



Appunti reti e sicurezza

Internet, Reti E Sicurezza (Università degli Studi di Camerino)



Scansiona per aprire su Studocu



RETI E SICUREZZA

APPUNTI + ESERCIZI

NICCOLÒ LUCOZZI
(2024)

Internet

Rete che collega dei calcolatori (PC, terminali, hosts, end systems)

I terminali sono collegati da link di comunicazione che vengono gestiti da Router

Indirizza i pacchetti in ingresso verso i link d'uscita
il tragitto dei messaggi è detto Route o Path

Internet è reso possibile tramite l'implementazione di Standard sviluppati da IETF

Gli standard sono documentati negli RFC

Request for comment

internet engineering task force

Protocolli: Simili a normative umane che regolano le interazioni tra 2 o più entità.

Descrivono anche il formato e l'ordine dei messaggi

Fact

Per dialogare bisogna utilizzare lo stesso protocollo

Struttura della rete:

Network Edge → App o programmi

Vengono usati 2 tipi di modelli

Client / Server → Il client fa una richiesta e il server risponde

Peer to Peer → Ogni dispositivo può essere un client o un server

Connection Oriented vs Connectionless

TCP

UDP

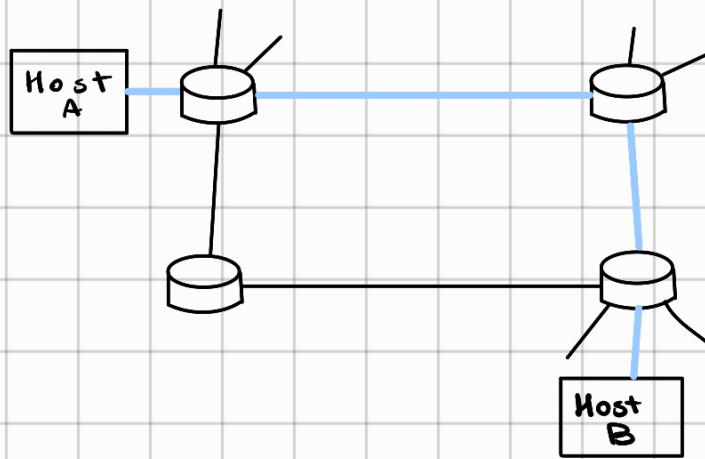
- Viene effettuato un handshake
 - Affidabile → i pacchetti persi vengono inviati di nuovo
 - Controllo del flusso → manca sovraccarico
 - Se la rete è congestionata viene abbassato il sending rate
- Niente handshake
 - I dati persi sono persi
 - Più veloce

Network Core → Trasferimento attraverso la rete

2 tipologie:

Circuit switching → Circuito dedicato per il trasferimento dati (rete telefonica)

Le risorse messarie vengono riservate per la durata della sessione.



Per inviare un messaggio da A a B viene prenotato il percorso.

La banda viene divisa equamente tra i link.

TDM → Time division Multiplexing

Si possono trasmettere 2 o più messaggi ma in tempi diversi

Totale banda divisa in diversi utenti
I segnali multiplexati possono provenire da diversi path

FDM → Frequency division multiplexing

Si possono inviare 2 o più messaggi sullo stesso circuito usando freq diverse
Tempo tot diviso in diversi utenti

Comportano uno spreco di risorse perché la banda è sempre allocata

Packet Switching → permette a più utenti di utilizzare la rete

Le App scambiano messaggi tramite l'invio e la ricezione di pacchetti.

I Router si occupano di trovare ed utilizzare il percorso migliore per i pacchetti, tramite Algoritmi di imstradamento (Forwarding).

Trasmissione store-and-forward:

Il commutatore deve ricevere l'intero pacchetto prima di ritrasmetterlo

Ogni commutatore connette più host, per ognuno di essi mantiene un buffer di output per conservare i pacchetti da inviare. Se il buffer è pieno avverrà una perdita di pacchetti quando ne arriverà uno nuovo.

Ogni router ha una tabella dioltro che serve a definire i collegamenti in uscita

Physical Media: materiale fisico usato per il trasferimento

Twisted Pair copper wire → Usato nelle LAN

Un cavo UTP Cat6 trasporta fino a 10 Gbps in velocità

Cavo Coassiale → Tipico cavo dell'antenna

Fibra ottica → Costoso ma molto veloce (39.8 Gbps)

Tempo di Trasmissione

$$\frac{L}{R} = \frac{\text{dimensione pacchetto}}{\text{rateo di trasmissione sul link}}$$

Backbone area: è una parte di rete che interconnecta vari pezzi di rete.
una Backbone può collegare interi edifici o vaste aree

Sistemi Autonomi (AS): è un insieme di host, router e reti fisiche
Viene identificata da un numero assegnato da IANA

Le AS possono affidare a dei router il compito di comunicare con l'esterno

Esistono 2 tipi di protocolli usati dalle AS:

IGP (Interior gateway protocol)

EGP (Exterior gateway protocol)

Internet service provider (ISP)

Soggetto che fornisce a degli utenti, l'accesso e una fornitura ai servizi internet.

Gli ISP hanno una gerarchia:

1° → Op internazionali che gestiscono i trasferimenti sulle dorsali,

2° → Op nazionali che raccolgono il traffico dei singoli utenti,

3° → Op locale

Tipi di ritardo:

Ritardo di elaborazione → tempo per determinare il destinatario e l'intestazione

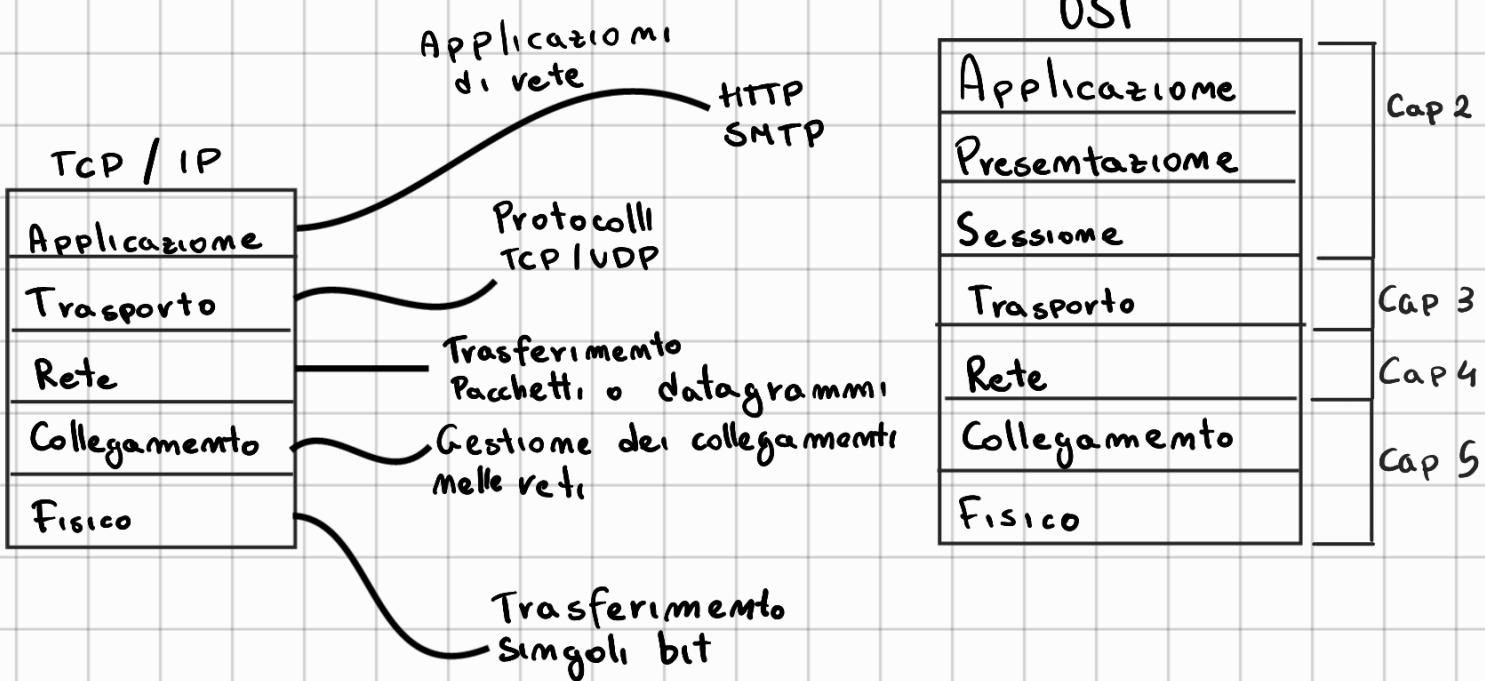
Ritardo di accodamento → Ritardo nella trasmissione sul collegamento

Ritardi di trasmissione → ritardo per via della trasmissione degli altri pacchetti in coda

Ritardo di Propagazione → tempo di propagazione fino al router

Ritardo End - To - End → Ritardo di elab a ciascun router e presso il mittente

Architettura a livelli:



Livello Applicativo → Messaggi

Livello di Trasporto → Segmenti,

Livello di rete → Datagrammi,

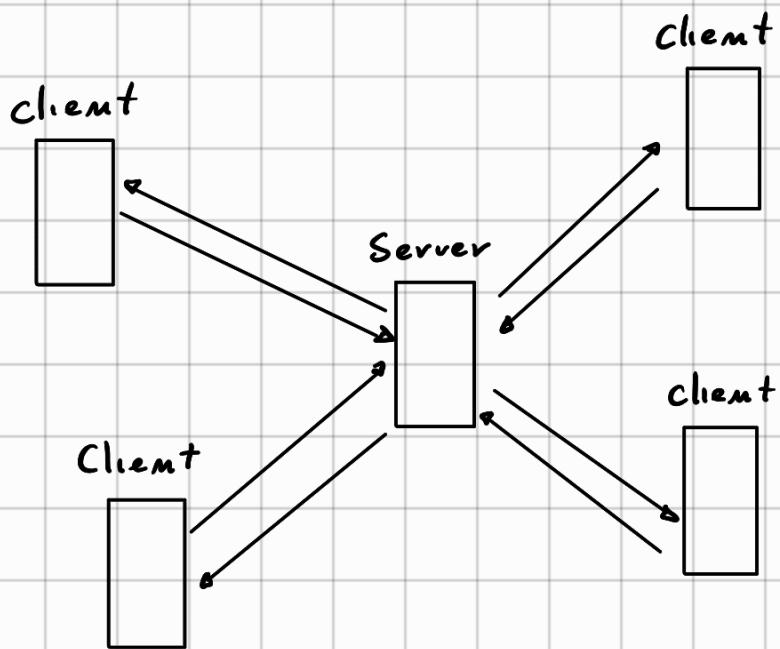
Livello Fisico → Frames

Livello di Applicazione

Esistono 2 tipi di architetture in uso:

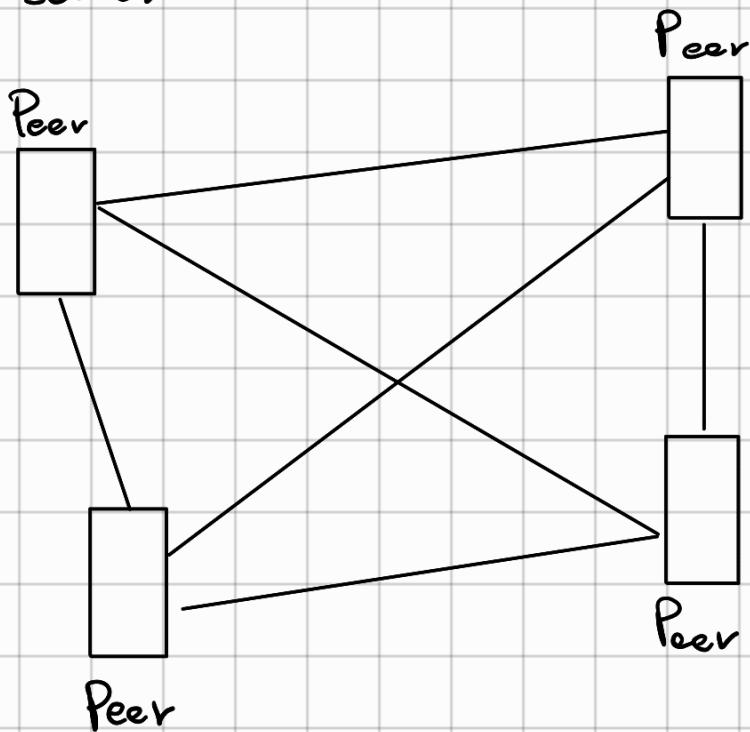
Client / Server

Architettura in cui diversi client contattano un server che risponde alle loro richieste



Peer 2 Peer

Gli host coinvolti sono considerati allo stesso tempo client e server



HTTP (Hyper text transfer protocol) porta 80

Protocollo client - server → client crea una commessione e richiede dei dati
e il server risponde

È un protocollo Stateless → non vengono mantenuti i dati delle sessioni

Commessioni:
non persistenti → Singolo oggetto trasmesso nella commessione
persistenti → Oggetti multipli nella stessa commessione

Pacchetto richiesta

metodo	SP	URL	SP	versione CR LF
Nome campo intestazione	SP	valore	CR	LF
	//			
Nome campo intestazione	SP	valore	CR	LF
CR LF				
corpo				

Metodi:

Head: è un get per i parametri dell'header

Get

Post

Put: trasferimento documenti

Delete: elimina doc

Trace: serve a diagnosticare

Connect: usato con proxy tunnel

RTT (Response Time Modeling)

tempo che un pacchetto impiega per viaggiare tra client e server e poi a ritorno.

