece, attende un intervallo di tempo casuale (random backoff) prima di verificare nuovamente se il canale è libero e riprovare la trasmissione
Questo approccio aiuta a ridurre la probabilità di collisioni rispetto al CSMA 1-persistente (dove i dispositivi trasmettono immediatamente quando rilevano il canale libero)
Esso può raggiungere performance fino al 90%

21.2 Ambiti d'uso

Il CSMA non persistente è adatto a scenari in cui la riduzione delle collisioni è cruciale e il traffico della rete non è eccessivamente intenso
Gli ambiti principali includono:
Reti locali cablate (LAN):
può essere utilizzato in reti Ethernet tradizionali con basso o moderato traffico
Reti di sensori e IoT (Internet of Things):
sistemi con dispositivi che trasmettono dati sporadicamente, dove si vuole ridurre il rischio di collisioni
Comunicazioni satellitari o radio:
in reti dove i tempi di propagazione sono elevati e si richiede un approccio più conservativo per ridurre le collisioni
Sistemi di controllo industriale:
utilizzato in ambienti con un numero limitato di dispositivi che devono trasmettere senza sovraccaricare il canale

21.3 Pregi

Il CSMA non persistente offre diversi vantaggi:
Riduzione delle collisioni:
l'attesa di un tempo casuale prima di riprovare la trasmissione riduce la probabilità che più dispositivi trasmettano contemporaneamente quando il canale diventa libero
Maggiore efficienza in condizioni di traffico moderato:
la probabilità di saturare il canale diminuisce rispetto ad altri approcci, come il CSMA 1-persistente
Semplicità di implementazione:
non richiede un coordinamento centrale o sincronizzazione complessa, rendendolo adatto a reti distribuite
Adattabilità dinamica:
funziona bene in reti con traffico non prevedibile o carico variabile

21.4 Difetti

Il CSMA non persistente presenta anche alcune limitazioni:
Maggiore latenza:
l'attesa casuale introduce ritardi anche quando il canale è libero, causando una latenza maggiore rispetto ad altri protocolli (ad esempio, CSMA 1-persistente)
Prestazioni degradate in reti congestionate:
in condizioni di alto traffico, il numero di tentativi falliti e le attese casuali possono aumentare il ritardo medio e diminuire l'efficienza

Minore utilizzo del canale in reti leggere:
Rispetto al CSMA 1-persistente, in situazioni con pochi dispositivi attivi, il protocollo non persistente può essere meno efficiente perché introduce attese inutili
Difficoltà nel garantire priorità:
Non offre meccanismi per assegnare priorità alla trasmissione di dati urgenti, rendendolo meno adatto a reti con traffico prioritario

22 Protocolli a contesa limitata: adaptive tree walk protocol (2015, 18, 24)

22.1 Descrizione

I protocolli a contesa limitata cercano di unire i lati positivi dei metodi della contesa e dei metodi senza collisioni
Infatti si cerca di crearne uno capace di usare il metodo della contesa per ottenere un ritardo limitato a basso carico e il metodo senza collisioni per raggiungere una buona efficienza di canale nelle situazioni a carico più elevato
SI basa sulle probabilità
Dividono le stazioni in gruppi in cui ognuno ha uno slot e solo le stazioni di quel gruppo possono competere per quello slot
Se uno di loro vince acquisisce il controllo del canale e trasmette il frame altrimenti se l'intervallo rimane inutilizzato o c'è una collisione si "avvia" il secondo gruppo
La difficoltà è ridurre il livello di contdesa per ogni intervallo
Lo slotted ALOHA è un tipo di protocollo in cui tutte le stazioni sono in un singolo gruppo
Un esempio è l'adaptive tree walk protocol, il quale può essere visto come un albero binario dove, nel primo slot tutti possono tentare di acquisire il controllo del canale ma se nessuno ci riesce viene diviso a metà in modo da far contendere N/2 stazioni ogni volta in modo ricorsivo fino a quando non si trova chi vince per trasmettere il suo frame
Dato che l'algoritmo ricerca dal basso all'alto si parte dal livello P che sarebbe il logaritmo in base 2 del numero di stazioni attive per individuare più velocemente la stazione a cui permettere di trasmettere il frame

