Slide del corso di Reti di Calcolatori tenuto dal prof . Agostino Poggi dell'Università di Parma.
Traduzione a cura di Bacchini Alessandro, Biasion Francesco e Davoli Luca.
Il prof. Poggi **non** è responsabile del contenuto e della traduzione di queste slide.
Le slide sono fornite "così come sono", senza garanzia di completa conformità agli originali, inoltre, i traduttori non si assumono alcuna responsabilità per errori di traduzione e interpretazione.

Reti di Calcolatori

Internetworking (interlavoro tra reti differenti)

Internetworking

- Ci sono molte tecnologie differenti di LAN e WAN
- Nel mondo reale, i computer sono connessi con molte tecnologie differenti
- Ogni sistema che si estende su larga scale deve gestire svariate tecnologie differenti
- I telefoni sono utili perché tutti i telefoni possono raggiungere qualsiasi altro telefono
- Servizi universali tra computer incrementano grandemente l'utilità di ogni computer
- Fornire servizi universali richiede di interconnettere le reti che impiegano tecnologie differenti

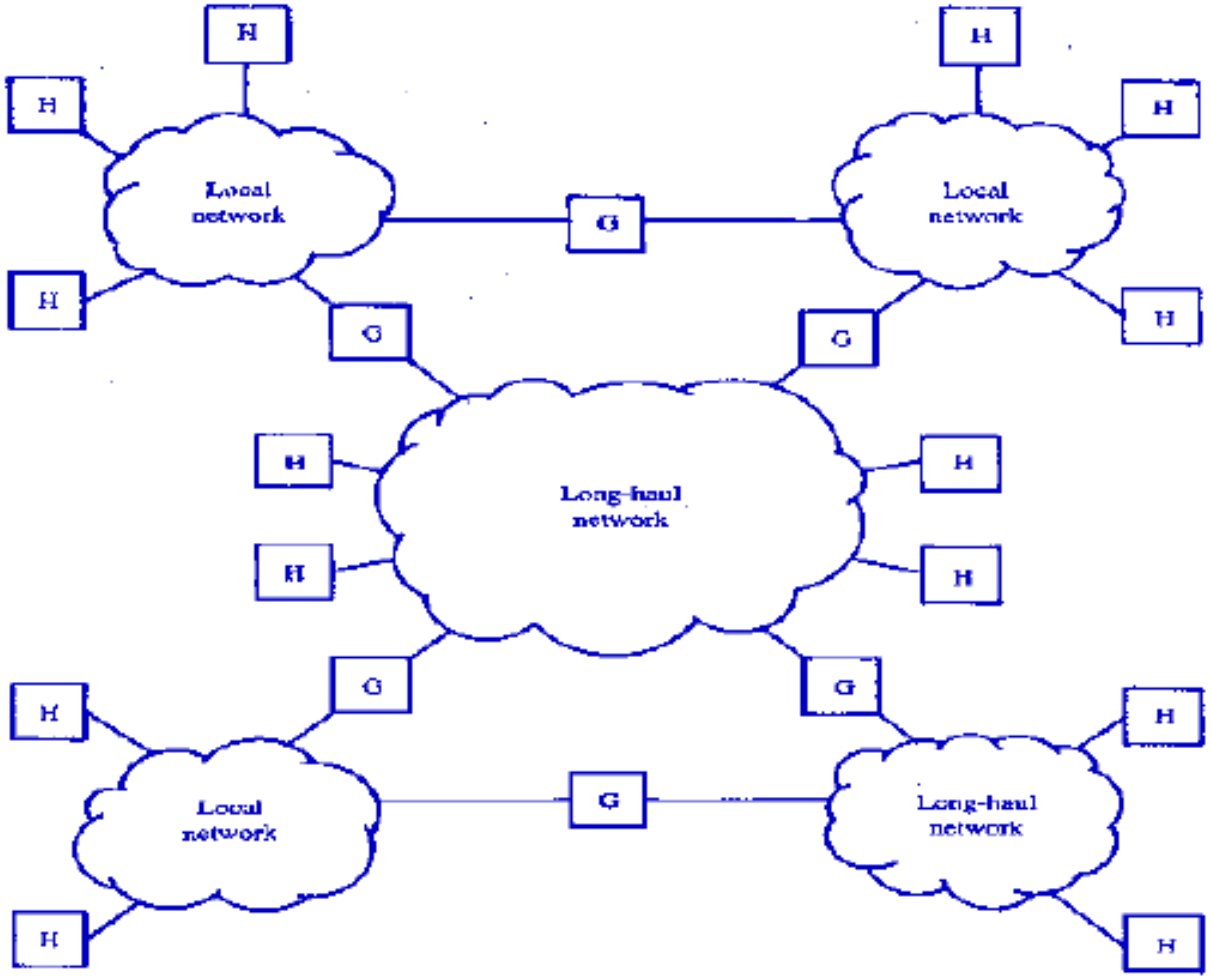
Internetworking

- Prevede un collegamento tra le reti
- Richiede un controllo fisico di collegamento
- Fornisce trasporto e distribuzione di dati tra processi su reti diverse
- Fornisce un servizio di account che tiene traccia dell'uso delle varie reti e gateway e mantiene le informazioni di stato

Internetworking

- Internetworking è uno schema per interconnettere più reti con tecnologie differenti