HTTP State Management Mechanism

Per gestire gli state tra una sessione e l'altra vengono utilizzati i cookies, ovvero dei file di testo dove a delle chiavi sono associati dei valori

POP3 (Posta elettronica) porta 111
Funziona tramite una connessione TCP
Dopo l'autenticazione lo User-Agent può recuperare
le email, cancellarle ecc...

Quando lo UA si disconnette il server cancella i
messaggi marcati come da eliminare

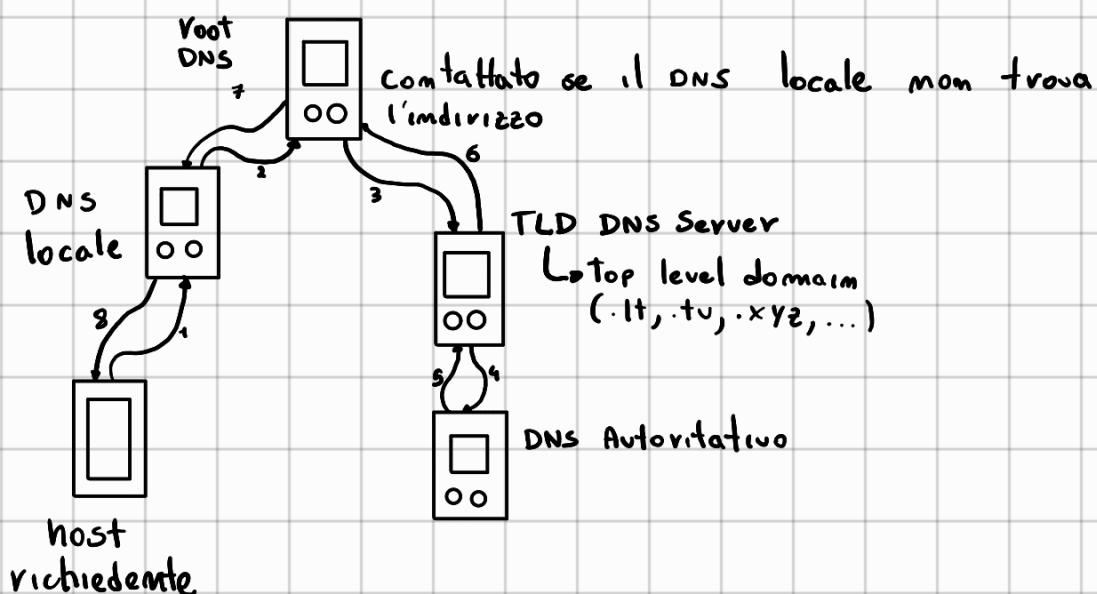
IMAP (Posta elettronica)

Il server IMAP associa ad ogni messaggio una cartella

DNS (Domain Name System)

S. tratta di un database distribuito e un protocollo che
associa ad un indirizzo il relativo dominio
 $102.45.97.201 \longrightarrow \text{www.amazon.com}$

Un host che decide di richiedere l'indirizzo di
un dominio effettua la seguente procedura.



Formato Messaggi DNS:

Identificazione	Flag
Mnum domande	Mnum RR in risposta
Mnum RR Autoritativi	Mnum RR Addizionali
Sezione domande	
Sezione Risposte	
Sezione Autoritativa	
Sezione Aggiuntiva	

Web cache (Proxy Server)

Il proxy server tenta di rispondere alle richieste senza dover accedere ad un server remoto

Un esempio di web cache è il nostro browser.

Invece di evitare di farci recapitare un contenuto già richiesto in precedenza cerca se ha in memoria il contenuto e lo carica localmente

Tramite il Get Condizionale la cache può chiedere al server remoto se i dati in memoria sono aggiornati ed in caso li aggiorna.

FTP (File Transfer Protocol) Porta 20/21

Usa il modello client/server.

Il client contatta il Server sulla porta 21 e vengono create 2 connessioni TCP: una per i dati, e una per i messaggi di controllo.

Viene creata e chiusa una connessione per ogni file trasferito.

SMTP (Simple Mail Transfer Protocol) Porta 25

Utilizza TCP per il trasferimento

3 fasi:

Handshake

Trasferimento

Chiusura

SNMP Porta 161 (UDP)

Protocollo utilizzato per monitorare dispositivi connessi nella rete

Telnet Porta 23

funziona tramite una connessione TCP non crittata.

Quando inviamo un carattere o un buffer dobbiamo aspettare che il server ci risponda con l'interfaccia da stampare

Livello di Trasporto

Differenza con il livello di rete

Il livello di trasporto prende i pacchetti, ne controlla eventuali errori e li manda al layer applicativo dove appartengono.

Il livello di rete si occupa di inviare i pacchetti al computer giusto.

Multiplexing e Demultiplexing

Per multiplexing si intende il processo di prendere tutti i pacchetti da inviare
aggiungere gli header e di inviarli

Per demultiplexing si intende il dividere e spedire i pacchetti
in avvio al layer giusto

Socket

È un software che consente la comunicazione tra due processi
nella rete

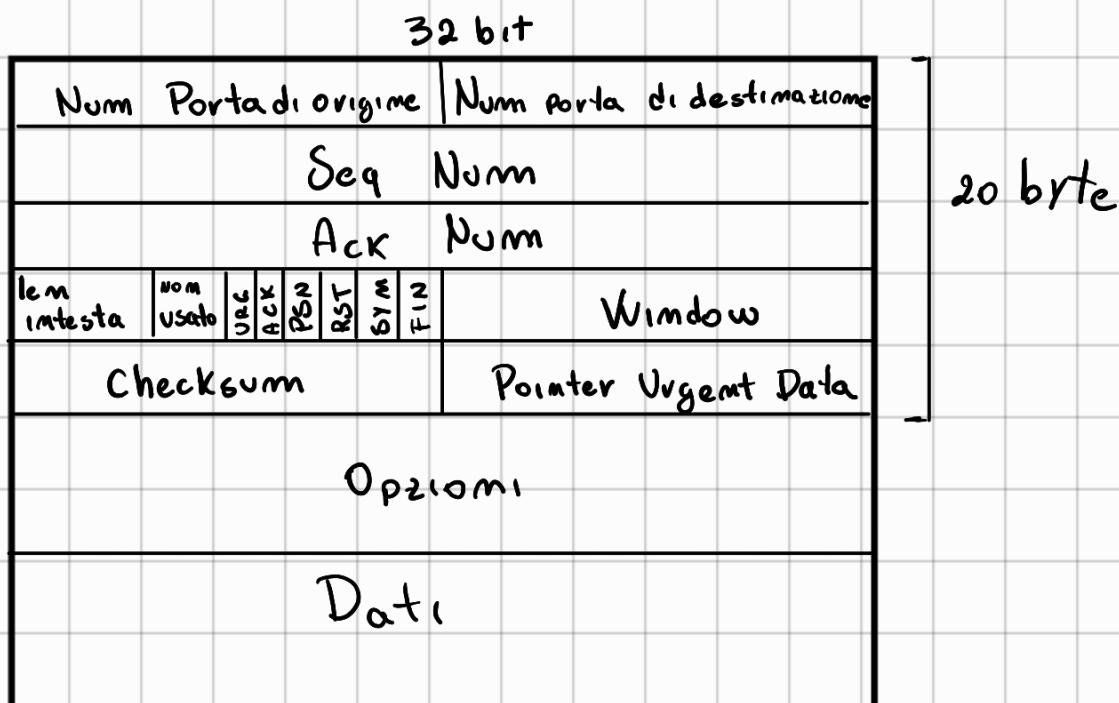
Tcp (Transmission Control Protocol)

Questo protocollo implementa lo scambio di pacchetti tra due host periferici tramite l'utilizzo di una connessione handshake e priva di salvataggio di stati

L'instaurazione della connessione avviene tramite una procedura di handshake triplo.

I segmenti TCP sono caratterizzati dai seguenti parametri:

- Sequence number] entrambi 32 bit, usati per garantire
- Acknowledgment number] una trasmissione affidabile
- Receive Window] 16 bit usato per il controllo del flusso



Connessione TCP (3 way-handshake)

Il client invia al server un segmento privo di dati ma con il bit SYN ad 1

Quando il segmento arriva al server capisce che il client vuole instaurare una connessione, quindi invia al client un segmento con il SYN a 1 e il campo Ack-num a $\text{client-ISM} + 1$. Nello stesso comunicato al client il

Seq number iniziale

numero di sequenza del server. (SYNACK)

Il client risponde con un segmento contenente nel campo Ack-num $\text{server-ISM} + 1$, il bit SYN a 0

Completati i 3 passaggi la connessione è instaurata

Chiusura connessione

Per terminare la connessione viene impostato il bit di FIN a 1

Quando il server riceve il segmento di fine invia al client un segmento con il bit FIN a 1 infine il client risponde con l'acknowledgment

Se il server deve ancora inviare dati usa un 4 way-handshake finché non ha finito di inviare

Gestione flusso

Serve ad evitare che il mittente saturi il buffer di ricezione
Il mittente ha una variabile detta finestra di ricezione
la cui grandezza è data dal ricevente ed è uguale a
ampiezza buffer - (ultimo byte letto - ultimo byte passato)

Il mittente per inviare dovrà assicurarsi di trasmettere i dati solo quando la diff tra l'ultimo byte inviato e l'ultimo riscontrato (ack) è \leq della finestra di ricezione

Controllo Congestione

Avieme una congestione quando vengono inviati troppi dati e la rete non può gestirli

Per controllare la congestione c'è bisogno di variare in modo dinamico la finestra di trasmissione

Questa finestra scorrevole è detta congestion window

Esistono alcuni algoritmi per la gestione della finestra

- AIMD

Ogni RTT la finestra aumenta di 1 MSS.

- Slow Start

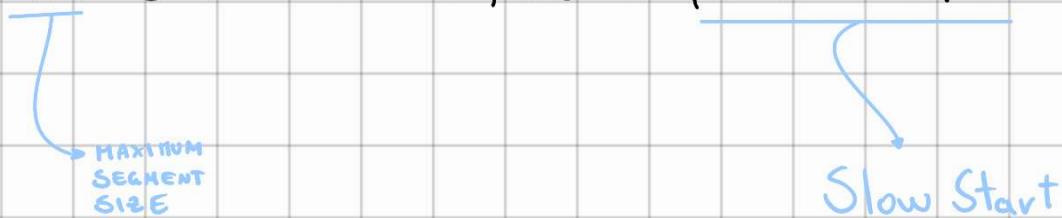
La finestra viene impostata ad 1 MSS. Ad ogni ACK viene aumentata di 1 MSS

- Fast Recovery

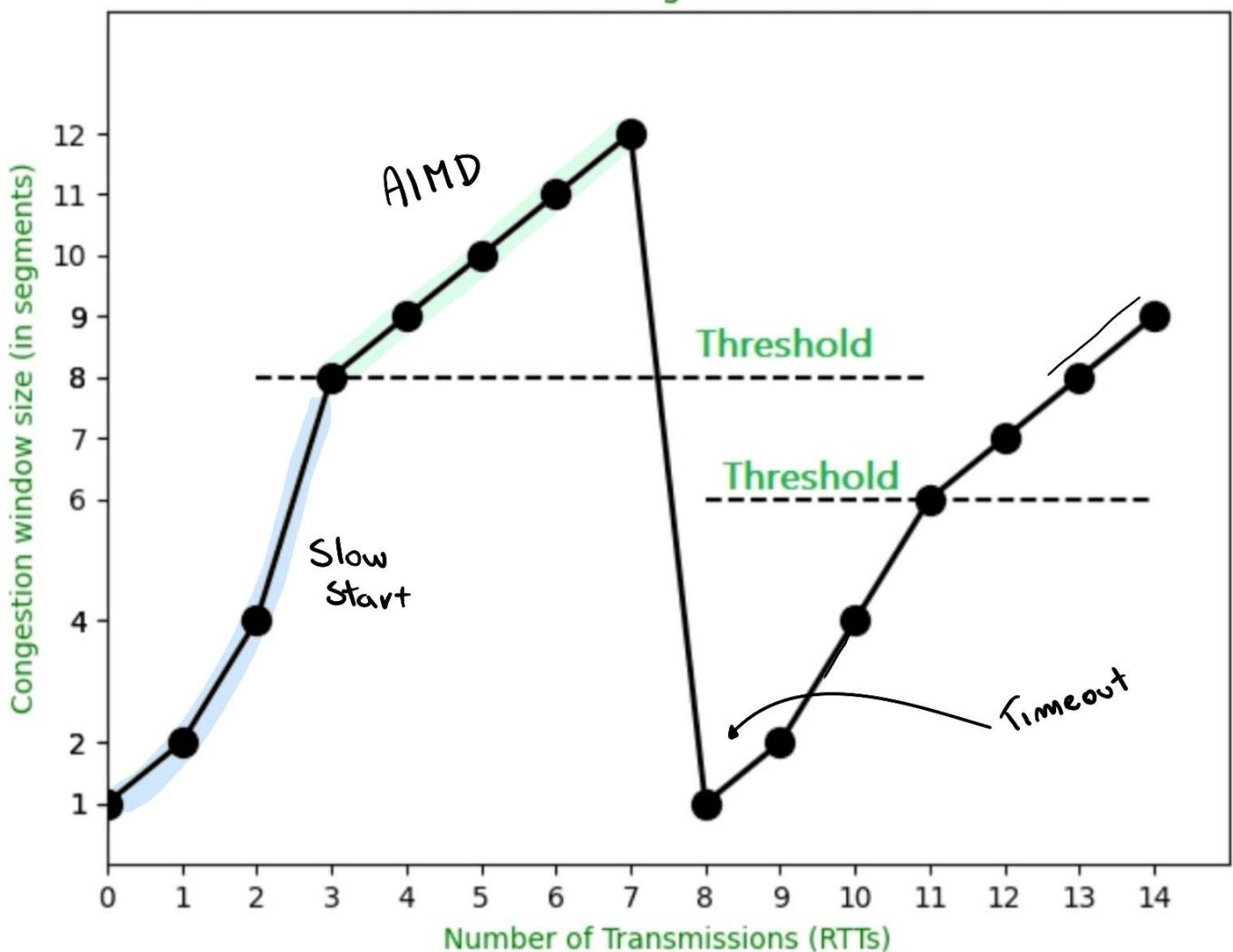
Quando vengono identificati 3 segmenti, ACK duplicati:

TCP Tahoe

Quando avviene un timeout viene tagliata la finestra a 1 MSS e si entra in fase di partenza lenta

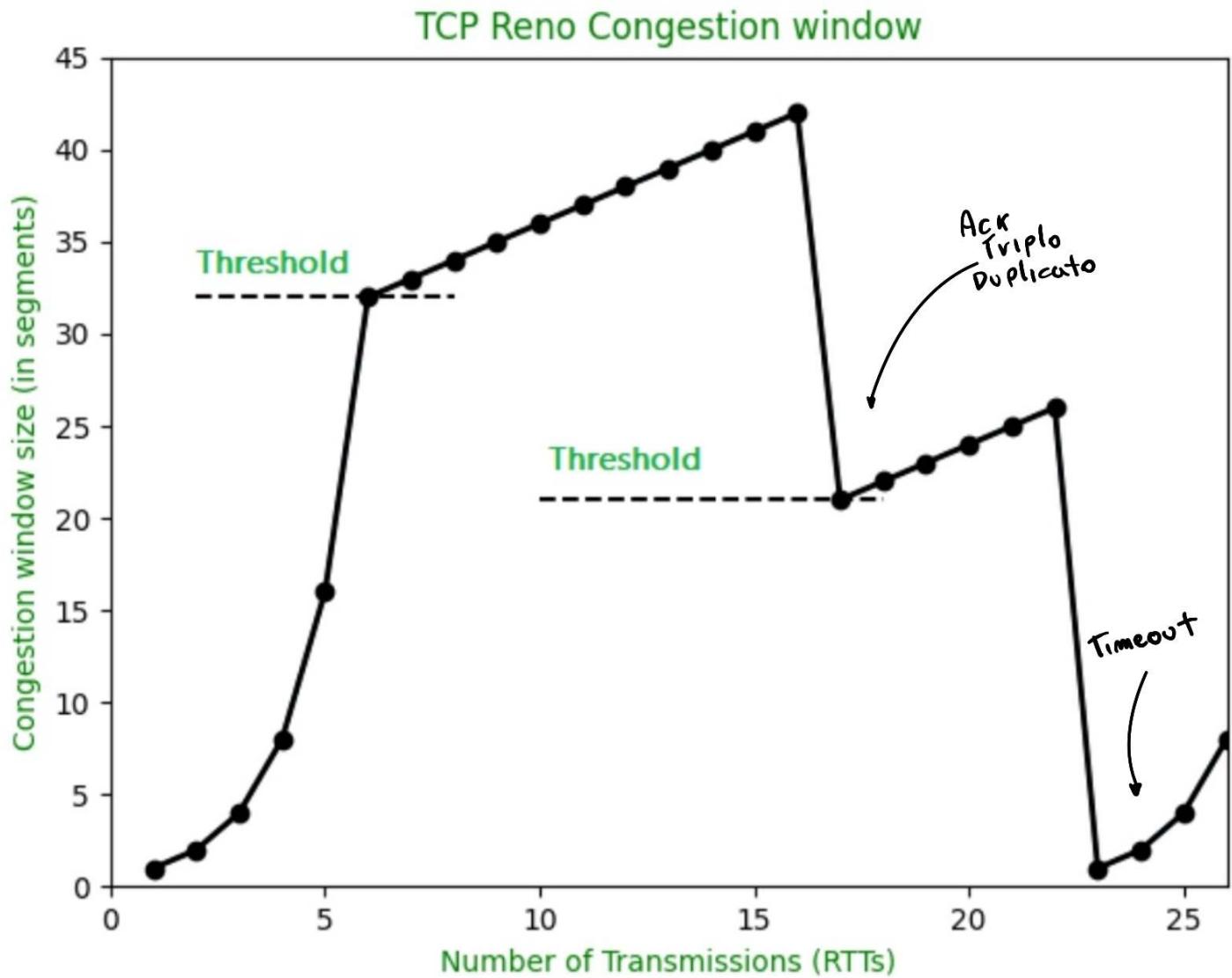


TCP Tahoe Congestion window



TCP Reno

Invece di effettuare una partenza lenta effettua un fast recovery



Se arriviamo 3 Ack allora la rete funziona perché i pacchetti arrivano

UDP (User Datagram Protocol)

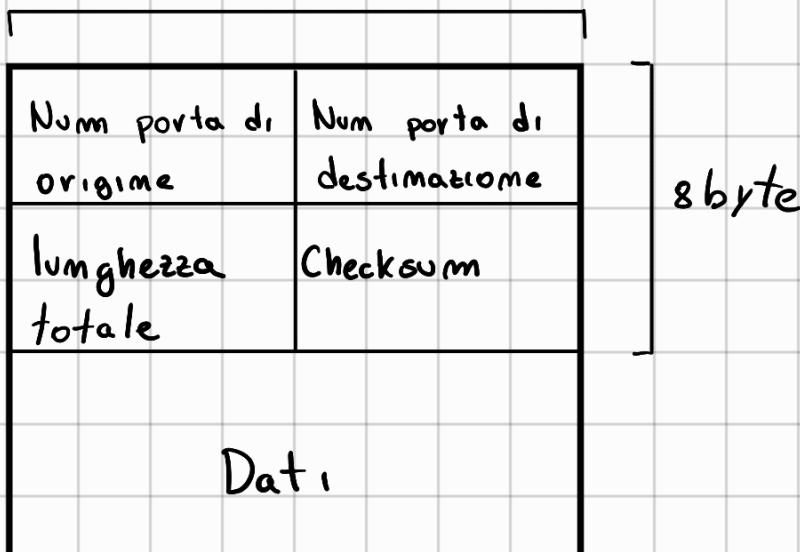
Si tratta di un protocollo di trasporto ridotto all'osso
l'unica cosa che fa è prendere i messaggi dal layer applicativo,
aggiunge la porta di destinazione e passa il tutto
al livello di rete

Non ha handshake → Non è orientato alla connessione

Perché scegliere UDP :

- Controllo maggiore su quando inviare i dati e quando (TCP ritarda l'invio in base alla congestione)
- Nessuno stato di connessione (UDP non mantiene informazioni su connessione e client, quindi il server è in grado di sostenere più connessioni)
- Intestazione dei pacchetti più corta (8 byte)

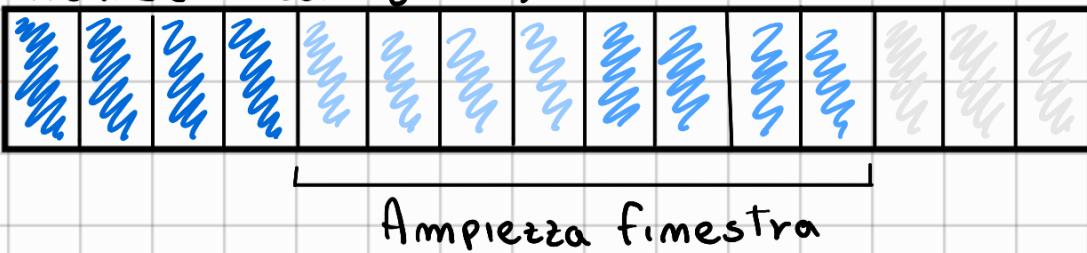
32 bit



Go - Back - N (GBN)

In questo tipo di protocolli possiamo essere mandati pacchetti senza dover aspettare l'ack, ma non si possono inviare più di n pacchetti

Pipeline (coda dei segmenti)



- Ack avvenuto
- Invia, No Ack
- Utilizzabile, non inviato
- Non utilizzabile

Il mittente GBN deve rispettare 3 eventi:

- Invocazione dall'alto

Quando viene inviato un pacchetto si controlla che la finestra (coda di invio) non sia piena. Se lo è rimanda il pacchetto al layer applicativo che ripeterà più tardi, al contrario invierà il pacchetto

- Ricezione Ack

L'ack del pacchetto con seq num viene considerato come cumulativo → tutti i pacchetti con seq num minore sono stati confermati

- Timeout

Quando avviene, il mittente invia di nuovo tutti i pacchetti che ancora non hanno ricevuto Ack

Ripetizione Selettiva (SR)

Invece di rimuovere tutti i pacchetti della finestra dopo il time out si rimuovono solo quelli non ancora riscontrati.

Stop and Wait

In questo tipo di protocolli il mittente manda solo un frame alla volta. Dopo l'invio aspetta l'ack per poter continuare.

Livello di Rete

Il ruolo del livello di rete è diviso in 2 funzioni:

- Imoltro → Invio da mittente a destinatario
- Istradamento → determinare il percorso dei pacchetti tramite algoritmi di routing

I Router estraggono dai pacchetti i valori da usare per indicizzare la tabella di imoltro. Tramite la tabella il router trova il percorso più veloce al prossimo modo.

Cosa contiene un Router?

- Porte in ingresso (Hardware)
- Struttura di commutazione → Commette le porte in ingresso con quelle in uscita
- Porte in Uscita (Hardware)
- Processore di Istradamento → Esegue protocolli di Istradamento e gestisce le tabelle di imoltro

Tipi di imoltro

- Basato sulla destinazione
Il Router stabilisce la prossima direzione ed invia lì il pacchetto
- Generalizzato
Il Router non valuta il percorso solo in base alla destinazione ma anche in base ad altri fattori

Struttura di commutazione

Struttura che inoltra i pacchetti dalla porta in ingresso a quella in uscita.

- Commutazione in memoria

Quando un pacchetto arriva nella porta ing. con un interrupt si segnala alla CPU il suo arrivo, il pacchetto viene copiato in memoria e poi viene imstradato

- Commutazione tramite BUS

le porte ing. Usano un BUS condiviso per inviare i pacchetti verso le uscite leggendo un etichetta al pacchetto che indica in quale porta in uscita deve andare.

Il pacchetto viene inviato a tutte le porte in uscita.

Se l'etichetta non corrisponde alla porta il pacchetto viene scartato

- Commutazione attraverso rete di interconnessione

Invece del Bus viene usata una matrice di comunicazione dove 2n Bus collegano m porte in. a m porte out

Questa matrice è non-blocking mentre negli altri metodi la trasmissione viene bloccata per tutti tranne uno.

Accodamento

Così l'arrivo dei pacchetti si possono formare code

Queste code possono portare a ritardi e perdite di pacchetti

- Accodamento in ingresso

Se il sistema non è abbastanza rapido a trasferire i pacchetti essi si accoderanno in ingresso

- Accodamento in uscita

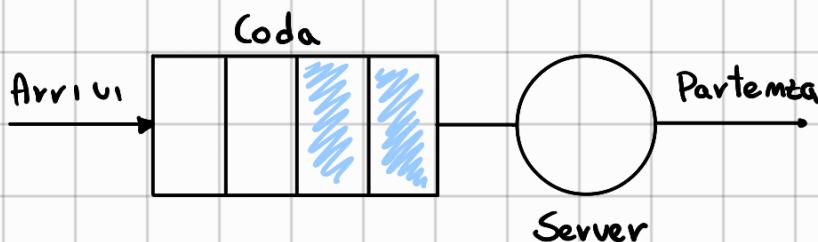
Visto che in uscita posso essere inviati solo N pacchetti ad un intervallo stabilito si rischia l'accodamento.