22.2 Ambiti d'uso

Sono protocolli utilizzati in ambiti come reti Ethernet, reti wirelsse, mobile, nei sistemi operativi per la gestione delle risorse condivise, nei sistemi distribuiti e nell'Internet of Things
L'adaptive tree walk protocol viene usato specialmente per reti a traffico elevato, reti satellitari, gestione delle trasmissioni dei disposivitivi Internet of Things, nelle applicazioni di monitoraggio

22.3 Pregi

1. C'è una notevole riduzione delle collisioni in cui i protocolli a contesa limitata riducono significativamente le collisioni rispetto ai protoccoli ran-

domici, l'adaptive tree walk protocol suddivide dinamicamente i dispositivi in gruppi gerarchici analizzandoli uno per uno in modo ordinato

2. Sono più efficienti in condizioni di traffico moderato o elevato, adattandosi dinamicamente al numero di dispositivi in contesa, l'adaptive tree walk protocol eccelle in questo contesto, poiché modifica il comportamento in base al libello di contesa

3. I protocolli garantiscono che tutti i dispositivi abbiano possibilità eque di accedere al canale

4. L'adaptive tree walk protocol ha una scalabilità molto elevata in quanto si può avere un numero crescente di nodi

22.4 Difetti

I difetti possono essere l'overhead di controllo, la latenza elevata in caso di traffico leggero, la complessità di implementazione (la navigazione dinamica e la costruzione di una struttura ad albero richiedono parecchia complessità) e non è ottimale in ambienti asincroni

23 Stazione nascosta (2019, 20, 24)

23.1 Descrizione

Nei casi wireless la topologia della rete non è fissa ma cambia dinamicamente causando il fatto che non c'è un singolo canale per tutti ma varie zone spaziali dove alcune stazioni interagiscono ed altre no
Quindi il controllo diventa locale compromettendo l'invio singolo di dati ma rischiando l'invio contemporaneo di più dati
La stazione nascosta è il problema in cui una stazione non riesce a vedere che la stazione alla quale vuole inviare dei dati ne sta già ricevendo altri, quindi ne invia causando l'arrivo contemporaneo di dati alla stessa stazione e di conseguenza la collisione
Infatti, nei casi wireless, si trasmette "a bolla" propagando le informazioni e non in linea retta verso l'obiettivo

23.2 Quando avviene

Ipotizziamo che ci siano A, B, C in sequenza in cui il segnale a bolla di A, arrivi a B, il segnale a bolla di B arriva ad A e C e il segnale a bolla di C arriva ad A
A vuole inviare dei dati a B, però anche C vuole inviare dei dati a B, ma C non sente che A sta già inviando dei dati quindi li invia a B causano la collisione dei dati trasmessi in contemporanea da A e C, la quale è la stazione nascosta per A

23.3 Come risolvere

Si usa il MACA (Multiple Access with Collision Avoidance) in cui si sfrutta l'idea che chi trasmette renda il suo spazio locale conosciuto anche agli altri

Avviene tramite due comandi: RTS (Request To Send) che contiene l'informazione del frame e a chi si vuole trasmettere
CTS (Confirm To Send) il quale è l'ACK
Chiunque sente l'RTS e il CTS ma non è né destinatario né mittente non trasmette a loro due fino a quando non è conclusa
Per controllare se la trasmissione è conclusa si sfrutta il protocollo Aloha in modalità non persistente che viene usato anche per trasmissioni multiple alla stessa stazione

24 802.3

24.1 Descrizione

802.3 è uno dei protocolli più famosi della storia ed è uno dei protocolli di Ethernet, il quale si prevede come minimo sarà in vigore fino al 2080/2100
Questo protocollo in particolare ha un tipo di cablaggio a "serpente", a "lisca di pesce" e ad "albero"
I suoi vari tipi hanno un nome identificato "XBaseY" in cui X è la banda in Mbps, "Base" indica che è una connessione baseband (a frequenza unica) e Y è il tipo di cavo che differisce a seconda della lunghezza massima di ogni tratto senza ripetitori

24.2 Ambiti d'uso

Utilizzato principalmente per le reti locali LAN in cui addirittura è l'ambito principale dello standard, per il data center e cloud computing (è necessario un Ethernet ad alte prestazioni), in ambienti industrali, per le reti di provider di servizi e per le reti domestiche

