Reti di Calcolatori

Matteo Mazzaretto

2024

ATTENZIONE: questo file è una rivisitazione personale delle domande chieste negli anni allo scritto di Reti di Calcolatori
Sono state aggiunte parecchie domande che secondo me può chiedere (sono quelle senza date fra parentesi), però non assicuro di dare tutte le risposte di un programma così ampio
Infatti, ad esempio, al 2 appello 2024/2025 ha chiesto il CSMA p-persistente, del quale non c'è la descrizione completa in questo file

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
   L'estensione di un cavo in fibra può avvenire attraverso: 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 soprattutto sulle lunghe distanze

2 Satelliti (2015, 16, 18, 19, 20 21, 23, 24, 25)

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 distanti dalla superficie terrestre, 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
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)

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 che, una volta finito il carburante necessario alla loro ricollocazione, vengono allontanati. Quando un satellite, attivo o meno, si scontra con un altro corpo, esso "esplode" in una miriade di frammenti, che a loro volta costituiscono un rischio per gli altri satelliti attivi. Per questo, i frammenti devono essere tracciati e monitorati, in modo da evitare la possibilità di eventuali effetti 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 sostituite 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 trasmessa ogni secondo e permettono di calcolare la larghezza di banda
Bit rate: è il numero di bit che si possono trasmettere contemporaneamente con ogni impulso, è uguale al baudrate*log2(numero simboli)
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, Quadrature Amplitude Modulation (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 simbolo) 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 sé stante e c'è controllo costante sulla qualità della trasmissione → ogni canale può essere rallentato/accelerato indipendentemente
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 FDM Multiplexing

8.1 Descrizione

Tecnica di multiplazione per trasmettere simultaneamente più segnali su un unico canale, separandoli in base alla frequenza
Ogni banda viene utilizzata per trasmettere un segnale indipendente

8.2 Ambiti d'uso

TV analogica
Radio (ogni stazione trasmette su una frequenza specifica)
Comunicazioni mobili e satellitari
Sistemi di trasmissione cablati
Reti ottiche

8.3 Pregi

Efficienza, trasmissione simultanea, bassa complessità hardware e basse latenze

8.4 Difetti

Guard Band: richiede porzione di frequenza inutilizzata per evitare sovrapposizioni, riducendo efficienza dello spettro
Scalabilità limitata
Sensibilità alle perdite di segnale

9 TDM Multiplexing (2016)

9.1 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

9.2 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)

9.3 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)

9.4 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

10 Handoff (2023)

10.1 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) verifica attraverso le celle lo stato del segnale ricevuto dal dispositivo ed esso viene assegnato alla cella con potenza più alta
Si presenta in due tipologie:

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

10.2 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

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

11.1 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, mentre se diminuisce, uno 0
Questa rappresentazione descrive l'andamento del segnale, ma non ne conserva la forma precisa

11.2 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

11.3 Pregi

Efficienza di compressione, basso consumo energetico e velocità di elaborazione

11.4 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

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

12.1 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

12.2 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

12.3 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

12.4 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)

13 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

13.1 Byte stuffing

13.1.1 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

13.1.2 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)

13.1.3 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

13.1.4 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 messaggio 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

13.2 Bit stuffing

13.2.1 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

13.2.2 Ambiti d'uso

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

13.2.3 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

13.2.4 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

14 Error control

14.1 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

14.2 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

14.3 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

14.4 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

15 Stop and wait

15.1 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

15.2 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

15.3 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

15.4 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

16 Go back n (2015, 20, 24)

16.1 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

16.2 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

16.3 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

16.4 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

17 Selective Repeat (2022)

17.1 Descrizione

Selective Repeat è protocollo di trasmissione basato sulle Sliding Windows, progettato per gestire in modo efficiente la comunicazione tra mittente e ricevente soprattutto 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), prevede la presenza di un buffer per la memorizzazione dei pacchetti mancanti dalla parte del ricevitore
In questo modo è possibile calcolare quali pacchetti manchino (grazie ai numeri di sequenza) e chiedere al mittente di rispedirli singolarmente
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

17.2 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

17.3 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

17.4 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

18 HDLC

18.1 Descrizione

Protocollo concreto ideato inizialmente dall'IBM
L'HDLC (High-Level Data Link Control) è un protocollo standard è un protocollo del livello data link
Si basa su una struttura a frame (trama) e supporta comunicazioni punto-punto e multipunto
Il protocollo si occupa principalmente di:
Organizzazione dei dati
Affidabilità: fornisce meccanismi di rilevamento e correzione degli errori
Controllo del flusso: evita la congestione gestendo il ritmo della trasmissione

18.2 Ambiti d'uso

Attualmente viene usato per modem/fax, reti di vario tipo (come reti LAN e WAN) e molti circuiti bancari

18.3 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
Efficienza nella trasmissione continua:
HDLC utilizza frame strutturati con overhead minimo, ottimizzando la trasmissione di dati su collegamenti con capacità elevate

18.4 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

19 PPP

19.1 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 del flusso 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

19.2 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

19.3 Pregi

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

19.4 Difetti

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

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

20.1 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), che lo occuperanno in momenti diversi
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 inutilizzabili)
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)

20.2 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
Sistemi di comunicazione a bassa velocità:
ideale per applicazioni a basso traffico e ridotta necessità di coordinamento

20.3 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

20.4 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

21 CSMA (2017, 18, 20)

21.1 Descrizione

CSMA (Carrier Sense Multiple Access) 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, si controlla che il canale sia libero
Se così fosse, viene effettuato un controllo l'istante successivo finché non si ha la possibilità di trasmettere
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

21.2 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

21.3 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

21.4 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

22 CSMA non persistent (2022)

22.1 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%

22.2 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

22.3 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

22.4 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

23 Protocolli a contesa limitata: adaptive tree walk protocol (2015, 18, 24, 25)

23.1 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 contesa 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 dall'alto al basso 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

23.2 Ambiti d'uso

Sono protocolli utilizzati in ambiti come reti Ethernet, reti wireless, 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

23.3 Pregi

1. C'è una notevole riduzione delle collisioni in cui i protocolli a contesa limitata riducono significativamente le collisioni rispetto ai protocolli randomici, 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 livello 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

23.4 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, oltre al continuo aggiornamento

24 Stazione nascosta (2019, 20, 24)

24.1 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

24.2 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

24.3 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

25 802.3

25.1 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" oppure ad "albero"
Per indicare i vari tipi di cavi si utilizza una notazione particolare, del tipo XbaseY, dove X indica 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

25.2 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 industriali, per le reti di provider di servizi e per le reti domestiche

25.3 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

25.4 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

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

26.1 Descrizione

La codifica Manchester è una tecnica di modulazione 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)

26.2 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

26.3 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

26.4 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

27 Flooding (2015, 16, 18, 20, 23, 25)

27.1 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 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

27.2 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 (indipendentemente dall'efficienza complessiva)

27.3 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

27.4 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

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

28.1 Descrizione

Il Distance Vector Routing è un altro algoritmo di routing in cui gni 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

28.2 Ambiti d'uso

1. Reti locali (LAN) e piccole reti aziendali: adatto in ambienti dove la topologia della rete è stabile e le risorse sono limitate.