Se il buffer si riempie bisognerà decidere se scartare i nuovi pacchetti o fare posto eliminando gli altri.

Schedulazione di pacchetti (come determinare l'ordine) dei pacchetti in uscita

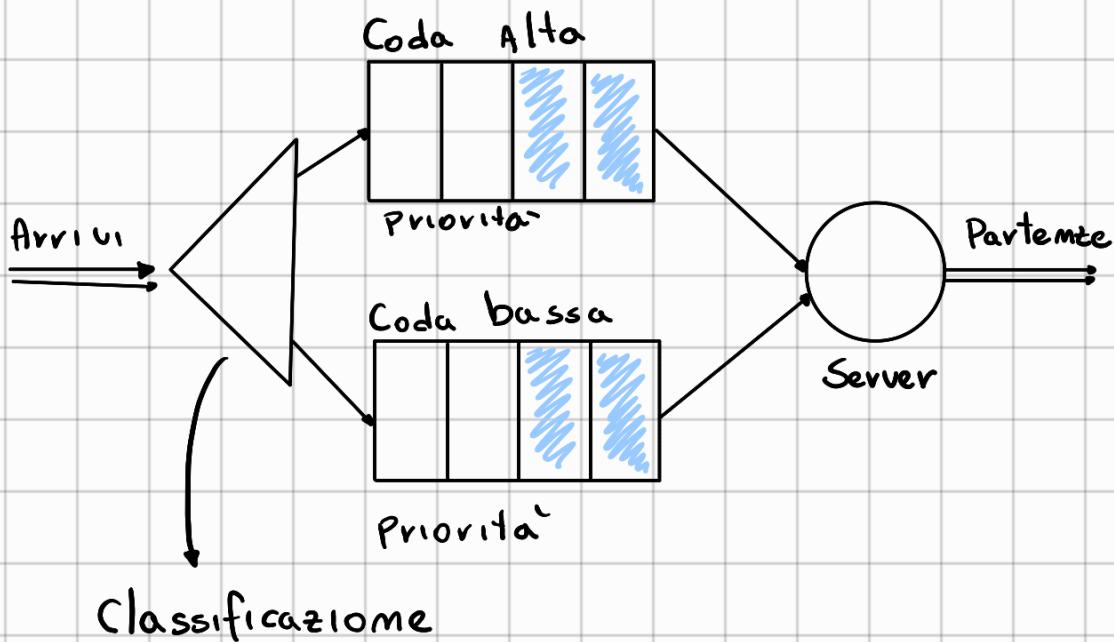
- F,F₀ (First in First Out)

Il primo che arriva è il primo ad essere servito



• Code con Priorità

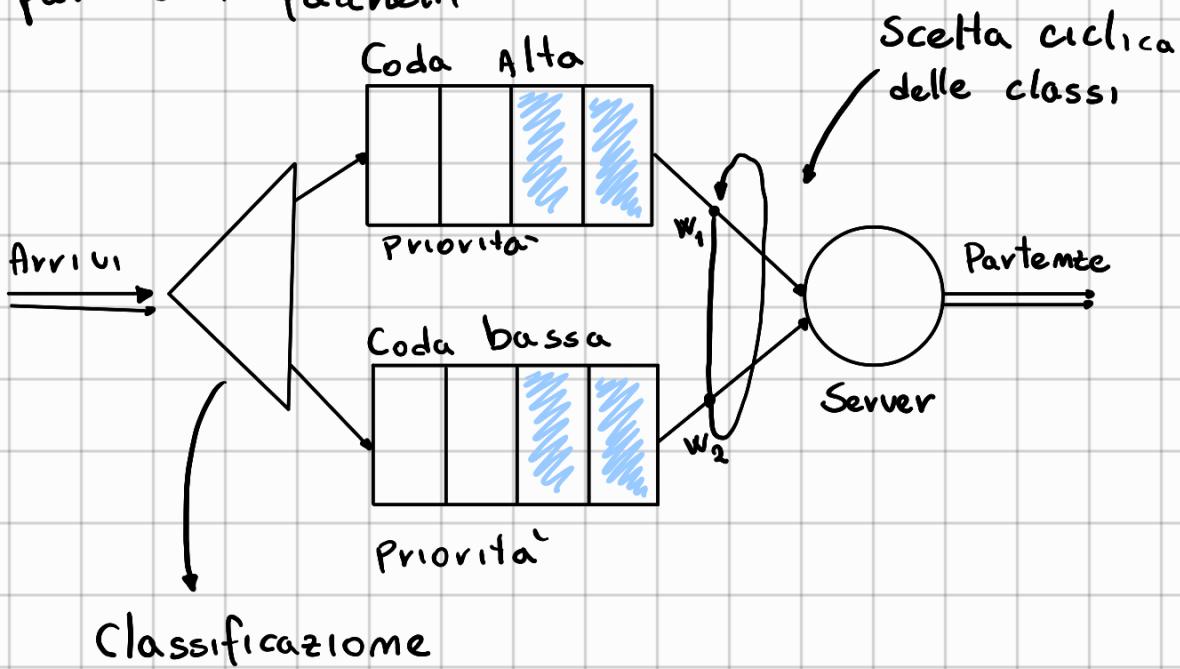
I pacchetti vengono classificati in base alle classi di priorità



Pacchetti di applicazioni real-time o con info di rete hanno la priorità

• Round Robin e accodamento equo ponderato

I pacchetti sono suddivisi in classi ma poi viene prevista una sequenza ciclica delle classi da cui far partire i pacchetti



Protocollo IP

Attualmente sono in uso 2 versioni del protocollo IP
(IPv4 e IPv6)

32 bit

Versio ne	lem header	Tipo di Servizio	lem datagramma (byte)
	Identificatore a 16 bit	Flag	offset di framme tazione (13 bit)
tempo di vita (TTL)	Protocollo di liv superiore		checksum header
Ind IP Sorgente (32 bit)			
Ind IP Destinazione (32 bit)			
Opzioni			
Dati			

Indirizzamento IPv4

Gli indirizzi IP sono lunghi 32 bit (4 byte) e quindi sono possibili 2^{32} indirizzi (circa 4 miliardi)

Ogni interfaccia e router su internet ha assegnato un indirizzo globale univoco (i sistemi gestiti da Nat non sono compresi)

Per IP esistono delle sottoreti, ovvero delle reti più piccole che connettono solo determinati host

Ad ogni indirizzo facente parte di una sottorete IP assegna una maschera di rete

Ad esempio "10.45.201.2 /22" dove /22 identifica la maschera e vuol dire che i primi 22 bit della maschera identificano la rete di appartenenza

La strategia di assegnazione degli indirizzi IP è detta CIDR (Classes interdomain routing)

L'indirizzo viene diviso in 2 parti "a.b.c.d/x" dove x indica il num di bit nella prima parte dell'indirizzo (prefisso di rete)

I rimanenti 32-x bit possono essere utilizzati per individuare i dispositivi nella rete.

Prima di CIDR gli indirizzi di sottoreti da 8, 16, 24 bit venivano classificati con il termine classe A, B, C

DHCP

Quando un'organizzazione ottiene un blocco di indirizzi (insieme) può assegnarli individualmente oppure dinamicamente tramite il Dynamic host Configuration Protocol

Il suo funzionamento è racchiuso in 4 punti

- Individuazione Server DHCP

Un host appena collegato alla rete invia un broadcast un messaggio detto DHCP DISCOVERY al quale solo il server DHCP può rispondere

- Offerta Server DHCP

Il server risponde con una DHCP OFFER contenente un indirizzo da poter utilizzare.

Il pacchetto viene inviato in broadcast

- Richiesta DHCP

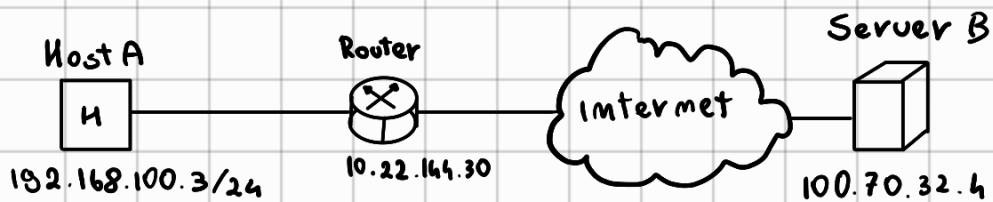
Il client sceglie una delle offerte e risponderà con una DHCP Request

- Conferma DHCP

Il server risponde con un messaggio di ACK (DHCP ACK)

NAT

Il Network Address translation si occupa di convertire un indirizzo IP privato in pubblico e viceversa quando ci si trova a confine di una rete



Quando l'host A vuole contattare il server B, interviene il NAT sul router che converte l'indirizzo privato in pubblico aggiungendo la porta.

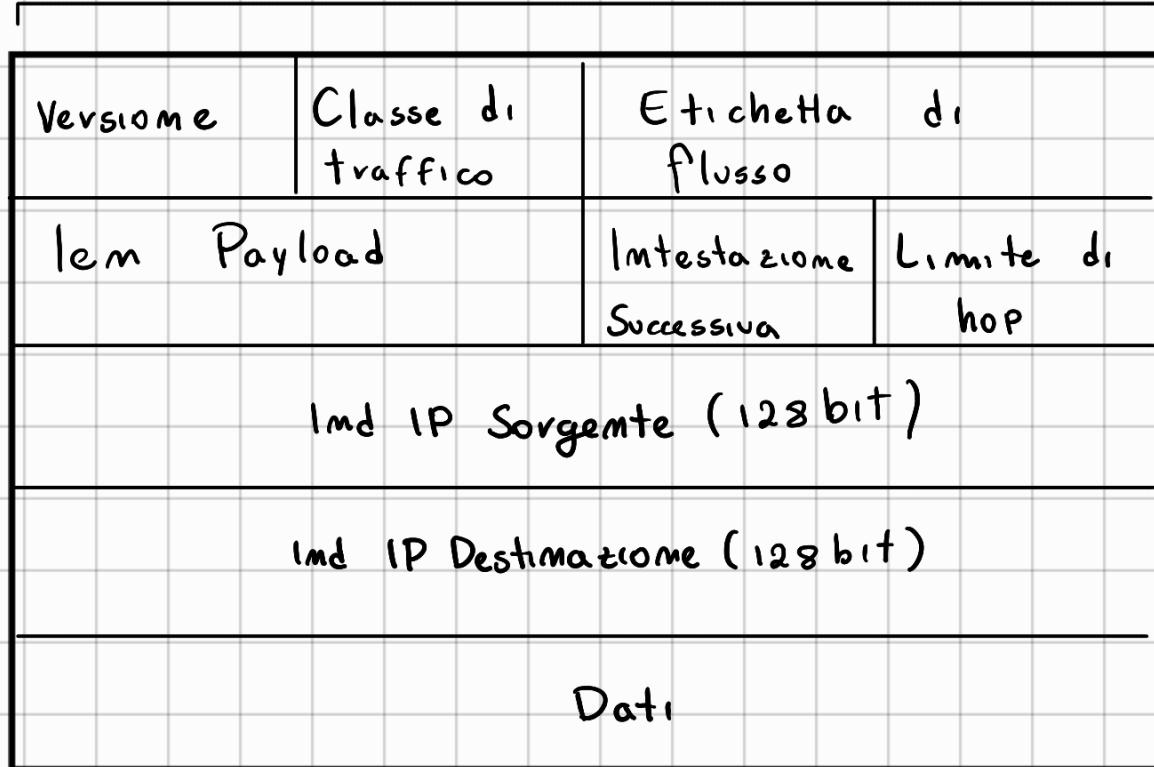
Viceversa se il Server tenta di contattare il client A utilizzerà l'indirizzo pubblico 10.22.164.30 e la porta specifica. Sarà poi il Router e il NAT a tradurre ed indirizzare il pacchetto correttamente

Il NAT fa uso di una tabella di traduzione. I Router abilitati al NAT appaiono come dispositivi singoli e quindi viene maschera la topologia della rete.

IPv6

Questa nuova versione venne ideata ed implementata quando cominciarono a scarseggiare gli indirizzi IPv4

32 bit



IPv6 aumenta l'indirizzamento a 128 bit, in questo modo ogni granello di sabbia potrebbe avere il suo indirizzo IP

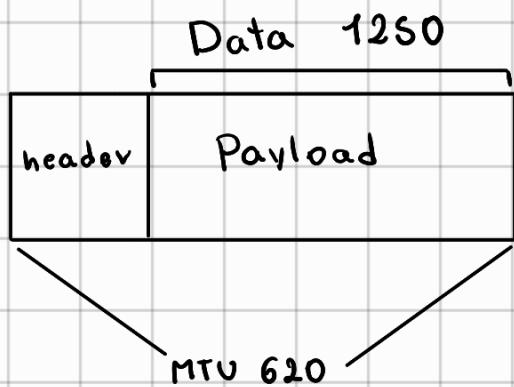
Inoltre alcuni campi dell'header sono stati rimossi fino ad arrivare a 40 byte per ottimizzare l'invio di pacchetti.

Nostante le migliorie del protocollo IPv6 non è ancora stato effettuato un passaggio completo

Frammentazione datagrammi IP

I pacchetti IP vengono frammentati per accomodare il MTU del collegamento.