24.3 Pregi

L'Ethernet ha un'elevatissima diffusione e interoperabilità, un'altissima affidabiltà grazie all'uso di tecnologie come il controllo delle collisioni e miglioramenti successivi con reti full-duplex, la velocità scalabile (dai 10Mbps ai 400Gbps), ai suoi costi contenuti grazie all'ampia adozione e alla facilità di installazione e manutenzione

24.4 Difetti

Alcuni difetti possono essere le limitazioni geografiche, la dipendenza dal cablaggio fisico, la scalabilità rispetto al wireless, il costo delle soluzioni ad alte prestazioni, la mancanza di mobilità e i consumi energetici

25 Codifica Manchester (2014, 18, 19, 20, 22, 24)

25.1 Descrizione

La codifica Manchester è una tecnica di comunicazione dati in cui ogni bit è rappresentato da una transizione all'interno di un intervallo di tempo predefinito
Questa caratteristica la rende auto-sincronizzante, consentendo una sincronizzazione precisa del flusso di dati tra il trasmettitore e il ricevitore
Ogni bit viene trasmesso con una transizione specifica che ne identifica il valore:
Una transizione da alto a basso può rappresentare uno 0
Una transizione da basso ad alto può rappresentare un 1 (o viceversa, a seconda della convenzione adottata)

25.2 Ambiti d'uso

La codifica Manchester è ampiamente utilizzata per la trasmissione dei dati a livello fisico in tecnologie come Ethernet
Il suo principale vantaggio è la capacità di risolvere i problemi di sincronizzazione dei segnali, rendendo superflua l'adozione di hardware complesso e costoso
Tuttavia, questo beneficio comporta un compromesso:
la larghezza di banda disponibile viene ridotta

25.3 Pregi

1. Hardware economico:
   la semplicità del segnale e delle transizioni permette di utilizzare hardware meno costoso

2. Auto-sincronizzazione:
   la presenza di una transizione in ogni intervallo di tempo del bit garantisce una sincronizzazione precisa senza l'uso di clock separati

3. Alta affidabilità:
   la robustezza della codifica consente di mantenere elevate prestazioni di rete anche in condizioni non ideali, rendendola adatta a incrementare la banda senza incrementare significativamente i costi hardware

25.4 Difetti

Riduzione della banda disponibile: il principale svantaggio della codifica Manchester è il dimezzamento della banda, poiché per ogni bit trasmesso sono necessarie due transizioni

26 Flooding (2015, 16, 18, 20, 23)

26.1 Descrizione

Il flooding è un algoritmo di routing, ovvero quel genere di algoritmi in cui ci si preoccupa di consegnare i pacchetti su una rete complessa

Nel flooding ogni pacchetto viene ritrasmesso su tutte le linee di uscita, garantendo che il pacchetto raggiunga ogni possibile destinazione
Per evitare problemi di ridondanza e congestione, si usano dei metodi di controlllo aggiuntivi fra cui:
1) hop counting: indica il numero massimo di stazioni dopo le quali il pacchetto è inutilizzabile
2) tracking: tiene traccia dei pacchetti già trasmessi e non li ritrasmette per prevenire duplicazioni

26.2 Ambiti d'uso

Utilissimo quando il carico di rete non è molto alto, la topologia di rete è estremamente variabile ed è critico che un messaggio arrivi nel minor tempo possibile (indipendemente dall'efficienza complessiva)

26.3 Pregi

1) il flooding sceglie sempre la via migliore
2) è il più robusto algoritmo di routing rispetto alle modifiche della rete grazie al fatto che non è dipendente da tabelle di routing statiche

26.4 Difetti

Generazione di traffico eccessivo: si crea una quantità enorme di pacchetti che può rapidamente saturare la rete, riducendone l'efficienza complessiva
Uso inefficiente delle risorse: la ridondanza intrinseca del flooding implica che molti pacchetti vengano inviati inutilmente sprecando larghezza di banda e capacità di elaborazione dei nodi

27 Distance Vector routing (2014, 19, 20, 24)

Altro algoritmo di routing (vedi sopra)