2. Reti non critiche: in contesti dove il traffico e la complessità sono bassi, il Distance Vector può ancora essere una soluzione pratica grazie alla sua semplicità

28.3 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

28.4 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
In altre parole: si verifica quando un nodo diventa irraggiungibile e gli altri router continuano ad aggiornarsi a vicenda con informazioni errate incrementando progressivamente la distanza

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

29.1 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

29.2 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

29.3 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

29.4 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

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

30.1 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

30.2 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)

30.3 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

30.4 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

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

31.1 Descrizione

Un choke packet funziona similmente al sistema a crediti di un bus: quando un router rileva una congestione nel flusso di trasmissione, si occupa di spedire ai vari mittenti un pacchetto di congestione, che obbliga un ritmo di spedizione

moderato
Dopo un po' il flusso tornerà al suo ritmo originale autonomamente (fading)

31.2 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

31.3 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

31.4 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

32 Leaky bucket (2015, 25)

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 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 traffico controllato
Questo meccanismo consente di evitare sovraccarichi della rete e di ridurre i burst di dati, ossia i picchi improvvisi di traffico
I due modi per implementare correttamente un algoritmo leaky bucket sono:

- Sul mittente: viene regolata la frequenza di spedizione dei pacchetti in modo da non superare la soglia di tolleranza della rete
- Sui nodi intermedi (router): il buffer di ricezione (secchio) è posto sul ricevente (router), e quando si riempie completamente (acqua) ciò che non può essere salvato viene perso

32.2 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 lo streaming video, per assicurare una qualità stabile del servizio

32.3 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

32.4 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

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

33.1 Descrizione

Il token 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 ogni certo intervallo di tempo genera un token
I pacchetti in arrivo possono uscire solo se "bruciano" un token disponibile

33.2 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

33.3 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 multimediali

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

33.4 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

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

34.1 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.

34.2 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

34.3 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.

34.4 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.

35 IPv4 (2024)

35.1 Descrizione

IPv4 (Internet Protocol versione 4) è il protocollo che definisce il formato del datagramma IP e il meccanismo per il trasferimento di dati tra dispositivi su reti basate su IP
L'intestazione (header) di un datagramma IPv4 è suddivisa in due parti principali:

- Parte fissa: È lunga 20 byte e include campi essenziali
- Parte variabile: può contenere aggiunte opzionali, come timestamp, sicurezza, o registrazione del percorso, pensate per eventuali funzionalità future

IPv4 è stato progettato con un'architettura robusta per gestire le comunicazioni su reti eterogenee, garantendo adattabilità

35.2 Ambiti d'uso

IPv4 è il protocollo fondamentale per l'invio di pacchetti nello strato di rete (network layer) e rappresenta la base delle comunicazioni su Internet
Alcuni ambiti di utilizzo:

- Trasporto dati su Internet:
  è il protocollo principale per il trasferimento di pacchetti tra dispositivi collegati alla rete
- Reti locali (LAN) e geografiche (WAN):
  IPv4 è utilizzato in contesti di rete di diversa scala, dal piccolo ufficio a reti globali
- Interconnessione di reti eterogenee:
  permette la comunicazione tra dispositivi con architetture diverse, garantendo universalità e flessibilità

- Gestione del traffico dinamico:
  IPv4 utilizza tecniche come il routing dinamico e il flooding per garantire la consegna anche in condizioni di rete non ottimali (es. congestione o attacchi)

IPv4 non implementa meccanismi di controllo degli errori per garantire alte prestazioni; questo compito è demandato ai livelli superiori

35.3 Pregi

- Struttura gerarchica degli indirizzi:
  gli indirizzi IPv4 vengono assegnati attraverso un sistema gerarchico gestito da autorità centralizzate garantendo efficienza nella distribuzione e nel routing

- Compatibilità universale:
  IPv4 è supportato da praticamente tutti i dispositivi connessi alla rete, rendendolo il protocollo più utilizzato per le comunicazioni IP

- Semplicità e robustezza:
  è progettato per essere operativo in contesti di rete dinamici, garantendo resilienza contro interruzioni o perdite di pacchetti

- Cachability e instradamento ottimizzato:
  grazie alla struttura gerarchica, il routing può essere ottimizzato attraverso subnetting e aggregazione degli indirizzi

35.4 Difetti

Nonostante i suoi pregi, IPv4 presenta alcuni limiti intrinseci:

- Limitazione degli indirizzi disponibili:
  gli indirizzi IPv4 sono a 32 bit, il che consente circa 4,3 miliardi di indirizzi univoci
  Tuttavia, lo spazio degli indirizzi è ormai quasi esaurito a causa della crescita esponenziale dei dispositivi connessi

- Frammentazione dei pacchetti:
  in reti con diverse dimensioni di MTU (Maximum Transmission Unit), i pacchetti devono essere frammentati, aumentando l'overhead e la complessità

- Vulnerabilità alla sicurezza:
  IPv4 non include nativamente meccanismi di sicurezza, come l'autenticazione o la crittografia, che devono essere implementati tramite protocolli aggiuntivi

- Limite del TTL:
  il campo TTL consente al datagramma un massimo di 255 salti
  Anche se i router possono rigenerare i datagrammi, questo valore rappresenta una limitazione nei casi estremi

36 NAT (Network Address Translation) (2015, 18, 19, 22, 23)

36.1 Descrizione

L'idea del protocollo NAT è simulare un'intera sottorete usando un solo indirizzo IP: gli indirizzi IP di una rete sono quelli, ma sono riutilizzabili tra sottoreti diverse (e anche da una sottorete "maggiore") perché non sono visibili al di fuori della loro sottorete di appartenenza
Internamente:
la rete funziona con degli indirizzi IP interni, che sono invisibili all'esterno
Esternamente:
la rete appare come un singolo indirizzo IP
Ogni pacchetto che esce dalla rete perde il suo indirizzo IP e viene sostituito dall'unico indirizzo NAT
Certi indirizzi sono riservati per le reti interne ai NAT e non possono essere usati come normali indirizzi Internet

- 10.0.0.0 (rete da 2^{24} hosts)
- 172.16.0.0 (rete da 2^{20} hosts)
- 192.168.0.0 (rete da 2^{16} hosts)

36.2 Ambiti d'uso

Il NAT è largamente utilizzato in diversi contesti, tra cui:

1. Reti domestiche e aziendali:
   permette a più dispositivi di connettersi a Internet utilizzando un unico indirizzo IP pubblico, riducendo la necessità di acquistare più indirizzi IP
2. Conservazione degli indirizzi IPv4:
   a causa della scarsità degli indirizzi IPv4 pubblici, il NAT è una soluzione pratica per estendere l'utilizzo di un singolo indirizzo IP su più dispositivi
3. Sicurezza di rete:
   nasconde gli indirizzi IP interni, rendendo più difficile per un attaccante esterno identificare e attaccare i dispositivi interni