- Usano sia hardware che software
  - L'hardware extra è posizionato tra le reti (è l'interconnessione tra le 2 reti)
  - Il software è su ogni computer connesso
- Un sistema di reti interconnesse è chiamato un internetwork o un internet

Internetworking



Routers

- Un internet è composto da una quantità arbitraria di reti interconnesse tramite router (gateway)
- Un router è un componente hardware usato per interconnettere reti
  - Ha interfacce su multiple reti
  - Reindirizza pacchetti tra le reti
  - Trasforma i pacchetti per adattarli agli standard di ogni rete

Routers

- Sarebbe possibile, in linea teorica, interconnettere tutte le reti di un'organizzazione con un singolo router
- La maggior parte delle organizzazioni vari router
  - Ogni router ha una capacità finita
  - Un singolo router non può gestire tutto il traffico dell'intera organizzazione
- Siccome la tecnologia di internetworking può automaticamente aggirare i componenti difettosi
  - Usando molteplici router si incrementa l'affidabilità

Una rete virtuale

- I software di internetworking generano una singola rete virtuale completamente separata dalle differenti reti fisiche
  - Uno schema di indirizzamento universale
  - Servizi universali
- Tutti i dettagli delle reti fisiche sono nascosti agli utenti ed alle applicazioni
- Esempi
  - TCP/IP
  - IPX
  - VINES
  - AppleTalk

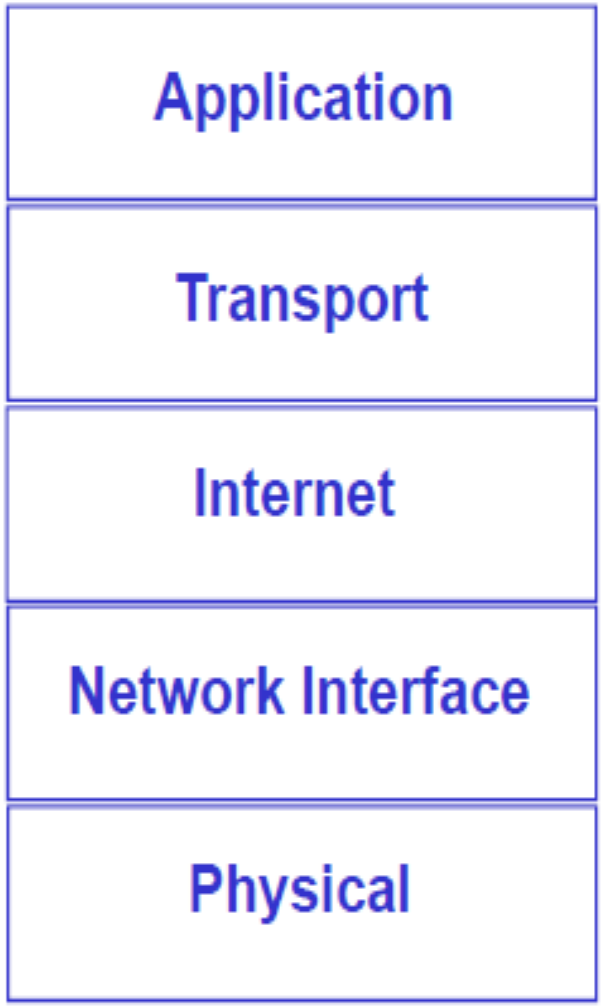
Una suite di protocolli per l'internetworking