27.1 Descrizione

Ogni router conserva una tabella che definisce la migliore distanza onosciuta per ogni destinazione e il collegamento che conduce a tale destinazione
Queste tabelle sono aggiornate scambiando informazioni con i router vicini
Alla fine del processo ogni router conosce il collegamento migliore per raggiungere qualsiasi destinazione

27.2 Ambiti d'uso

27.3 Pregi

Reagisce molto rapidamente alle buone notizie, convergendo velocemente alle risposte corrette calcolando i cammini minimi
Infatti le buone notizie sono elaborate in un solo scambio di vettori

27.4 Difetti

Reagisce troppo lentamente alle cattive notizie
Per esempio si supponga che il percorso il migliore da un router ad una destinazione X sia molto lungo, se uno degli scambi successivi con il vicino A imporvvisamente indica un ritardo breve verso X il router inizia ad utilizzare la linea che punta ad A per inoltrare il traffico verso X
In pratica questo è definito il problema del "conteggio all'infinito" e avviene quando X comunica a Y che ha un percorso che punta da qualche parte, Y non ha modo di sapere se fa parte di quel percorso

28 Link State Routing (2018, 21, 22, 23)

28.1 Descrizione

Il Link State Routing è un algoritmo di routing che consente ai nodi di una rete di ottenere una visione completa della topologia di rete, permettendo il calcolo dei percorsi ottimali per l'instradamento dei pacchetti
Il processo si articola in diversi passaggi:
Rilevamento dei vicini: ogni nodo identifica i propri nodi vicini tramite l'invio di pacchetti HELLO
Misurazione delle distanze: i nodi misurano la distanza dai loro vicini utilizzando pacchetti ECHO
Costruzione delle informazioni locali: ogni nodo raccoglie informazioni sui propri vicini e sulla distanza che li separa, costruendo un pacchetto denominato Link State Packet (LSP)
Broadcast delle informazioni: il pacchetto LSP viene inviato a tutti gli altri nodi della rete tramite un'operazione di broadcast basata sul flooding
Ricostruzione della mappa globale: ogni nodo riceve le informazioni locali di tutti gli altri nodi, ricostruendo così una mappa completa della rete
Calcolo dei percorsi ottimali: Utilizzando la mappa completa, ogni nodo applica un algoritmo di instradamento (ad esempio, l'algoritmo di Dijkstra) per calcolare i percorsi migliori verso ciascuna destinazione
Poiché la topologia della rete può variare nel tempo, il processo di broadcast deve essere ripetuto periodicamente per effettuare il refresh delle informazioni, garantendo che la mappa sia aggiornata e accurata
Questo comporta un maggiore utilizzo di banda rispetto ad altri algoritmi, ma migliora notevolmente la robustezza globale della rete, superando i limiti di soluzioni basate su informazioni locali

28.2 Ambiti d'uso

Il Link State Routing è utilizzato in contesti in cui è necessario un routing altamente dinamico, accurato e robusto
Gli ambiti principali includono:
Reti complesse con topologie dinamiche: ad esempio, reti di grandi dimensioni come le reti geografiche (WAN) o le dorsali Internet, dove la topologia varia frequentemente
Reti ad alta priorità sulla robustezza: applicazioni critiche che richiedono affidabilità elevata, come reti di provider di servizi e sistemi di controllo industriale

28.3 Pregi

1. Conoscenza globale della rete: ogni nodo dispone di una mappa completa della rete, consentendo di calcolare i percorsi ottimali per qualsiasi destinazione

2. Adattabilità ai cambiamenti: grazie al processo periodico di broadcasting, l'algoritmo reagisce rapidamente ai cambiamenti nella topologia della rete, mantenendo la mappa aggiornata

3. Robustezza: essendo basato su informazioni globali, il Link State Routing evita i problemi legati alla conoscenza locale, riducendo il rischio di instradamenti inefficienti o errori di rete

4. Calcolo di percorsi ottimali: utilizzando algoritmi come Dijkstra, garantisce sempre il percorso più corto e veloce tra i nodi

5. Scalabilità: funziona bene anche in reti di grandi dimensioni, grazie alla precisione e alla granularità delle informazioni trasmesse

28.4 Difetti

1. Elevato consumo di banda: il processo di broadcasting dei pacchetti LSP richiede una quantità significativa di larghezza di banda, specialmente in reti di grandi dimensioni