36.3 Pregi

Il NAT presenta numerosi vantaggi, tra cui:

1. Risparmio di indirizzi IPv4:
   consente l'uso di un singolo indirizzo IP pubblico per una rete di molti dispositivi, riducendo il consumo di indirizzi IPv4
2. Maggiore sicurezza:
   gli indirizzi IP privati della rete interna non sono visibili all'esterno, il che aumenta la sicurezza contro attacchi diretti

3. Facilità di configurazione:
   il NAT può essere implementato facilmente su router e dispositivi di rete senza modificare i dispositivi della rete interna

4. Flessibilità:
   permette di cambiare gli indirizzi interni senza influire sulle comunicazioni esterne

5. Supporto per il port forwarding:
   consente di configurare regole per inoltrare il traffico specifico verso determinati dispositivi interni

36.4 Difetti

1. Difficoltà di tracciamento:
   il NAT modifica gli indirizzi IP nei pacchetti, rendendo più complessa l'analisi del traffico e il tracciamento delle connessioni

2. Performance:
   nei router con risorse limitate, il processo di traduzione degli indirizzi può introdurre un leggero overhead e rallentare le connessioni

3. Incompatibilità con IPv6 puro:
   con l'adozione di IPv6, il NAT diventa meno rilevante poiché IPv6 offre un numero sufficiente di indirizzi unici per ogni dispositivo

37 ARP (Address Resolution Protocol) (2014, 17, 18, 19, 20, 22, 23, 24, 25)

37.1 Descrizione

L'Address Resolution Protocol (ARP) è un protocollo appartenente al livello di rete (network layer) che consente di trovare la corrispondenza tra un indirizzo IP e un indirizzo MAC (Media Access Control) necessario per la comunicazione all'interno di una rete locale (LAN)
Il suo funzionamento può essere riassunto come segue:

- Ogni macchina all'interno della rete mantiene una tabella ARP, che contiene le corrispondenze tra indirizzi IP e indirizzi MAC conosciuti.
- Quando un dispositivo deve inviare un pacchetto a un altro dispositivo della rete e conosce solo l'indirizzo IP di destinazione, genera un messaggio ARP in broadcast (richiesta ARP).
- La macchina destinataria, riconoscendo il proprio indirizzo IP nella richiesta, risponde con un messaggio ARP di risposta (unicast) contenente il proprio indirizzo MAC.
- La corrispondenza IP-MAC viene salvata nella cache ARP del dispositivo richiedente per ottimizzare le comunicazioni future.

Ogni pacchetto ARP include in piggyback (ossia come dato aggiuntivo) la corrispondenza tra indirizzo IP e indirizzo MAC, permettendo così il continuo aggiornamento della tabella ARP

37.2 Ambiti d'uso

Il protocollo ARP è fondamentale per la comunicazione in reti IPv4 locali e viene utilizzato in diverse situazioni, tra cui:

1. Trasmissione in reti Ethernet:
   consente a un dispositivo di determinare l'indirizzo MAC del destinatario per poter incapsulare correttamente il pacchetto a livello data-link

2. Routing locale:
   è indispensabile quando un router deve inviare pacchetti a un dispositivo nella rete locale

3. Comunicazioni client-server:
   viene utilizzato ogni volta che un client locale deve comunicare con un server nella stessa rete, come in reti domestiche o aziendali

37.3 Pregi

ARP offre diversi vantaggi nel contesto delle reti:

1. Semplicità:
   il protocollo ARP è semplice e diretto, progettato per svolgere una funzione specifica: risolvere gli indirizzi IP in indirizzi MAC

2. Trasparenza:
   il processo di risoluzione degli indirizzi avviene automaticamente e in modo trasparente per l'utente finale e le applicazioni

3. Efficienza:
   una volta risolta la corrispondenza, i risultati vengono memorizzati nella cache ARP per ridurre la latenza e migliorare le prestazioni in comunicazioni successive

4. Compatibilità universale:
   ARP è supportato dalla maggior parte delle reti Ethernet e IPv4, garantendo interoperabilità tra dispositivi di rete

37.4 Difetti

Nonostante la sua utilità, il protocollo ARP presenta alcune limitazioni e vulnerabilità:

1. Dipendenza da IPv4:
   ARP è progettato per IPv4, e quindi non è utilizzabile in reti IPv6

2. Possibili sovraccarichi di rete:
   in reti molto grandi o con dispositivi instabili, un numero elevato di richieste ARP può causare congestione, degradando le prestazioni della rete

38 ICMP (2014, 15, 22)

38.1 Descrizione

Internet Control Message Protocol (ICMP) è un protocollo di rete del livello 3 (network layer) progettato per trasmettere messaggi di controllo e segnalazione tra dispositivi in una rete IP
ICMP non è utilizzato per il trasferimento di dati applicativi, ma per comunicare errori, condizioni di rete o informazioni diagnostiche
Alcune delle sue funzioni principali includono

- Segnalare errori, come l'inaccessibilità di una destinazione o il superamento del TTL (Time to Live)
- Gestione del controllo del traffico, ad esempio avvisando un mittente di ridurre la velocità di trasmissione

I messaggi ICMP vengono trasportati all'interno di datagrammi IP, ma non garantiscono la consegna: ICMP si basa sul protocollo IP, che è di tipo best-effort (il sistema fa del suo meglio per consegnare i dati, ma non garantisce alcuna affidabilità, ordine o tempi di consegna precisi)

38.2 Ambiti d'uso

ICMP è utilizzato in vari contesti per il controllo e la gestione delle reti:

1. Diagnostica della rete
2. Gestione degli errori:
   (a) Notifica di destinazione irraggiungibile (Destination Unreachable) quando un pacchetto non può essere consegnato
   (b) Avviso di superamento del TTL (Time Exceeded) quando un pacchetto supera il numero massimo di salti consentiti
3. Ottimizzazione della rete:
   ICMP può suggerire al mittente di ridurre la velocità di trasmissione o instradare i pacchetti su percorsi alternativi
4. Supporto al routing dinamico:
   ICMP viene utilizzato dai router per segnalare problemi o aggiornamenti di stato ai sistemi di gestione della rete

38.3 Pregi

ICMP offre numerosi vantaggi per il monitoraggio e la gestione delle reti:

1. Leggerezza:
   ICMP è un protocollo leggero con overhead minimo, rendendolo ideale per notifiche e diagnosi rapide
2. Strumento diagnostico essenziale:
   fornisce informazioni cruciali sulla connettività e le prestazioni di rete, indispensabili per i tecnici e gli amministratori di rete

3. Universalità:
   essendo parte integrante del protocollo IP, ICMP è supportato da quasi tutti i dispositivi di rete

38.4 Difetti

Nonostante la sua utilità, ICMP presenta alcune limitazioni e vulnerabilità:

1. Nessuna garanzia di consegna: ICMP si basa sul protocollo IP, che è un protocollo best-effort, quindi i messaggi ICMP possono andare persi
2. Vulnerabilità alla sicurezza
3. Blocco in alcune reti:
   per motivi di sicurezza, molti firewall e dispositivi di rete bloccano i messaggi ICMP, riducendo la loro utilità per diagnosi o gestione della rete

39 IPv6 (2016, 20, 23)

39.1 Descrizione

IPv6 (Internet Protocol versione 6) è la nuova versione del protocollo IP progettata per superare i limiti di IPv4, in particolare il problema dell'esaurimento degli indirizzi
Le principali caratteristiche di IPv6 sono:

1. Indirizzi più grandi:
   gli indirizzi IPv6 sono lunghi 16 byte rispetto ai 4 byte di IPv4
   Questo consente di avere un numero quasi illimitato di indirizzi, sufficiente per soddisfare le esigenze future di Internet e l'espansione dell'Internet of Things (IoT)
2. Eliminazione del checksum:
   IPv6 non include un campo checksum nell'header per velocizzare l'elaborazione dei pacchetti
3. Struttura dell'header semplificata:
   l'header di IPv6 è più semplice e uniforme rispetto a quello di IPv4, riducendo il carico sui router e migliorando l'efficienza del routing
4. Supporto nativo per QoS:
   IPv6 include un campo chiamato Flow Label, progettato per facilitare la gestione della qualità del servizio (QoS) per applicazioni in tempo reale, come voce e video

39.2 Ambiti d'uso

IPv6 è progettato per essere il protocollo fondamentale di Internet nel futuro e trova applicazione nei seguenti contesti:

1. Reti moderne: viene utilizzato in infrastrutture che richiedono scalabilità, sicurezza e gestione avanzata della rete, come i data center e le reti aziendali

2. Trasmissioni multicast: IPv6 supporta nativamente la trasmissione multicast, ottimizzando la distribuzione di dati a più destinatari, ad esempio per lo streaming video o l'aggiornamento simultaneo di dispositivi

3. Reti con mobilità: IPv6 semplifica la gestione degli indirizzi in scenari di mobilità, come nei dispositivi mobili, supportando handover efficienti e connessioni stabili

39.3 Pregi

IPv6 offre numerosi vantaggi rispetto a IPv4:

1. Indirizzi illimitati: Con i suoi 128 bit, IPv6 consente la creazione di circa 3.4×10^{38} indirizzi univoci, risolvendo il problema dell'esaurimento degli indirizzi IP

2. Efficienza nel routing: L'header semplificato e l'uso di tecniche come il prefix aggregation migliorano la velocità di instradamento e riducono il carico sui router

3. Supporto alla mobilità: IPv6 include funzionalità avanzate per supportare dispositivi mobili, migliorando la gestione delle connessioni durante gli spostamenti

39.4 Difetti

IPv6 presenta anche alcune limitazioni e sfide:

1. Compatibilità limitata con IPv4:
   IPv6 non è direttamente compatibile con IPv4, richiedendo l'uso di meccanismi di transizione

2. Adozione lenta:
   nonostante i vantaggi, l'adozione di IPv6 è stata lenta a causa della necessità di aggiornare le infrastrutture, i dispositivi e il software

3. Overhead maggiore:
   l'header di IPv6 è più grande di quello di IPv4 (40 byte contro 20 byte), il che può aumentare leggermente l'overhead in alcune reti a bassa capacità

40 UDP (2014, 16, 17, 18, 20, 22, 23, 24, 25)

40.1 Descrizione

Il User Datagram Protocol (UDP) è un protocollo di trasporto
UDP è progettato per la trasmissione rapida di dati con un overhead minimo, adottando un approccio best-effort
A differenza del TCP, non fornisce meccanismi di controllo della connessione, ritrasmissione o verifica dell'ordine dei pacchetti
Le principali caratteristiche di UDP includono:

1. Nessuna connessione:
   UDP è un protocollo connectionless, il che significa che non stabilisce una connessione prima dell'invio dei dati

2. Struttura semplice:
   il segmento UDP contiene solo informazioni essenziali: porta di origine, porta di destinazione, lunghezza del segmento e checksum

3. Velocità e leggerezza:
   poiché non implementa controlli di errore o ritrasmissione, UDP è parecchio veloce

4. Multiplexing:
   UDP consente la comunicazione tra più applicazioni attraverso l'uso delle porte

5. Affidabilità delegata:
   qualsiasi controllo di errore o meccanismo di affidabilità deve essere implementato dall'applicazione che utilizza UDP

40.2 Ambiti d'uso

UDP viene utilizzato in diversi scenari, principalmente in applicazioni che richiedono bassa latenza, velocità o trasmissione continua di dati:

1. Streaming audio e video:
   per garantire una riproduzione fluida, è preferibile perdere qualche pacchetto piuttosto che ritardare la trasmissione

2. Trasmissioni multicast e broadcast:
   UDP è utilizzato per inviare dati a più destinatari contemporaneamente

40.3 Pregi

UDP presenta numerosi vantaggi per applicazioni specifiche:

1. Bassa latenza:
   l'assenza di meccanismi di controllo della connessione rende UDP ideale per applicazioni in tempo reale

2. Efficienza:
   il ridotto overhead del protocollo garantisce una trasmissione dei dati più veloce rispetto a TCP

3. Semplicità:
   grazie alla sua struttura minimale, UDP è facile da implementare e consuma meno risorse di sistema

4. Supporto multicast e broadcast:
   UDP consente trasmissioni simultanee a più destinatari, a differenza di TCP

5. Adatto per applicazioni specifiche:
   è perfetto per scenari in cui la perdita di pacchetti non compromette l'esperienza complessiva, come lo streaming

40.4 Difetti

Nonostante i suoi vantaggi, UDP ha delle limitazioni:

1. Mancanza di affidabilità:
   UDP non garantisce la consegna dei pacchetti, che possono essere persi o arrivare fuori ordine
2. Assenza di controllo di errore:
   il checksum di UDP rileva solo errori nei dati, ma non offre alcuna correzione o ritrasmissione automatica
3. Non adatto per dati critici:
   applicazioni che richiedono integrità e affidabilità dei dati (come il trasferimento di file) devono utilizzare protocolli come TCP

41 TCP, Trasmission Control Protocol (2016)

41.1 Descrizione

TCP è uno dei principali protocolli di rete su Internet
È un protocollo di comunicazione orientato alla connessione, che si basa sul 3-way handshake
Full-duplex e point-to-point, è un protocollo reliable (affidabile) e il checksum è solo frutto di semplici somme e non codici di error detection complessi
Oltretutto ha integrati il controllo del flusso, il controllo della congestione e la ritrasmissione automatica

41.2 Ambiti d'uso

TCP viene utilizzato in tutti quei contesti dove è essenziale avere una trasmissione dati affidabile, anche a costo di una maggiore latenza
Alcuni esempi includono:

1. Navigazione web: protocollo HTTP e HTTPS
2. Email: protocolli come SMTP, IMAP e POP3
3. Trasferimenti di file: FTP (File Transfer Protocol)
4. Applicazioni di gestione remota: SSH e Telnet
5. Sistemi di database: comunicazioni tra client e server di database

41.3 Pregi

I suoi pregi sono anche le sue principali caratteristiche:

1. Affidabile
2. Permette di controllare la congestione
3. Supporto universale: ampiamente supportato su tutti i sistemi operativi e dispositivi connessi a Internet
4. Versatilità: adatto a una vasta gamma di applicazioni, dalle comunicazioni interattive (come SSH) ai trasferimenti di file

41.4 Difetti

1. Maggiore latenza: l'affidabilità e il controllo di flusso aumentano la latenza rispetto ai protocolli più semplici, come UDP
2. Overhead elevato: le informazioni aggiuntive necessarie per la gestione di sequenze, ritrasmissioni e controllo della congestione aumentano l'overhead
3. Non adatto a trasmissioni in tempo reale: per applicazioni come lo streaming video o i giochi online, l'elevata latenza e la gestione dell'ordine dei pacchetti possono essere controproducenti
4. Gestione della connessione: essendo orientato alla connessione, richiede una fase di handshake iniziale, che può essere onerosa in applicazioni con molte connessioni brevi
5. Difficoltà in reti instabili: in reti molto instabili, il numero di ritrasmissioni può crescere significativamente, rallentando ulteriormente la comunicazione

42 BGP: Border Gateway Protocol

42.1 Descrizione

Il BGP è un protocollo che stabilisce le regole per l'instradamento dei dati tra reti autonome, definendo come devono essere condivise e applicate le informazioni sulle rotte quando il traffico passa da una rete all'altra

42.2 Ambiti d'uso

Internet: gestisce l'instradamento globale del traffico tra provider di servizi Internet (ISP) e grandi reti aziendali
Data center: ottimizza la comunicazione tra reti interne ed esterne nei grandi data center
Grandi aziende: permette di gestire infrastrutture di rete distribuite su scala globale con resilienza garantita

42.3 Pregi

Scalabilità: è in grado di gestire milioni di rotte, rendendolo adatto alle reti più grandi
Flessibilità: permette un controllo dettagliato del routing tramite policy personalizzate
Resilienza: garantisce continuità della connessione grazie al supporto per ridondanza e failover
Standard globale: è il protocollo di routing principale di Internet e universalmente supportato

42.4 Difetti

Complessità: la configurazione e gestione di BGP richiedono competenze tecniche avanzate
Sicurezza debole: non dispone di meccanismi di sicurezza intrinseci ed è vulnerabile ad attacchi
Errori umani: configurazioni errate possono propagarsi su larga scala, causando problemi globali
Dipendenza da policy: le decisioni di instradamento non sempre garantiscono il percorso più rapido o ottimale

43 Attacchi ciphertext only (2019, 20)

Uno dei più comuni esempi di questo tipo di attacco è l'attacco brute-force

43.1 Descrizione

Gli attacchi ciphertext-only sono un tipo di attacco crittografico in cui l'attaccante dispone solo di uno o più testi cifrati, senza alcuna conoscenza aggiuntiva sul testo in chiaro o sulla chiave utilizzata per cifrarli
L'obiettivo è dedurre il contenuto dei messaggi (testo in chiaro) o, idealmente, la chiave crittografica, sfruttando le caratteristiche del testo cifrato e potenziali vulnerabilità nell'algoritmo di cifratura

43.2 Ambiti d'uso

Attualmente non sono molto utilizzabili in contesti molto più moderni, infatti vengono usati per cifrari deboli o obsoleti come il cifrario di Cesare (o potenzialmente qualsiasi sostituzione monoalfabetica o un DES a chiave singola),
Però è utile quando ad esempio si intercettano delle comunicazioni oppure per analizzare vecchi documenti cifrati
Infine, è usato come un parametro di criptoanalisi per un nuovo algoritmo

43.3 Pregi

1) non richiede l'accesso al plaintext (testo in chiaro) o alla chiave
2) applicabile in condizioni realistiche

43.4 Difetti

1) come menzionato prima, quasi inutile su algoritmi moderni, i quali non rendono noti pattern significativi nel cyphertext
2) dipendente da schemi ripetitivi
3) alta complessità computazionale

44 Sostituzione monoalfabetica (2019, 24)

44.1 Descrizione

Tipo di crittografia molto debole nell'epoca moderna
Consiste nel sostituire ogni lettera con un'altra cosicché il testo sia pressoché indecifrabile (se letto senza opportuni algoritmi di cifratura)
Viene considerato un algoritmo che è parte del principio di Kerchoff, ovvero che "Il design di un sistema non dovrebbe richiedere segretezza e compromettere il sistema non dovrebbe dare problemi ai corrispondenti"
Infatti il suo principio ha dato vita all'idea che l'algoritmo di encrypting deve essere pubblico (tutti sanno che ogni lettera è sostituita con un'altra) ma le chiavi sono segrete (nessuno sa quale lettere sono state sostituite)

44.2 Ambiti d'uso

Il suo uso è nato nel passato, grazie all'uso di questa tecnica in documenti militari e diplomatici
L'esempio più famoso è il cifrario di Cesare, il quale consiste nel scambiare ogni lettera con quella 3 lettere davanti nell'alfabeto (esempio la A con la D, la B con la E e così via)
Attualmente viene usato anche come principio d'insegnamento della crittografia e per sfide educative ma non trova quasi mai contesti moderni nell'ambito di internet in cui esso sia realmente utilizzato e sicuro, infatti ormai viene usato più per comunicazioni informali o non critiche

44.3 Pregi

Il suo grosso pregio è che ci possono essere tantissime chiavi, ovvero 26!-1 chiavi diverse e, con la brute-force, per tentare tutte le combinazioni ci vorrebbe troppo tempo
Inoltre ha dalla sua la facilità d'implementazione e decifratura, comodo se si vuole dare un minimo di sicurezza, ha una bassa dipendenza da risorse tecnologiche ed è ottimo contro i "non esperti"
Inoltre un errore nella cifratura o decifratura di un singolo carattere non compromette gli altri caratteri del messaggio, infatti ogni lettera è cifrata in modo indipendente, a differenza di cifrari più avanzati che collegano i blocchi.