- Il TCP/IP Internet Protocol, o semplicemente TCP/IP, è l'insieme di protocolli di internetworking maggiormente utilizzato
  - Primo insieme di protocolli di internetworking
  - Prima implementazione nel 1970 (ARPAnet) con 5 nodi (UCLA, Standford University, UC Santa Barbara, University of Utah e BBN) ed una velocità iniziale di 50 kbps
  - Indipendente dal venditore e dalla piattaforma
  - Servizi sia connectionless che connection-oriented
- Il concetto di Internet è stato sviluppato in congiunzione al TCP/IP

Tasso di diffusione di Internet

- 1977: 111 hosts on Internet
- 1981: 213 hosts
- 1983: 562 hosts
- 1984: 1,000 hosts
- 1986: 5,000 hosts
- 1987: 10,000 hosts
- 1989: 100,000 hosts
- 1992: 1,000,000 hosts
- 2001: 150 – 175 million hosts
- 2002: over 200 million hosts
- By 2010, about 80% of the planet will be on the Internet

Strati TCP/IP



(5) Corrisponde ai livelli ISO 6 e 7 ed è utilizzato per la comunicazione tra applicazioni

(4) Corrisponde al livello ISO 4 e fornisce consegna affidabile dei dati

(3) Definisce un formato uniforme per l'indirizzamento dei pacchetti attraverso reti con tecnologie differenti e regole per l'indirizzamento dei pacchetti nei router