2. Maggiore complessità computazionale: il calcolo dei percorsi ottimali basato su una mappa globale richiede una maggiore capacità di elaborazione da parte dei nodi rispetto agli algoritmi di routing locali

3. Overhead per aggiornamenti periodici: anche quando la topologia della rete non cambia, il flooding deve essere ripetuto periodicamente per mantenere aggiornate le informazioni, causando un sovraccarico inutile in assenza di modifiche

29 Quality of Service (QOS) (2014, 20, 23)

29.1 Descrizione

Alcune applicazioni richiedono garanzie di prestazione rassicuranti, infatti possono richiedere un livello minimo di capacità di trasmissione e non funzionano bene quando la latenza è superiore a una certa soglia
Le esigenze di ogni flusso sono caratterizzati da quattro parametri primari: ampiezza di banda, ritardo, jitter (la deviazione standard del ritardo o nel tempo di arrivo di un pacchetto) e perdita
Questi parametri assieme determinano la QoS richiesta dal flusso

29.2 Ambiti d'uso

Usato attualmente per descrivere le esigenze che ogni servizio ha, ad esempio:
La posta elettronica necessita bassa rigidità di ampiezza di banda, ritardo e jitter, mentre la perdita richiede una rigidità media

La condivisione dei file richiede queste rigidità: un'ampiezza di banda elevata, ritardo e jitter non sono importanti ma con una perdita anch'essa media
L'audio, il video, la telefonia richiedono una rigidità del jitter elevata (ovvero jitter molto basso) perché anche una differenza di qualche millisecondo sarebbe riconoscibile, tutti con una rigidità di perdita bassa (poco importa se si perde qualche bit nella trasmissione, infatti può essere che non abbiano nemmeno un sistema di error control)

29.3 Pregi

1. Garanzia della Qualità del Servizio
   QoS consente di allocare risorse di rete a specifici tipi di traffico, garantendo che applicazioni critiche (es. VoIP, streaming video) ricevano priorità rispetto a traffico meno importante

2. Ottimizzazione dell'Utilizzo della Banda
   Distribuisce in modo efficiente la larghezza di banda disponibile tra i vari tipi di traffico, evitando che applicazioni non prioritarie congestionino la rete

3. Flessibilità
   QoS può essere configurata per adattarsi a diversi scenari di rete e politiche aziendali, offrendo un controllo granulare sul traffico

29.4 Difetti

1. Complessità di Implementazione
   La configurazione di QoS può essere complicata e richiedere conoscenze tecniche approfondite, specialmente in reti grandi o eterogenee

2. Costi Elevati
   L'implementazione di QoS può richiedere hardware specifico (es. router e switch avanzati) e software dedicato, aumentando i costi infrastrutturali

3. Manutenzione Continuativa
   QoS richiede monitoraggio e aggiornamenti costanti per garantire che le politiche rimangano efficaci in base ai cambiamenti delle condizioni di rete e delle esigenze aziendali

4. Impatto sulle Applicazioni Non Prioritarie
   Il traffico a bassa priorità potrebbe risentire negativamente di QoS, con prestazioni degradate a causa dell'allocazione preferenziale verso traffico critico

30 Choke packet (2016, 18, 19, 21, 22, 23, 24)

30.1 Descrizione

Il choke packet è una tecnica che avviene quando la capacità della linea o di qualche stazione si satura
In questa tecnica un host dimezza il suo data rate appena riceve un choke packet,

ovvero un pacchetto che si invia quando la rete è congestionata Per l'uscita dal choke ci si aspetta un periodo di tempo detto fading

30.2 Ambiti d'uso

Il suo ambito d'uso principale è al fine di "decongestionare" la rete, infatti con questa tecnica si dimezza il flusso dati in uscita e permette di elaborare al meglio i pacchetti già arrivati

30.3 Pregi

1. Riduzione della Congestione
   Aiuta a limitare la congestione della rete comunicando rapidamente al mittente di rallentare il flusso di dati, prevenendo ulteriori sovraccarichi

2. Semplicità del Meccanismo
   La logica alla base del choke packet è relativamente semplice da implementare: il nodo rileva il sovraccarico e invia un messaggio di feedback al mittente