Prendiamo come esempio l'invio di questo pacchetto TCP



MTU

Quantità massima di dati che un frame a livello di collegamento può trasmettere

Dal valore di MTU elimineremo l'header TCP che di solito è di 20 byte
MTU = 600.

Quindi invieremo diversi pacchetti da 600 byte contenenti i dati frammentati.

Questi frammenti vengono riassemblati prima di raggiungere il livello di trasporto del destinatario.

Per capire come riassemblarli e in quale ordine bisogna usare i campi predisposti a questa funzione (id, flag, offset di frammentazione)

Il flag è posto a 0 solo se si tratta dell'ultimo pacchetto altrimenti è impostato a 1

Lan (Local area network)

È una rete locale che ricopre una piccola area geografica grazie a ciò ha migliori prestazioni in termini di velocità di trasferimento.

Hanno un unico canale trasmissivo condiviso tra tutti i dispositivi. Funziona tipo un BUS perciò la trasmissione è di tipo broadcast.

Una LAN è

- Affidabile
- Flessibile
- Modulare
- Espandibile
- Gestibile

Elementi principali

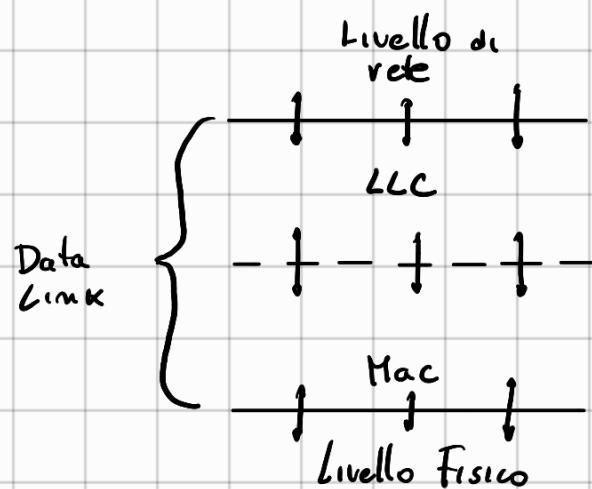
protocolli
IEEE 802

cablaggio
strutturato

Standard per
i livelli fisico
e data link

Livello Data-Link

Nel modello OSI troviamo il livello Data-Link che si occupa di strutturare il messaggio in base al formato in uscita



LLC (Logical Link Control)

Serve ad aggiungere al frame l'indirizzo di destinazione e il sorgente

Gestisce gli errori (Ack e timeout)

frammenta i frame troppo lunghi e gestisce la sliding window

Mac (Medium Access Control)

Il Mac serve ad identificare uno specifico host nel mondo

Il suo indirizzo è formato da 48 bit



MAC PDU (Protocol Data Unit) Frame

I campi principali sono

- Header che contiene (indirizzi SAP)
 - DSAP (indirizzo di destinazione)
 - SSAP (indirizzo di partenza)
- Payload (contiene i dati)
- FCS (Frame check sequence)
effettua il controllo integrità dei dati (CRC)

PDV e MAC

Bridge / Ponte cosa legge in ingresso

Tipi di cavi

UTP (Unshielded Twisted Pair)

STP (Shielded Twisted Pair)

Diritto → Collega 2 disp diversi fra loro

Crossover → Usato per connettere 2 dispositivi uguali

Rollover → Usato per connettersi e configurare router e switch

Coassiale → Cavo dell'antenna

Standard IEEE 802.3 (CSMA/CD)

ThickNet (10 base 5)

Lem massima 500 mt

Vel massima 10 Mbps

ThinNet (10 base 2)

Lem max 185 mt

Vel max 10 Mbps

100 base 2 → Vel max 100 Mbps Lem max 200mt

10 base T → doppimo telefonico (2 coppie di ramme) Lem max 100mt

100 base TX → Full duplex (Cavo in entrambi le direzioni)

IEEE 802.4 / 5 Token BUS / RING

Utilizzo nelle 2 topologie il sistema di token per decidere chi trasmette

FDDI: Uso di 2 anelli indipendenti controrotanti
Rete autoriparante

IEEE 802.11 b Wireless LAN

Freq a 2.4 Ghz

Vel massima di trasmissione di 11Mbps

Costo e vel basso

Possibili interferenze

Algoritmi di indirizzamento

Questi algoritmi vengono utilizzati per determinare i percorsi tra sorgente e destinatario attraverso la rete

Il percorso minore ha un costo minimo ma ci sono altri parametri che determinano il percorso da scegliere (policy)

Per applicare questi algoritmi si considera la rete come un grafo dove i nodi sono router e gli archi i collegamenti fisici tra di loro

Gli Algoritmi possono essere classificati come

- Centralizzati

Viene calcolato il percorso dal costo minimo tra sorgente e destinazione sfruttando una conoscenza globale della rete

Spesso questi sono Algoritmi Link-State

- Decentralizzati

Il percorso a costo minimo viene calcolato in modo distribuito e iterativo.

Ogni router possiede le informazioni dei suoi adiacenti. Tramite un processo iterativo calcola il percorso migliore.

Questi sono algoritmi Distance-Vector

Possono anche essere classificati come

- Statici

Le tabelle che determinano i percorsi cambiano raramente (intervento umano)

- Dinamici

Gli stradamenti vengono determinati in base al volume del traffico.

Possono essere eseguiti al cambio della topologia o costo di un arco

Il terzo metodo per catalogarli è determinare se sono sensibili o no al carico
(se un arco ha un costo alto verrà ignorato o no)

Link-State

Ogni costo e tutta la topologia sono noti all'algoritmo (Ad esempio OSPF o Dijkstra/Prim)

Distance-Vector

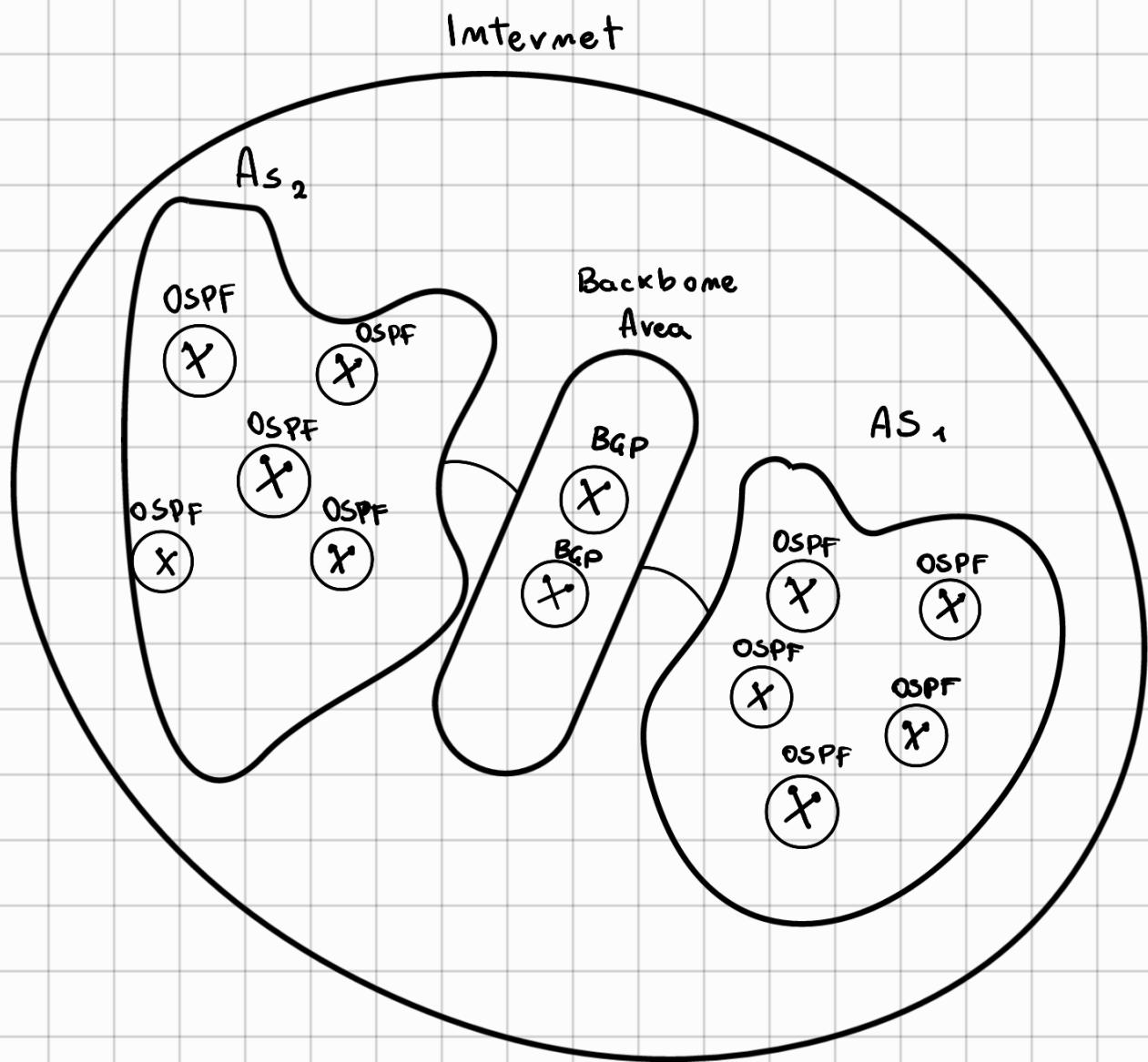
Ciascun nodo riceve parte delle informazioni dai suoi vicini direttamente connessi. Otenute le informazioni si ottiene il risultato poi iterativamente si ricevono altre informazioni e si effettua di nuovo il calcolo termina quando non arrivano altre informazioni.

Il costo minimo è associato alla formula di Bellman-Ford (iterativa)

$$d_x(y) = \min_v \{ c(x, v) + d_v(v) \}$$

Sistemi Autonomi (AS)

Sono gruppi di router sotto lo stesso controllo amministrativo (rete di un ISP)



OSPF

È un protocollo link-state che utilizza il flooding per informare tutti sullo stato e costo dei nodi e Dijkstra per il percorso minimo.

Ora viene maggiormente usato il protocollo RIP e RIP 2

Protocollo RIP (Routing Information Protocol)

È un protocollo di tipo Distance-Vector e ogni 30 secondi invia la sua tabella di routing ai router vicini

Quando un percorso viene tolto dalla tabella di routing gli altri router impiegano 180 sec per taggarlo come inutilizzabile e altri 120 per eliminarlo

le route sono specificate in base all'ip di destinazione e al numero di hop

Indirizzamento tra ISP

Per gestire l'indirizzamento tra diverse AS viene usato il BGP (Border Gateway Protocol)

BGP permette di:

- Ottenere informazioni su come raggiungere le sottoreti. (Ogni sottorete può comunicare la sua esistenza su internet)
- Determinare percorsi ottimi verso le sottoreti

BGP Distribuzione informazioni

Due router che vogliono scambiarsi informazioni si chiamano "Peer", prima di farlo devono stabilire una commessione.

Successivamente iniziamo a condividere quello che conosciamo

BGP Selezione rotte migliori

Vengono scelte in base a:

- Prefisso più lungo
- AS-PATH più corto → Su due rotte verso una AS verrà scelta quella con costo minore
- Politiche stabilite dalla rete → Politiche degli amministratori di ignorare una determinata rotta

131.175.23.1 /22 Trouare rete di appartenenza

↓ Trasformiamo in binario (anche la maschera)