44.4 Difetti

Ampiamente superata dagli algoritmi moderni, come il DES o anche il triple DES, è decifrabile da qualunque attaccante che abbia una quasi minima conoscenza di crittografia
Infatti, quando si hanno ulteriori informazioni sul sistema, come l'alfabeto utilizzato, la frequenza delle lettere più presenti in quell'alfabeto, i bigrammi e i trigrammi più frequenti, è facile risalire con un'analisi semi-statistica ogni lettere quale lettera rappresenta realmente, rendendo poi più facile la decifratura nei successivi passaggi
Tutto questo infatti si chiama frequency analysis

45 Cifrari a trasposizione (2014, 15, 20)

45.1 Descrizione

I cifrari a trasposizione sono tecniche di cifratura che consistono nel riordinare le lettere del testo in chiaro seguendo uno schema predeterminato, senza modificarne il valore
A differenza dei cifrari a sostituzione, che sostituiscono i caratteri con altri, la trasposizione si limita a permutare l'ordine delle lettere, generando un testo cifrato che appare casuale
Questi metodi possono essere applicati in vari modi, come attraverso griglie, schemi a zig-zag o scacchiere

45.2 Ambiti d'uso

1. Storia: Utilizzati in contesti militari antichi, come la Scitala spartana, per la trasmissione sicura di messaggi
2. Didattica: Usati per insegnare i principi fondamentali della crittografia e introdurre le differenze tra trasposizione e sostituzione
3. Giochi e enigmistica: Applicati in puzzle crittografici o escape room per simulare la decifrazione di messaggi cifrati

45.3 Pregi

1. Semplicità di implementazione: i cifrari a trasposizione sono facili da applicare sia manualmente che con strumenti minimi, come carta e penna
2. Maggiore sicurezza rispetto alla sostituzione semplice: non conservano direttamente la frequenza delle lettere del testo in chiaro, rendendo più complessa l'analisi di frequenza
3. Combinabilità: possono essere combinati con altri cifrari per aumentare la complessità della cifratura
4. Nessuna propagazione degli errori: un errore nel testo cifrato influisce solo sulla posizione specifica e non compromette il resto del messaggio

45.4 Difetti

1. Pattern evidenti: la trasposizione, se applicata a testi lunghi o con schemi ripetuti, può lasciare indizi utili per la decifrazione
2. Vulnerabilità ad attacchi combinatori: con strumenti moderni, uno schema di trasposizione può essere decifrato analizzando tutte le possibili permutazioni
3. Necessità di una chiave condivisa: la decifratura richiede che il destinatario conosca lo schema esatto usato per la trasposizione
4. Limitata sicurezza moderna: contro i metodi crittografici avanzati, i cifrari a trasposizione non offrono un livello di protezione adeguato

46 One time pad (blocco monouso) (2015, 16, 18, 20)

46.1 Descrizione

Il One Time Pad (OTP), o cifrario a blocco monouso, è un metodo di cifratura simmetrica che garantisce sicurezza perfetta, a condizione che venga utilizzato correttamente
Il testo in chiaro viene combinato con una chiave completamente casuale, lunga almeno quanto il messaggio, utilizzando lo XOR (esclusivo logico)
Ogni chiave deve essere usata una sola volta, da cui il nome "blocco monouso"
L'OTP è teoricamente inviolabile, ma è inutilizzabile in tutti i contesti moderni, è utilizzato infatti solamente in situazioni eccezionali come comunicazioni segretissime che non possono in nessuna situazione trapelare all'esterno

46.2 Ambiti d'uso

1. Comunicazioni militari e diplomatiche: utilizzato per la trasmissione di informazioni estremamente sensibili, come i messaggi tra capi di stato o militari durante la guerra

2. Sistemi ad alta sicurezza: Impiegato in sistemi dove la sicurezza assoluta è prioritaria, come nel caso di reti di intelligence

3. Applicazioni teoriche: usato come esempio ideale per comprendere i limiti e i principi fondamentali della crittografia

46.3 Pregi

1. Sicurezza perfetta: Se usato correttamente, l'OTP è matematicamente inviolabile, perché il testo cifrato non contiene informazioni statistiche sul testo in chiaro

2. Semplicità matematica: Il metodo utilizza operazioni semplici, come lo XOR, che lo rendono facile da implementare

3. Resistenza a tutti gli attacchi crittografici: nessun attacco basato sulla crittoanalisi può violare l'OTP se le sue regole vengono seguite

46.4 Difetti

1. Gestione della chiave: richiede una chiave lunga quanto il messaggio, che deve essere distribuita e conservata in modo assolutamente sicuro

2. Uso unico della chiave: ogni chiave può essere utilizzata una sola volta, aumentando la complessità logistica nelle comunicazioni frequenti

3. Impraticabilità per messaggi lunghi: per messaggi di grandi dimensioni, la gestione delle chiavi diventa onerosa

4. Difficoltà di distribuzione: la trasmissione sicura della chiave tra le parti è un problema significativo, soprattutto in scenari moderni.

5. Dipendenza dalla casualità: la sicurezza dipende dalla qualità della chiave, che deve essere completamente casuale

47 DES e triplo DES (2016, 18, 20, 21, 22, 23, 24, 25)

47.1 Descrizione

Il DES (Data Encryption Standard) è un algoritmo di cifratura simmetrica sviluppato negli anni '70 e standardizzato nel 1977
Utilizza una chiave di 56 bit e un approccio basato sulla cifratura a blocchi di 64 bit, combinando sostituzione e trasposizione attraverso 16 round di operazioni
Il Triple DES (3DES) è un'estensione del DES che applica l'algoritmo tre volte in sequenza con due o tre chiavi separate per migliorare la sicurezza
Encrypting e decrypting sono oltretutto intercambiabili perché non ci deve essere un ordine preciso, l'importante è non criptare e decriptare con la stessa chiave, altrimenti si applicherebbe un DES singolo

47.2 Ambiti d'uso

1. Bancario: DES e 3DES sono stati ampiamente utilizzati nei sistemi bancari per proteggere transazioni elettroniche, come nei bancomat e nei POS
2. Standard di sicurezza: 3DES è stato adottato come standard di sicurezza degli USA

47.3 Pregi

1. Semplicità: DES e 3DES sono ben documentati e semplici da implementare
2. Compatibilità: 3DES ha garantito una transizione graduale dai sistemi basati su DES
3. Maggiore sicurezza rispetto a DES: l'uso di tre chiavi in 3DES aumenta significativamente la lunghezza effettiva della chiave, rendendo più difficile il brute-force

47.4 Difetti

1. Chiave corta (DES): i 56 bit di chiave di DES sono vulnerabili agli attacchi brute-force con le tecnologie attuali.
2. Prestazioni (3DES): l'applicazione tripla dell'algoritmo lo rende più lento rispetto ad alcune soluzioni moderne
3. Deprecazione: DES è considerato insicuro ed è stato deprecato dagli standard
   Anche 3DES è in fase di abbandono, venendo sostituito da AES
4. Lunghezza effettiva della chiave (3DES con 2 chiavi): l'uso di 2 chiavi in 3DES fornisce solo una lunghezza effettiva di 112 bit

48 AES

48.1 Descrizione

L'Advanced Encryption Standard (AES) è il successore del Data Encryption Standard (DES) ed è l'attuale standard mondiale per la crittografia simmetrica AES è composto da diversi algoritmi di cifratura a blocchi, utilizzando chiavi di lunghezza variabile
Le chiavi e i blocchi possono essere scelti a 128 bit, 192 bit o 256 bit, sin dal momento della creazione dello standard, permettendo l'evoluzione della sicurezza e la scalabilità dello stesso quando necessario