3. Adattamento Dinamico del Traffico
   Permette al sistema di adattarsi in tempo reale alle condizioni della rete, mantenendo un flusso dati che evita il collasso

4. Minimizzazione della Perdita di Pacchetti
   Riducendo la velocità di invio prima che la rete raggiunga uno stato critico, si evita la perdita massiccia di pacchetti dovuta alla saturazione dei buffer

5. Compatibilità con Altri Meccanismi di Controllo
   Il choke packet può essere utilizzato insieme ad altri metodi di controllo della congestione, come il controllo basato sulla finestra (ad esempio TCP), per migliorare l'efficacia complessiva

30.4 Difetti

Il suo principale problema è "il problema dell'entrata"
Se si ha una sequenza di router A, B, C, D, E ed avviene la congestione della rete fra A ed E i router B, C, D inviano ad A un choke portando il suo data rate a 12,5%
Infatti, quando si riceve un choke, per un certo periodo di tempo detto fading alla rovescia (minore del fading) si ignorano degli eventuali altri choke in arrivo
Un altro problema è che una richiesta di choke può metterci troppo per decongestionare la rete, infatti si è progettata una variante choke hop-by-hop in cui ogni router incontrato subisce gli effetti del choke

31 Leaky bucket (2015)

31.1 Descrizione

Il leaky bucket è un tipo di algoritmo utilizzato per regolare il flusso di dati in una rete al fine di garantire una trasmissione controllata e costante

Si basa sull'analogia di un secchio che perde: i dati entrano nel secchio a una velocità arbitraria, ma ne escono a un ritmo costante
Se il secchio si riempie oltre la sua capacità, i dati in eccesso vengono scartati, garantendo così un controllo efficace del traffico
Questo meccanismo consente di evitare sovraccarichi della rete e di ridurre i burst di dati, ossia i picchi improvvisi di traffico
L'algoritmo è solitamente implementato dal mittente per regolare il proprio tasso di trasmissione e rispettare i vincoli imposti dalla rete

31.2 Ambiti d'uso

Il leaky bucket trova applicazione in diversi contesti, tra cui:

1. Reti di telecomunicazione, per controllare il traffico e garantire una trasmissione fluida
2. QoS (Quality of Service), per rispettare i contratti di traffico che limitano la banda o impongono requisiti di ritardo e jitter
3. Reti locali (LAN) e reti geografiche (WAN), per prevenire congestioni dovute a picchi di traffico generati da applicazioni o dispositivi
4. Applicazioni multimediali, come streaming video o chiamate VoIP, per assicurare una qualità stabile del servizio

31.3 Pregi

1. Controllo della congestione: l'algoritmo garantisce un flusso costante, riducendo il rischio di sovraccarichi nella rete
2. Semplicità di implementazione: il meccanismo è semplice da implementare sia a livello hardware che software
3. Prevedibilità del traffico: limita i burst e rende il traffico più prevedibile, facilitando la gestione della rete
4. Riduzione della perdita di pacchetti a valle: regolando il traffico in modo proattivo, riduce il rischio che i nodi successivi debbano scartare pacchetti

31.4 Difetti

1. Scarto dei dati in eccesso: se i burst superano la capacità del secchio, i dati vengono scartati, portando a possibili perdite di informazioni
2. Limitazione della flessibilità: il tasso costante imposto dal leaky bucket potrebbe non adattarsi bene a tutte le applicazioni, specialmente quelle che richiedono un traffico variabile
3. Possibili ritardi: in alcuni casi, il meccanismo può introdurre ritardi nella trasmissione dei dati se il secchio non si svuota abbastanza rapidamente
4. Overhead di configurazione: determinare la capacità ottimale del secchio e il tasso di perdita richiede una buona conoscenza delle esigenze della rete e delle applicazioni

32 Token bucket (2016, 18, 19, 20, 21, 24)

32.1 Descrizione

Il leaky bucket è un tipo di algoritmo utilizzato per regolare il flusso di dati in una rete al fine di garantire una trasmissione controllata e costante
Si basa sull'analogia di un secchio che ogni tanto perde, infatti il suo funzionamento è la generazione, ogni certo intervallo di tempo, un token
I pacchetti in arrivo possono uscire solo se "bruciamo" un token disponibile