10000011.10101111.00010111.00000001 Eseguiamo l'AND bit a bit

11111111.11111111.11111100.00000000

↓

10000011.10101111.00010100.00000000

131.175.20.0 => Indirizzo di rete

Dire se questi indirizzi sono hosts o reti

A) 192.168.72.0 /18

B) 192.168.72.0 /21

A) Host

11000000.10101000.01001000.00000000

11111111.11111111.11000000.00000000

192.168.64.0 /18 quindi è un host di questa rete

B) Rete

11000000.10101000.01001000.00000000

11111111.11111111.11110000.00000000

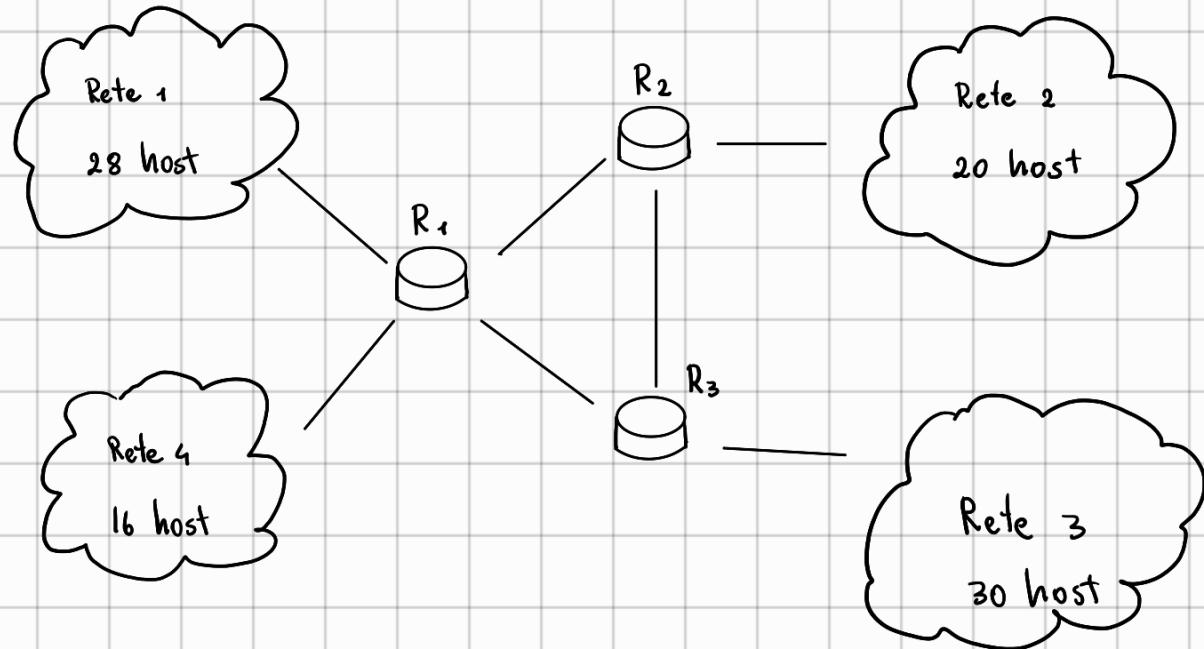
192.168.72.0 /21 l'ind corrisponde a quello di rete

Determinare Netmask minima per una rete da 31 host

$$2^6 - 2 = 64 - 2 = 62 \quad 31 < 62 \quad \checkmark$$

$$\text{Netmask } 32 - 6 = 26 \rightarrow /26$$

Submetting



193.205.92.0 /24

$$32 - 27 = 5 \quad 2^5 = 32 \quad 30 \text{ host + rete = broad}$$

Rete 3 /27

rete 193.205.92.0

host // // // .1 - 30

broad 193.205.92.31

Rete 2 /27

192.168.92.64

//.//.//.65 - 94

//.//.//.95

Rete 1 /27

rete 193.205.92.32

host //.//.//.33 - 62

broad //.//.//.63

Rete 4 /27

192.168.92.86

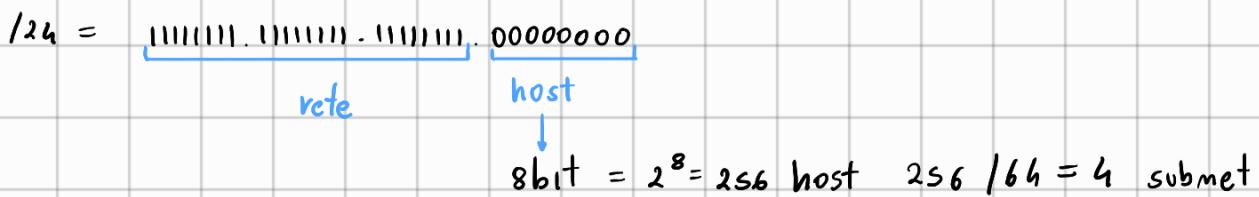
//.//.//.87 - 126

//.//.//.127

Router da fare

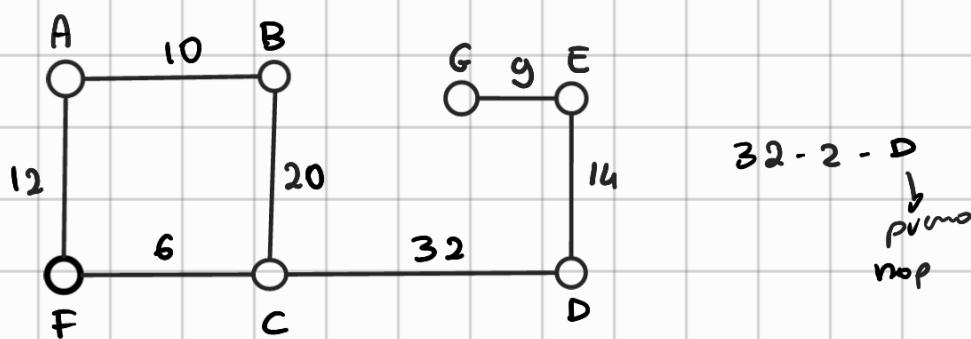
Data la Lan 192.168.0.0 /24 , dire quante sottoreti da 62 host
possono essere create

Per orgm. vete 62 + 2 host = 126

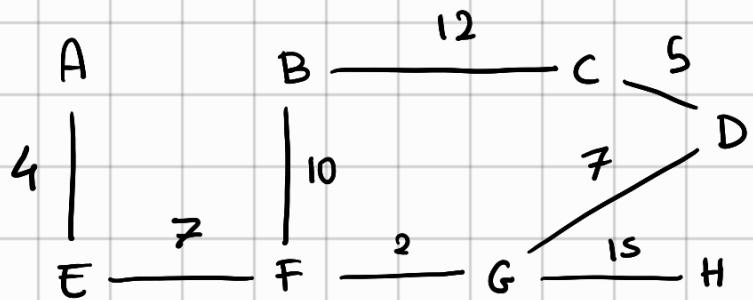


Rete 1:	Rete 2	Rete 3	Rete 4
Net 192.168.0.0 /26	192.168.0.64 /26	192.168.0.128 /26	192.168.0.192 /26
host 192.168.0.1 - 62	192.168.0.65 - 126	11 . 11 . 11 . 129 - 190	192.168.0.193 - 254
broad 192.168.0.63	192.168.0.127	11 . 11 . 11 . 191	192.168.0.255

Protocollo Rip



A	B	C	D	E	F	G
10 - 1 - /	10 - 1 - /	20 - 1 - /	14 - 1 - /	9 - 1 - /	12 - 1 - /	9 - 1 - /
12 - 1 - /	20 - 1 - /	6 - 1 - /	32 - 1 - /	14 - 1 - /	6 - 1 - /	14 - 2 - E
20 - 2 - B	12 - 2 - A	32 - 1 - /	9 - 2 - E	32 - 2 - D	10 - 2 - A	32 - 3 - E
6 - 2 - F	6 - 2 - C	10 - 2 - B	20 - 2 - C	20 - 3 - D	32 - 2 - C	20 - 4 - E
32 - 3 - B	32 - 2 - C	12 - 2 - F	6 - 2 - C	6 - 3 - D	20 - 2 - C	6 - 4 - E
14 - 4 - B	14 - 3 - C	14 - 2 - D	10 - 3 - C	10 - 4 - D	14 - 3 - C	10 - 5 - E
9 - 5 - B	9 - 4 - C	9 - 3 - D	12 - 3 - F	12 - 4 - D	9 - 4 - C	12 - 5 - E



A	B	C	D	E	F	G	H
4 - 1	12 - 1	5 - 1	7 - 1	4 - 1	10 - 1	15 - 1	15 - 1
7 - 2 - E	10 - 1	12 - 1	5 - 1	7 - 1	2 - 1	2 - 1	2 - 2 - G
10 - 3 - E	6 - 2 - C	7 - 2 - D	2 - 2 - G	10 - 2 - F	7 - 1	7 - 1	7 - 2 - G
2 - 3 - E	7 - 2 - F	10 - 2 - B	15 - 2 - G	2 - 2 - F	12 - 2 - C	5 - 2 - O	5 - 3 - G
15 - 4 - E	2 - 2 - F	2 - 3 - D	12 - 2 - C	15 - 3 - F	7 - 2 - G	10 - 2 - F	7 - 3 - G
12 - h - E	4 - 3 - F	15 - 3 - D	10 - 3 - C	12 - 3 - F	15 - 2 - G	7 - 2 - E	10 - 3 - G
7 - 4 - E	15 - 3 - F	7 - 3 - B	7 - 3 - G	7 - 3 - F	4 - 2 - E	12 - 3 - D	4 - 4 - G
5 - 5 - E	7 - 3 - F	4 - 4 - B	4 - 4 - G	5 - 4 - F	5 - 3 - G	4 - 3 - F	12 - 4 - G

Link State

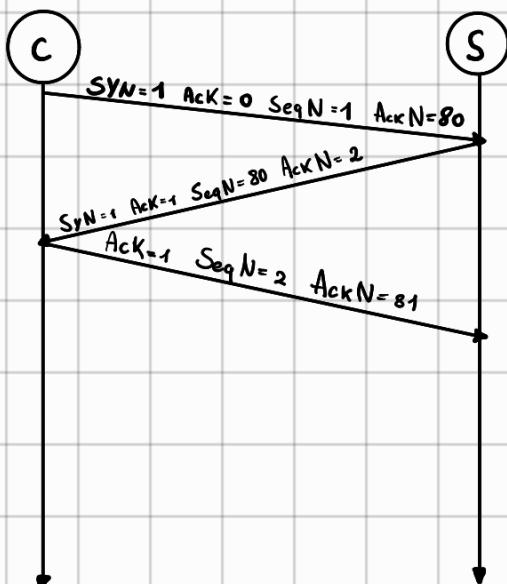
12 - E \rightsquigarrow ultimo
hop

PASSO	A	B	C	D	E	F
0	∞	∞	∞	∞	\checkmark	∞
1	∞	∞	2 - E	3 - E		12 - E
2	∞	10 - C	\checkmark	3 - E		12 - E
3	∞	1 - D		\checkmark		11 - D
4	8 - B	\checkmark				11 - D
5	\checkmark				10 - A	
6					\checkmark	

Router	Next hop	Costo
A	B	8
B	D	4
C	E	2
D	E	3
E	/	/
F	A	10

Comessioni Telnet

Triple Handshake SYN , SYN-Ack , ACK



Seq N = 1

Ack N = 80

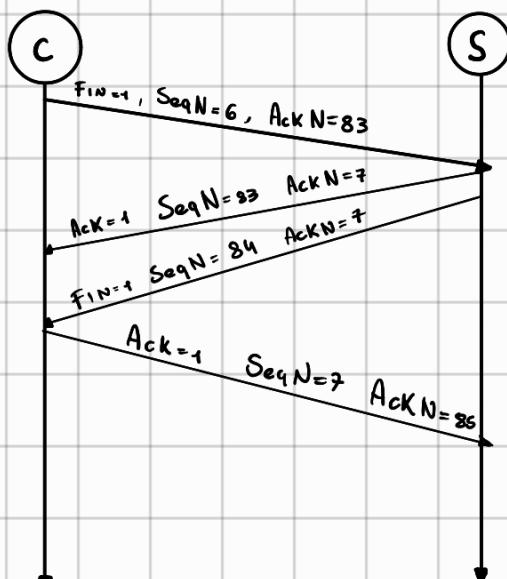
Aprire connessione

con 3-Handshake

AckN : Quando c'è uno zigzag

Il SeqN e AckN si scambiano e
l'ackN aumenta di 1

Se bisogna mandare un messaggio si aggiunge nel campo
data



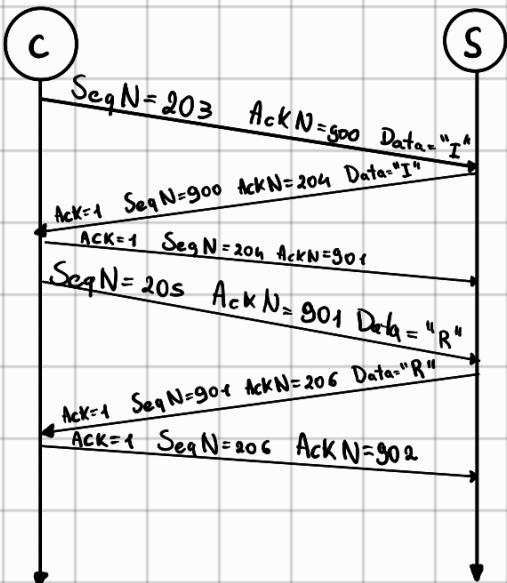
Seq N₁ = 6 Chiusura

Seq N₂ = 83 Connessione

Quando vanno tutti e

due della stessa parte

SeqN e AckN non si scambiano
ma il SeqN aumenta di 1



Seq N = 203
Ack N = 900

Inviare "I" e
poi "R" com
connessione già aperta

- 1) Aprire comm
- 2) Invio Singolarmente "IRS"
- 3) Chiudere comm

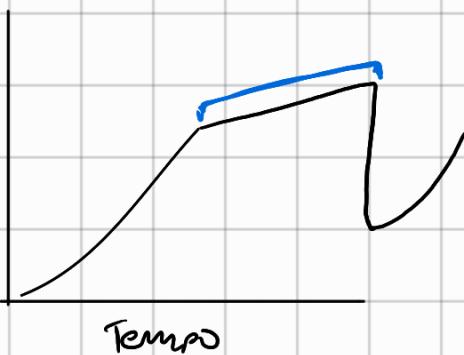
Seq N = 1
Seq N - 2 = 80

TCP Reno Must Know

- 1) Avvi lenti
- 2) Controlli di congestione
- 3) Ack tripli duplicati
- 4) Timeout