48.2 Ambiti d'uso

AES è ampiamente utilizzato in molti ambiti, tra cui:

1. Crittografia dei dati: protezione dei dati sensibili in archiviazione e durante il trasferimento (ad esempio, in HTTPS, VPN, e-mail criptate).
2. Sistemi di autenticazione: protezione delle password e delle credenziali di accesso
3. Comunicazioni sicure: impiegato nei protocolli di sicurezza come SSL/TLS, WPA2 (Wi-Fi Protected Access), e IPsec
4. Sistemi di pagamento: crittografia delle transazioni bancarie e carte di credito

48.3 Pregi

I principali vantaggi di AES includono:

1. Elevata sicurezza: AES è considerato sicuro contro attacchi come il brute force, e le chiavi di 256 bit offrono un livello di sicurezza molto elevato
2. Velocità: AES è molto veloce sia in hardware che in software, ed è progettato per essere efficiente anche in dispositivi con risorse limitate
3. Resilienza: AES è resistente a vari tipi di attacchi crittografici, come quelli basati su analisi delle frequenze
4. Standard ampiamente supportato: AES è universalmente adottato e supportato in numerosi dispositivi e software di sicurezza

48.4 Difetti

Nonostante i numerosi vantaggi, AES presenta alcuni svantaggi:

1. Efficienza in dispositivi a bassa potenza: sebbene AES sia efficiente in hardware, può risultare meno ottimizzato in ambienti a bassa potenza o risorse limitate se implementato in software
2. Dipendenza dalla gestione delle chiavi: la sicurezza di AES dipende fortemente dalla corretta gestione delle chiavi. Se le chiavi vengono compromesse, la protezione dei dati è compromessa

49 RSA

49.1 Descrizione

RSA è un algoritmo di crittografia a chiave pubblica, ampiamente utilizzato per la protezione dei dati
La sicurezza di RSA si basa sulla difficoltà di fattorizzare numeri molto grandi, il che lo rende adatto per applicazioni come la firma digitale e lo scambio sicuro di chiavi

49.2 Ambiti d'uso

1. Firma digitale: utilizzato per verificare l'autenticità dei documenti e dei messaggi
2. Scambio sicuro di chiavi: usato per stabilire connessioni sicure tra due parti

49.3 Pregi

1. Sicurezza basata su matematica solida: la sicurezza di RSA è ben compresa e si basa su principi matematici comprovati
2. Flessibilità: può essere utilizzato sia per la crittografia che per la firma digitale

49.4 Difetti

1. Bassa velocità: RSA è più lento rispetto ad altri algoritmi simmetrici, il che lo rende meno ideale per cifrare grandi quantità di dati
2. Vulnerabilità alla fattorizzazione: la sicurezza di RSA può essere compromessa se i numeri utilizzati sono troppo piccoli o se vengono sviluppati metodi di fattorizzazione più efficienti

50 ECB (2014)

50.1 Descrizione

ECB (Electronic Code Book) è un modo di trasmettere testi cifrati
Infatti, il testo viene suddiviso in blocchi, e ogni blocco viene considerato come se fosse la pagina di un libro
Per risolvere eventuali mescolamenti delle pagine da parte di attaccanti, si creano dipendenze tra le pagine del libro in modo che non sia possibile scambiarle di posto

50.2 Ambiti d'uso

1. Cifratura di dati in batch: adatto per situazioni in cui i dati devono essere cifrati separatamente e senza dipendenza tra i blocchi

2. Applicazioni con requisiti di alta velocità: l'assenza di dipendenza tra i blocchi permette un'elaborazione rapida, ideale per applicazioni che richiedono performance elevate

3. Sistemi legacy: utilizzato in sistemi più vecchi o in ambienti con limitate risorse di elaborazione

50.3 Pregi

I principali vantaggi dell'ECB includono:

1. Semplicità: il funzionamento di ECB è facile da comprendere e implementare

2. Parallellizzazione: poiché ogni blocco è cifrato separatamente, l'algoritmo può essere facilmente parallellizzato per migliorare le performance

3. Velocità: essendo una modalità senza dipendenza tra i blocchi, è generalmente veloce e consuma meno risorse computazionali rispetto ad altri metodi

50.4 Difetti

Nonostante i vantaggi, ECB presenta anche alcuni svantaggi significativi:

1. Vulnerabilità agli attacchi di pattern: poiché lo stesso blocco di testo in chiaro viene sempre cifrato nello stesso modo, i pattern nei dati possono essere facilmente identificati, rendendo ECB meno sicuro per dati sensibili, come quelli contenenti informazioni ripetitive

2. Mancanza di diffusione: non essendo basato su meccanismi di mescolamento tra blocchi, eventuali debolezze in un singolo blocco possono propagarsi attraverso i dati cifrati

51 Stream cipher (2015, 16, 18, 19, 20, 23, 24)

51.1 Descrizione

I cifrari a flusso cifrano i dati un bit o un byte alla volta
A differenza dei cifrari a blocchi, che operano su intere unità di dati (blocchi), i cifrari a flusso utilizzano una chiave segreta per generare una sequenza di bit che viene combinata con il testo in chiaro tramite XOR
Sono più adatti per applicazioni che richiedono una cifratura continua, come nei canali di comunicazione

51.2 Ambiti d'uso

1. Comunicazioni in tempo reale: utilizzato in ambienti come il VoIP (Voice over IP) e altre forme di comunicazione in tempo reale

2. Protezione dei dati mobili: implementato in dispositivi mobili per garantire la cifratura continua dei dati

3. Trasmissioni in tempo reale: impiegato per la cifratura di flussi di dati in tempo reale in applicazioni come video streaming e giochi online

51.3 Pregi

1. Alta velocità: i cifrari a flusso sono veloci, poiché operano su singoli bit o byte, rendendoli ideali per applicazioni che richiedono elevata velocità di cifratura

2. Efficienza in spazi limitati: essendo basati su una chiave continua, i cifrari a flusso sono ideali per dispositivi con risorse di calcolo limitate

3. Adatti per flussi di dati infiniti: sono perfetti per applicazioni dove il flusso di dati non è predefinito o è continuo nel tempo

51.4 Difetti

1. Vulnerabilità al riutilizzo della chiave: se la stessa chiave viene riutilizzata, i dati cifrati diventano vulnerabili agli attacchi

2. Difficoltà di implementazione sicura: un'implementazione scorretta può esporre la chiave segreta a possibili attacchi

52 MTM

52.1 Descrizione

MTM (Man In The Middle) si riferisce a un tipo di attacco in cui un attaccante modifica i dati scambiati tra due parti senza il loro consenso
Questi attacchi possono compromettere l'integrità e l'autenticità delle informazioni, inoltre i dati possono essere rubati dagli attaccanti
Per essere contrastato, sono stati ideati i CA (Certification Authority) che certificano che l'unità con cui si sta parlando è effettivamente quella vera e non qualcuno che finge di essere ad esempio una banca