32.2 Ambiti d'uso

Come detto prima è un sistema necessario per garantire il flusso di dati ed è determinante in alcuni ambiti per il rispetto dei parametri del QoS
Infatti, se il traffico per un certo periodo è lento ma poi c'è un burst (aumento) si riesce a gestire meglio consumando i token che si sono accumulati

32.3 Pregi

1. Flessibilità per traffico:
   il token bucket consente di accumulare token, permettendo al traffico bursty (picchi) di essere trasmesso rapidamente, purché ci siano token sufficienti

2. Controllo della banda media:
   garantisce che il tasso medio di trasmissione rimanga entro i limiti impostati, evitando congestioni di rete

3. Adattabilità:
   è adatto sia a traffico regolare che irregolare, rendendolo versatile per molte applicazioni, come streaming multimediale e servizi VoIP

4. Supporto per QoS:
   consente di rispettare i vincoli di qualità del servizio (Quality of Service), garantendo priorità o limitazioni al traffico

5. Configurabilità:
   i parametri (capacità del secchio e tasso di accumulo dei token) possono essere facilmente regolati per adattarsi a esigenze specifiche

32.4 Difetti

1. Ritardi possibili:
   in caso di esaurimento dei token, i pacchetti devono attendere che i token si rigenerino, introducendo ritardi nel traffico

2. Gestione di traffico costante meno rigida:
   a differenza del leaky bucket, che forza un tasso di trasmissione costante, il token bucket consente picchi che potrebbero causare congestione se non ben gestiti

3. Possibili perdite di pacchetti:
   se i burst superano la capacità del secchio e non ci sono token disponibili, i pacchetti in eccesso vengono scartati, causando perdita di dati

4. Necessità di monitoraggio:
   Per garantire prestazioni ottimali, il meccanismo richiede un monitoraggio continuo della rete e una manutenzione periodica dei parametri configurati

33 CIDR (2014, 15, 16, 17, 18, 19, 22)

33.1 Descrizione

Il CIDR (Classless Inter-Domain Routing) è una tecnica di indirizzamento IP introdotta per superare le limitazioni delle vecchie classi di rete (Class A, B, C)
Permette di utilizzare blocchi di indirizzi di lunghezza variabile, invece dei blocchi fissi imposti dalle classi tradizionali (classless)
Con il CIDR, gli indirizzi IP sono rappresentati in forma di prefisso, ad esempio '192.168.0.0/24', dove il numero dopo la barra indica la lunghezza del prefisso di rete. Questo permette una suddivisione più granulare o un'aggregazione, ottimizzando l'uso degli indirizzi IP.

33.2 Ambiti d'uso

Principalmente utilizzato per l'ottimizzazione delle tabelle di routing (reti con prefissi comuni possono essere aggregate) e per la gestione degli indirizzi IP (evita sprechi dovuti ai blocchi fissi delle classi tradizionali)
Quando più classi di indirizzi devono essere indirizzate allo stesso router, possono essere combinate in un'unica voce di routing se condividono un prefisso comune
Tuttavia, in caso di sovrapposizione, l'entrata con il prefisso di rete più lungo (più specifica) ha la priorità, secondo la regola del Longest Prefix Match

33.3 Pregi

1. Migliore efficienza nell'uso degli indirizzi IP: Permette di ridurre il problema dello spreco di indirizzi grazie alla flessibilità della lunghezza del prefisso

2. Riduzione delle dimensioni delle tabelle di routing:
   l'aggregazione di reti consente di semplificare e ottimizzare le tabelle di routing

3. Facilità di gestione del subnetting:
   consente di creare sottoreti adattabili alle esigenze di organizzazioni di diverse dimensioni.

33.4 Difetti

1. Complessità di configurazione:
   la flessibilità del CIDR richiede una maggiore attenzione nella pianificazione e configurazione delle reti

2. Necessità di hardware aggiornato:
   i router più vecchi potrebbero non supportare pienamente il CIDR, richiedendo aggiornamenti o sostituzioni

3. Maggiore difficoltà nella risoluzione dei problemi:
   la granularità dei prefissi può complicare l'analisi e la diagnosi di problemi di rete

4. Dipendenza da un'adeguata progettazione del routing:
   una configurazione errata può portare a inefficienze o a conflitti nel routing.