1) Intervalli di Avvio lento TCP
Si riconosce da una curva esponenziale

2) Intervalli di tempo del controllo di congestione
Si riconoscono dalle lineerette che salgono



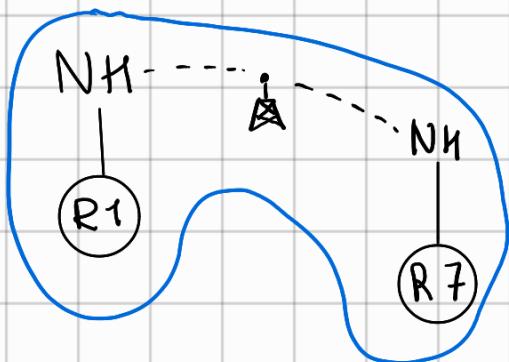
3) Dopo il tempo x avviene un Ack tripla-duplicato o Timeout
Si riconosce quando si ferma ad un certo punto e quindi c'è un Ack Tripla-duplicato

(Se va ad 1 e dopo c'è un avvio lento o un Timeout)

4) Dopo il tempo x Ack T-D o Timeout
Se riparte un controllo di gestione c'è un Ack T-D

5) Threshold

Submitting



Quando c'è un ripetitore la rete si fonde come vetro
unica

Wireshark

Se chiede il MAC di un disp controllare ARP o DNS prima
Se chiede commessione sicura filtrare per 443 o TLS

Tcp

Se RTT cercare iRTT in SYN/ACK Analysis

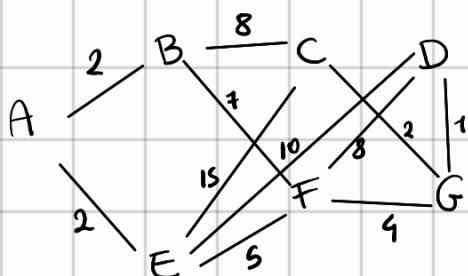
WS = Window Scale

Wm = Window Size

HTTP

Payload dati = file data

Link-State

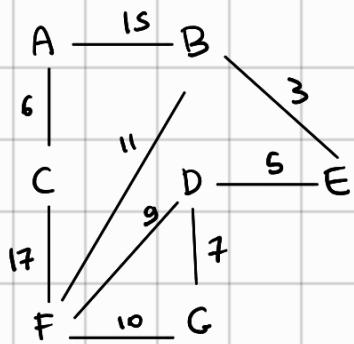


Ogni volta che scopro un nuovo modo aggiungo il valore del percorso dalla radice

P	A	B	C	D	E	F	G
0	✓	∞	∞	∞	∞	∞	∞
1	2.A	∞	∞	2.A	∞	∞	
2	✓	10.B	∞	2.A	9.F	∞	
3		10.B	12.E	✓	7.E	∞	
4		10.B	12.E		✓	11.F	
5			✓	12.E		11.F	
6				12.E		✓	
7					✓		

R	NH	Costo
A	/	/
B	A	2
C	B	10
D	E	12
E	A	2
F	E	7
G	F	11

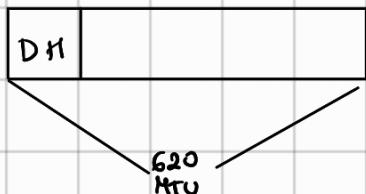
RIP



A	B	C	D	E	F	G	
15-1-1	15-1-1	6-1-1	3-1-1	5-1-1	11-1-1	7-1-1	
6-1-1	3-1-1	17-1-1	5-1-1	3-1-1	9-1-1	10-1-1	
3-2-B	11-1-1	15-2-A	7-1-1	7-2-D	10-1-1	8-2-D	
11-2-B	9-2-F	10-2-F	10-2-C	9-2-D	17-1-1	8-2-D	
17-2-C	17-2-F	11-2-F	11-2-F	15-2-B	6-2-C	17-2-F	
10-3-C	10-2-G	8-2-F	17-2-F	5-3-G	15-2-B	10-3-D	
13-3-C	5-2-E	3 3 F	3-2-E	17 3 G	3-2-B	11-3-D	
5-3-E	6-2-A	7 3 F	6 3 F		5-2-D	3-3-E	
8-3-B		5 3 F			7-2-D	6-3-F	
10-3-B	7-3-F					15-3-F	

Frammentazione

Data : 1480



ID: 777
Offset: 0 Il primo indice dell'intervalle inviato diviso 8
Flag: 0

TCP header : 20 byte

Come viene frammentato ?

$$\boxed{\text{Header}} \quad 600 = \text{MTU} - \text{TCP header} = 620 - 20$$

ID: 777

Offset: 0

MF Flag: 1 Indica se c'è un pacchetto successivo

$0 - 599$

$\boxed{\text{Header}} \quad 600$

ID: 777

$$\text{Offset} : 600 / 8 = 75$$

MF Flag: 1

$600 - 1199$

$\boxed{\text{Header}} \quad 280$

ID: 777

$$\text{Offset} : 1200 / 8 = 150$$

MF Flag: 0

$1200 - 1479$

Pacc IP 5265 byte MTU = 1500

Seq	ID	TOT	DF	MF	OFF
0	126	5265	0	0	0

Seq	ID	Pay	DF	MF	OFF
0	126	1480 - MTU - 20 (FCS)	0	1	0

1	126	1480	0	1	148018 = 18S
---	-----	------	---	---	-----------------

2	126	1480	0	1	370
---	-----	------	---	---	-----

3	126	825	0	0	555
---	-----	-----	---	---	-----

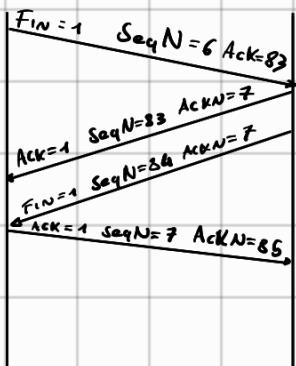
Aprivre connessione 3 wh



Seq N = 1

Ack N = 80

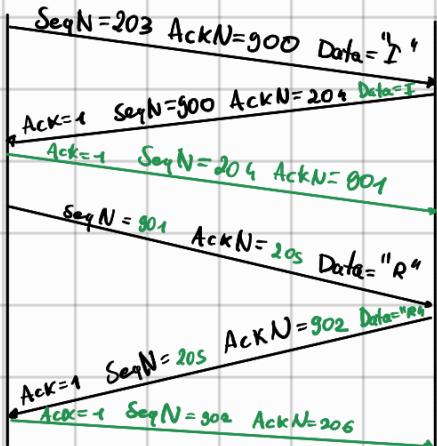
Chiudere connessione



Seq N - 1 = 6

Seq N - 2 = 83

Mandare "I" e poi "R"



Seq N = 203

Ack N = 900

A prive Comm

SeqN=1

Inviare sing "IRS"

SeqN-2=80

Chiudere Com

Syn=1 SeqN=1 AckN=80

Syn=1 Ack=1 SeqN=80 AckN=2

Ack=1 SeqN=2 AckN=81 Data="I"

Ack=1 Seq=81 AckN=3 Data="I"

Ack=1 Seq=3 AckN=82

SeqN=4 AckN=82 Data="R"

Ack=1 SeqN=82 AckN=5 Data="R"

Ack=1 SeqN=5 AckN=83

Ack=1 SeqN=6 AckN=83 Data="S"

Ack=1 SeqN=83 AckN=7 Data="S"

Ack=7 SeqN=84 Ack=85

FIN=1 SeqN=8 Ack=84

Ack=1 SeqN=84 AckN=9

FIN=1 SeqN=85 AckN=9

Ack=1 SeqN=9 Ack N=86

A pertura

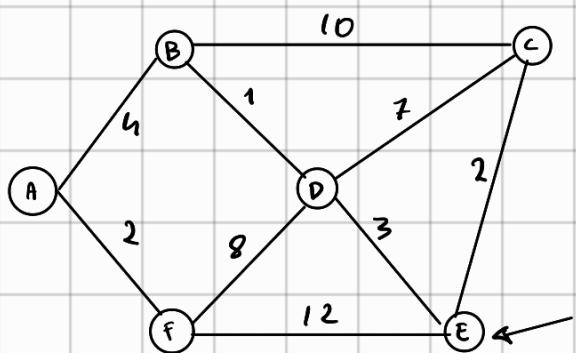
I

R

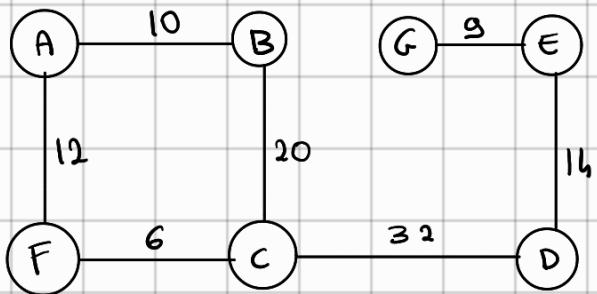
S

FIN

Link - State

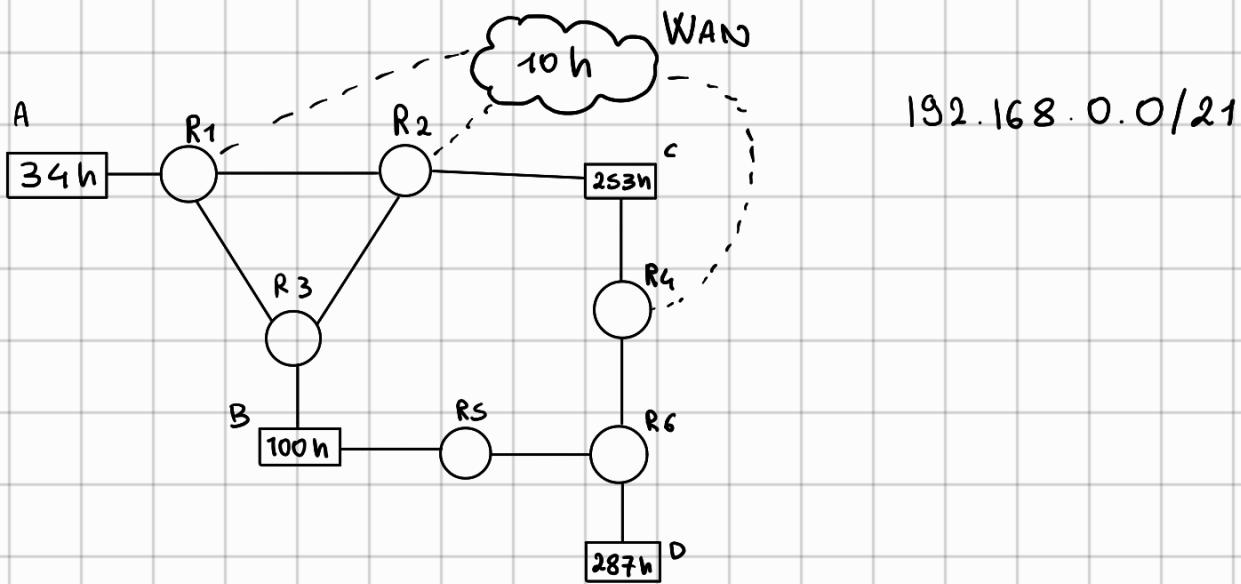


	A	B	C	D	E	F	R	NH	Costo
1	∞	∞	$2-E$	$3-E$	✓	$12-E$	A	B	8
2	∞	$12-C$	✓	$3-E$	✓	$12-E$	B	D	4
3	∞	$4-D$	✓	✓	✓	$12-E$	C	E	2
4	$8-B$	✓	✓	✓	✓	$12-E$	D	E	3
5	✓	✓	✓	✓	✓	$10-A$	E	/	/
6	✓	✓	✓	✓	✓	✓	F	A	10



A B C D E F G

10-1	10-1	6-1	32-1	14-1	6-1	9-1
12-1	20-1	32-1	14-1	9-1	12-1	142E
202B	122A	20-1	92E	322D	102B	323D
62F	62C	102B	62C	63D	322C	64E
323B	322C	142D	202C	103D	202C	204E
144B	143C	122F	103C	104D	143C	104E
95B	94C	93D	123C	124D	94C	124E