52.2 Ambiti d'uso

1. Attacchi contro i sistemi di comunicazione sicura: utilizzati per compromettere l'integrità dei dati trasmessi su reti sicure

2. Furto di dati sensibili: Gli attacchi MTM possono essere utilizzati per alterare o rubare dati sensibili

52.3 Pregi

1. Facilità di esecuzione: gli attacchi MTM non richiedono necessariamente una conoscenza avanzata delle tecniche di hacking

2. Alta efficacia: gli attacchi MTM possono compromettere rapidamente la sicurezza dei sistemi target

52.4 Difetti

1. Contrasto tramite crittografia: l'uso di crittografia e firme digitali può prevenire gli attacchi MTM
2. Alta visibilità in ambienti protetti: gli attacchi MTM sono più facili da rilevare in ambienti sicuri e ben protetti

53 IPSec (2019, 20, 22)

53.1 Descrizione

IPsec è un protocollo di rete che fornisce crittografia e autenticazione per le comunicazioni IP
Viene utilizzato per garantire la sicurezza delle comunicazioni tramite reti non sicure, come Internet, ed è particolarmente utile per la creazione di VPN sicure

53.2 Ambiti d'uso

1. VPN (Virtual Private Network): utilizzato per creare reti private virtuali sicure su reti pubbliche
2. Comunicazioni sicure tra dispositivi: protegge le comunicazioni tra dispositivi in reti aziendali o su Internet

53.3 Pregi

1. Sicurezza forte: fornisce protezione contro intercettazioni e alterazioni dei dati
2. Compatibilità con vari protocolli di rete: IPSec può essere utilizzato su molteplici protocolli di rete, inclusi IPv4 e IPv6

53.4 Difetti

1. Complessità di implementazione: la configurazione e la gestione di IPSec possono essere complesse
2. Overhead di rete: l'uso di IPSec può introdurre un overhead di rete, rallentando le comunicazioni

54 Modi di attaccare DNS (2018)

54.1 Descrizione

Gli attacchi al Domain Name System (DNS) mirano a compromettere la risoluzione dei nomi di dominio, influenzando le comunicazioni su Internet. Due delle principali tecniche di attacco sono il DNS spoofing e il DDoS (Distributed Denial of Service)
Il DNS spoofing consiste nell'inviare risposte DNS false a un client o a un server DNS, ingannando il sistema di risoluzione dei domini e redirigendo il traffico

verso destinazioni non desiderate
Il DDoS contro i server DNS può essere utilizzato per sovraccaricare un server DNS con un volume massiccio di traffico, impedendo che possa risolvere correttamente i domini per gli utenti legittimi

54.2 Ambiti d'uso

1. Attacchi contro la disponibilità di siti web: utilizzati per dirottare il traffico Internet verso server malevoli (DNS spoofing) o per sovraccaricare i server DNS, rendendo i siti web e i servizi online irraggiungibili (DDoS)
2. Attacchi di phishing: il DNS spoofing viene utilizzato per reindirizzare gli utenti a siti web fasulli, rubando informazioni sensibili come credenziali di login, dati bancari, e altro
3. Interruzione di servizio: il DDoS su server DNS è utilizzato per impedire la risoluzione dei domini, causando interruzioni nei servizi di rete

54.3 Pregi

1. Semplicità: gli attacchi come il DNS spoofing sono relativamente facili da eseguire, richiedendo poche risorse e conoscenze tecniche
2. Efficacia: Il DNS spoofing può compromettere rapidamente la navigazione web, reindirizzando gli utenti a siti malevoli

54.4 Difetti

1. Difesa con DNSSEC: meccanismi di protezione come DNSSEC (DNS Security Extensions) possono prevenire il DNS spoofing
2. Difficoltà di difesa contro DDoS: i DDoS contro i server DNS richiedono soluzioni scalabili come il bilanciamento del carico e l'uso di reti distribuite per mitigare l'impatto

55 Hash crittografici, HMAC (2016, 18, 19)

55.1 Descrizione

Un hash crittografico è una funzione che prende un input e restituisce una stringa di lunghezza fissa
Le funzioni hash sono progettate per essere unidirezionali, cioè facili da calcolare ma difficili da invertire
HMAC (Hashed Message Authentication Code) è una costruzione basata su una funzione hash che fornisce un meccanismo di autenticazione per verificare l'integrità e l'autenticità dei messaggi

55.2 Ambiti d'uso

1. Autenticazione nei protocolli di rete: utilizzato in protocollo come IPsec, TLS e HTTPS per garantire che i dati non siano stati alterati durante la trasmissione

2. Verifica dell'integrità dei dati: impiegato per assicurare che i dati non siano stati modificati durante la trasmissione o l'archiviazione

3. Generazione di chiavi segrete: utilizzato per la generazione di chiavi segrete condivise tra due parti

55.3 Pregi

1. Sicurezza: HMAC fornisce una forte garanzia di integrità e autenticità, proteggendo i dati da modifiche non autorizzate

2. Flessibilità: È compatibile con qualsiasi funzione hash, come SHA-1, SHA-256, ecc

3. Efficienza: HMAC è relativamente efficiente dal punto di vista computazionale, rendendolo adatto anche a dispositivi con risorse limitate

55.4 Difetti

Lentezza con funzioni hash deboli: se la funzione hash utilizzata non è ottimale le prestazioni e la sicurezza possono essere compromesse

56 WEP

56.1 Descrizione

WEP (Wired Equivalent Privacy) è un protocollo di sicurezza per le reti wireless, progettato per fornire un livello di protezione simile a quello delle reti cablate Utilizza il sistema di cifratura RC4 e una chiave di 64 o 128 bit per criptare i dati trasmessi tra il dispositivo wireless e il punto di accesso

56.2 Ambiti d'uso

1. Reti wireless domestiche: WEP è stato uno dei primi protocolli di sicurezza per reti Wi-Fi e veniva utilizzato principalmente nelle reti domestiche

2. Reti aziendali: In passato, molte aziende implementavano WEP per proteggere le loro reti wireless interne, sebbene sia stato successivamente sostituito da protocolli più sicuri come WPA e WPA2

56.3 Pregi

1. Implementazione semplice: WEP è facile da configurare e implementare, rendendolo una scelta popolare nelle prime fasi della sicurezza delle reti wireless

2. Supporto diffuso: essendo uno dei primi protocolli di sicurezza per le reti wireless, WEP è stato ampiamente supportato da vari dispositivi

56.4 Difetti

1. Vulnerabilità nella cifratura: Il metodo di cifratura RC4 e la gestione delle chiavi sono vulnerabili ad attacchi di forza bruta e attacchi di tipo "cracking", rendendo WEP obsoleto

2. Debolezza nella gestione delle chiavi: WEP utilizza una chiave condivisa statica, il che rende facile per un attaccante decifrare i dati dopo l'acquisizione di una quantità sufficiente di pacchetti cifrati