D /23

R 192.168.0.0

H // .0.1 - // .1.254

B 192.168.1.255

C /23

R 192.168.2.0

H // .2.1 - // .3.254

B 192.168.3.255

B /25

R 192.168.4.0

H // .4.1 - // .4.126

B 192.168.4.127

A /26

R 192.168.4.128

H // .4.129 - // .4.190

B 192.168.4.191

WAN /28

R 192.168.4.192

H // .4.193 - // .4.206

B 192.168.4.207

R1-R2 /30

R 192.168.4.208

H // .209 - // .210

B 192.168.4.211

R1-R3 /30

R // .4.212

H // .213 - // .214

B // .4.215

R2-R3 /30

R // .216

H // .217 - // .218

B // .219

R4-R6 /30

R // .220

H // .221 - // .222

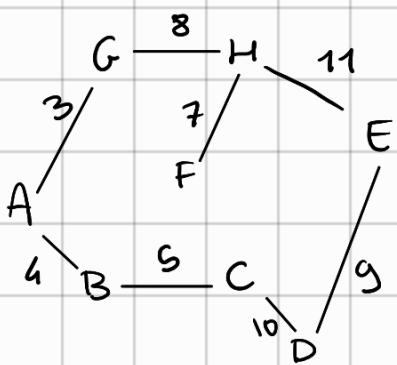
B // .223

R5-R6 /30

R // .224

H // .225 - // .226

B // .227

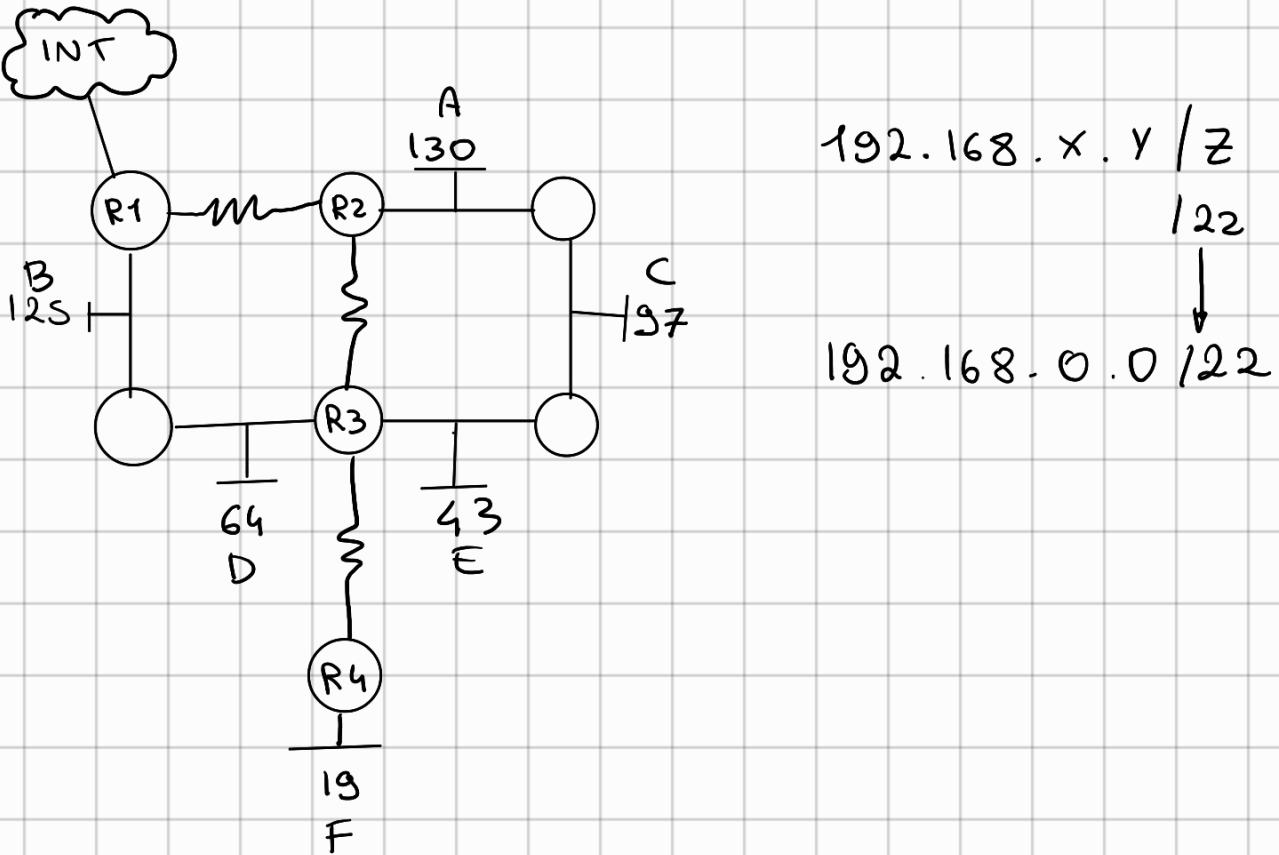


A B C D E F G H

3-1	4-1	5-1	10-1	11-1	7-1	3-1	8-1
4-1	5-1	10-1	9-1	9-1	1124	8-1	11-1
52B	32A	42B	112E	82H	82H	42A	7-1
82C	102C	92B	62E	72H	83H	112H	32G
73G	83A	33B	43C	102D	33H	72H	92E
103B	93C	113C	83E	53D	44H	53A	43G
113G	74A	84B	103E	33G	104H	93H	103E
94G	114A	75B	34C	44D	55H	104A	54G

Passo	A	B	C	D	E	F	G
1	✓	2	∞	∞	∞	∞	5
2	✓	✓	5 B	∞	∞	∞	5
3	✓	✓	5 B	∞	8 G	g c	✓
4	✓	✓	✓	7 C	8 G	7 C	✓
5	✓	✓	✓	✓	8 G	7 C	✓
6	✓	✓	✓	✓	8 G	✓	✓
7	✓	✓	✓	✓	✓	✓	✓

R	NH	C
A	/	/
B	A	2
C	B	5
D	C	7
E	G	8
F	C	7
G	A	5



A 124

R 192.168.0.0

H .0.1 - .0.254

B 192.168.0.255

B 124

R 192.168.1.0

H 1.1 - 1.254

B 192.168.1.255

C 125

R 192.168.2.0

H .2.1 - .2.126

B 192.168.2.127

D 125

R 192.168.2.128

H .2.129 - .2.254

B 192.168.2.255

E 126

R 192.168.3.0

H .3.1 - .3.62

B 192.168.3.63

F 127

R 192.168.3.64

H .3.65 - .3.94

B 192.168.3.95

R1-R2 130

R 192.168.3.96

H 3.87 - 3.98

B 192.168.3.99

R2-R3 130

R 192.168.3.100

H .3.101 - 3.102

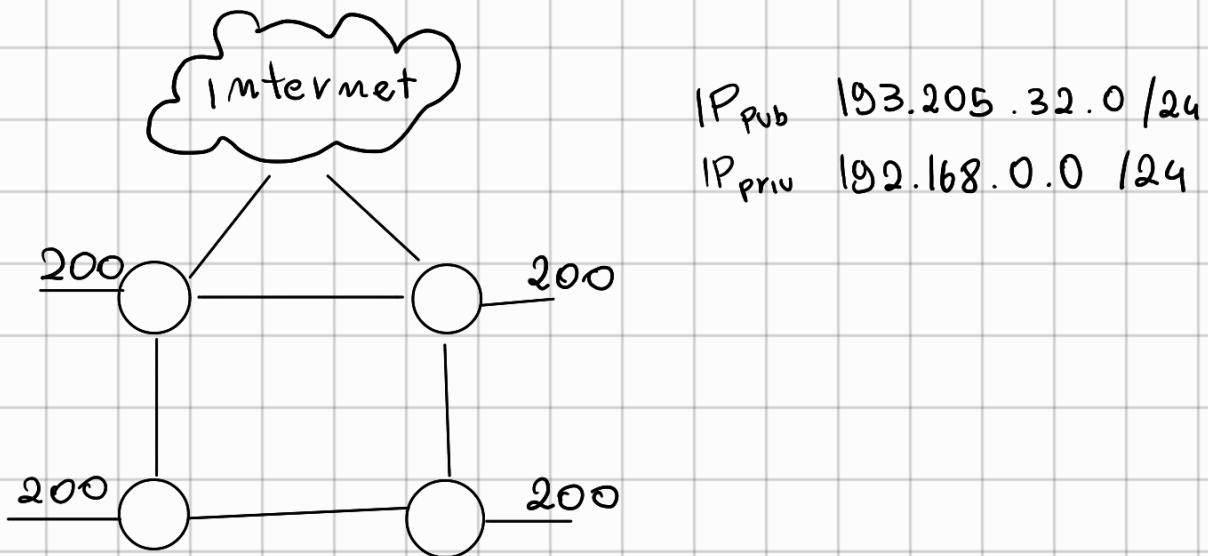
B 192.168.3.103

R3-R4 130

R 192.168.3.104

H .3.105 - .3.106

B 192.168.3.107



Frammentazione

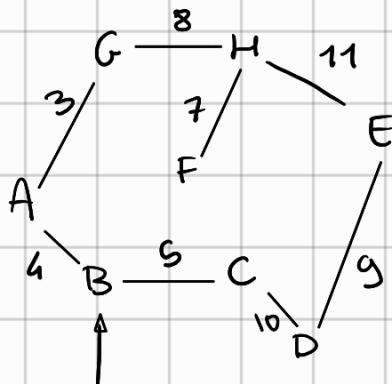
Data = 6595 byte ID = 126 TCP header = 20 bytes
 MTU = 1500 byte

Seq	ID	Payload	DF	MF	offset
0	126	H + 1480 (0 → 1479)	0	1	0
1	126	H + 1480 (1480 → 2959)	0	1	$(1480 / 8) = 185$
2	126	H + 1480 (2960 → 4439)	0	1	$(2960 / 8) = 370$
3	126	H + 1480 (4440 - SG19)	0	1	$(4440 / 8) = 555$
4	126	H + 676 (SG20 - 6595)	0	1	$(5820 / 8) = 740$
		$ \begin{array}{r} S \\ 6 \\ 5 \\ 8 \\ 5 \\ - \\ SG19 \\ \hline 0676 \end{array} $			

Data = 6595 byte ID = 126 TCP header = 20 bytes
 MTU = 1500 byte

Seq	ID	Payload	DF	MF	Offset
0	126	H + 1480 (0 - 1479)	0	1	0
1	126	H + 1480 (1480 - 2969)	0	1	185
2	126	H + 1480 (2960 - 4439)	0	1	370
3	126	H + 1480 (4440 - 5919)	0	1	555
4	126	H + 676 (5920 - 6595)	0	0	740

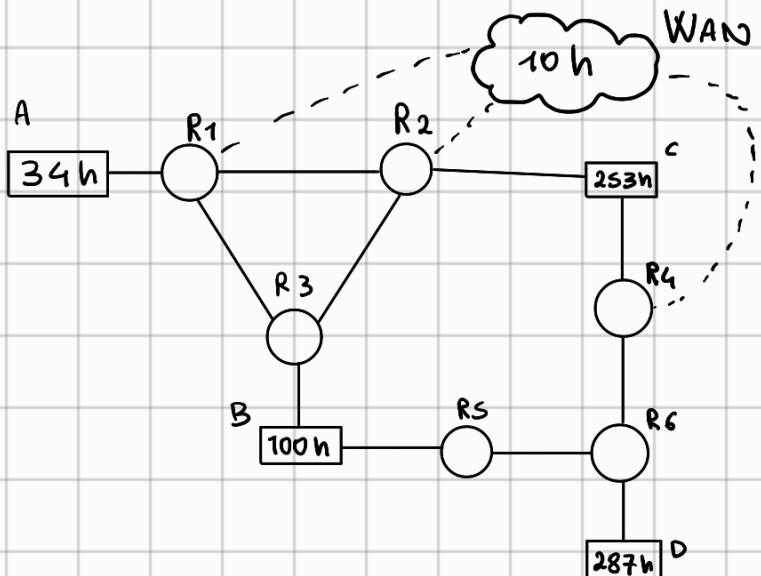
$$\begin{array}{r}
 \overbrace{1480}^8 \\
 8 \\
 \hline
 \overbrace{680}^{185} \\
 64 \\
 \hline
 40 \\
 40 \\
 \hline
 0
 \end{array}$$



R NH C
 A B 4
 B --
 C B S
 D C IS

R NK C
 E D 24
 F U 22
 G B 7
 H G IS

Passo	A	B	C	D	E	F	G	H
1	✓ - B	✓	S - B	∞	∞	∞	∞	∞
2	✓	✓	✓ - B	∞	∞	∞	7 - B	∞
3	✓	✓	✓	IS - C	∞	∞	7 - B	∞
4	✓	✓	✓	✓ - C	∞	∞	✓	IS - G
5	✓	✓	✓	✓	24 - D	∞	✓	✓ - G
6	✓	✓	✓	✓	24 - D	22 - H	✓	✓
7	✓	✓	✓	✓	24 - D	✓	✓	✓
8	✓	✓	✓	✓	✓	✓	✓	✓



$192.168.x.y/2$
 $192.168.0.0/21$
 $S12 + S12 + 16 + 64 + 128$
 $h + h + h + h + h = 1282$
 $2048 \rightarrow 121$

D /23 $S12h$
 R $192.168.0.0$
 H $0.1 - 1.25h$
 B $192.168.1.255$

C /23 $S12h$
 R $192.168.2.0$
 H $2.1 - 3.25h$
 B $192.168.3.255$

B /25 $128h$
 R $192.168.h.0$
 H $h.1 - h.126$
 B $192.168.h.127$

A /26 $64h$
 R $192.168.h.128$
 H $h.129 - h.190$
 B $192.168.h.191$

WAN /28
 R $192.168.h.192$
 H $h.193 - h.206$
 B $192.168.h.207$