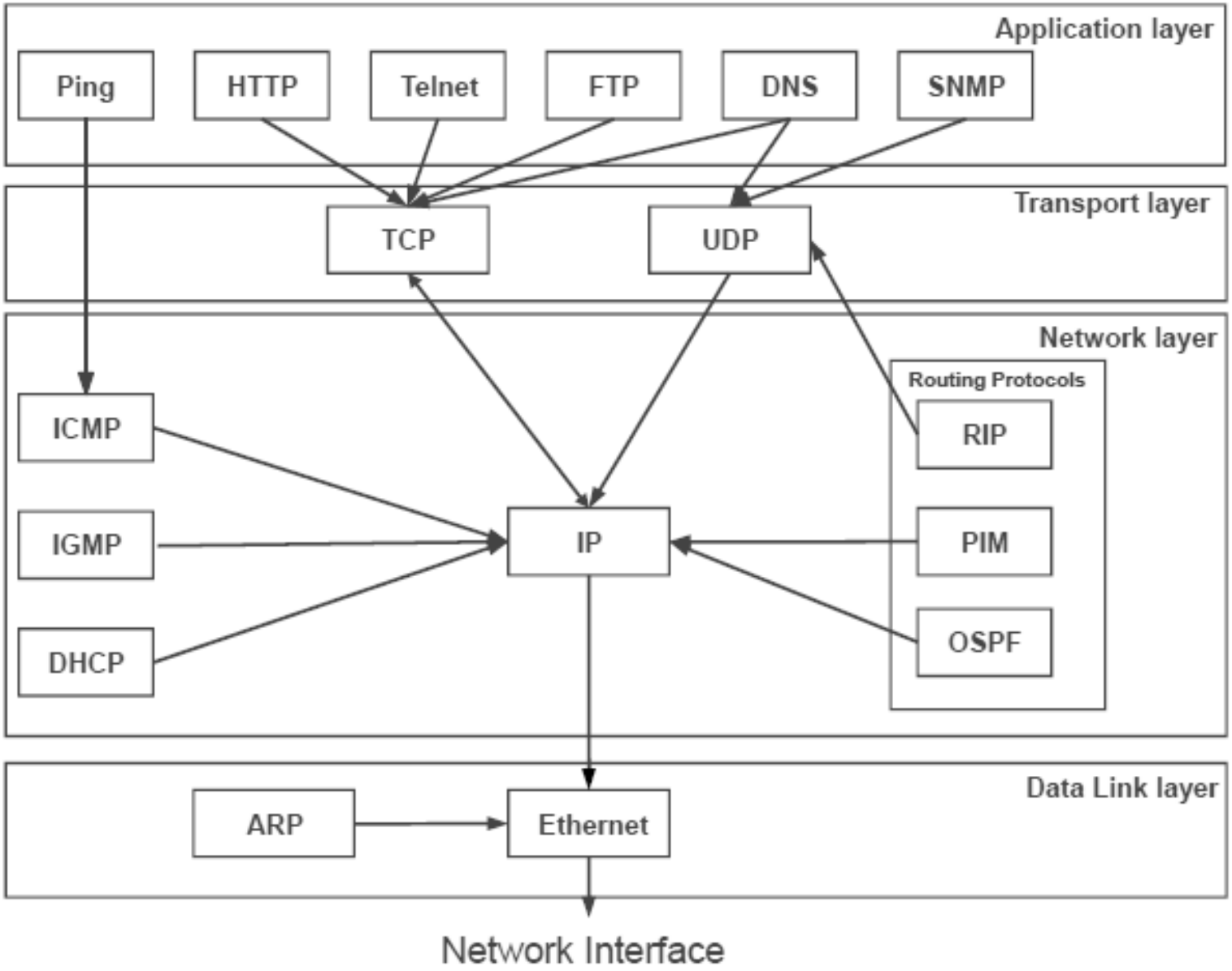
(2) Corrisponde al livello ISO 2 e definisce formati per codificare pacchetti in frame hardware

(1) Corrisponde al livello ISO 1 e definisce l'hardware di base delle reti

Host e router

- Un computer host o semplicemente host è un qualsiasi sistema connesso ad internet che esegue applicazioni
- Gli host possono essere supercomputer o piccoli dispositivi
- TCP/IP permette ad ogni coppia di host su internet di comunicare
- Sia gli host che i router hanno stack TCP/IP
  - Gli host di solito hanno una sola interfaccia e non reindirizzano pacchetti
  - I router non necessitano del livello 5 per le applicazioni

Protocolli TCP/IP



Indirizzi TCP/IP

- L’indirizzamento nel TCP/IP è specificato dall’Internet Protocol (IP)
- Ad ogni host è assegnato un numero a 32 bit
  - Chiamato indirizzo IP o indirizzo Internet
  - Univoco all’interno dell’intera rete

Gerarchia degli indirizzi IP

- Ogni indirizzo IP è diviso in un prefisso ed un suffisso
  - Il prefisso identifica la rete a cui il computer è connesso
  - Il suffisso identifica il computer all'interno di quella rete
- Il formato degli indirizzi rende il routing efficiente

Reti e numero di host

- Ad ogni rete all'interno di un internet TCP/IP è assegnato un numero di rete univoco
- Ad ogni host su una certa rete è assegnato un numero host o indirizzo host che è univoco all'interno di quella rete
- L'indirizzo IP degli host è la combinazione del numero della rete (prefisso) e dell'indirizzo dell'host (suffisso)

Proprietà degli indirizzi IP

- Il numero di rete è univoco
- Gli indirizzi degli host possono essere riutilizzati su reti differenti
- La combinazione del numero di rete (prefisso) e dell'indirizzo dell'host (suffisso) è univoca
  - Gli assegnamenti del numero di rete devono essere coordinati globalmente
  - Gli assegnamenti degli indirizzi degli host possono essere gestiti localmente

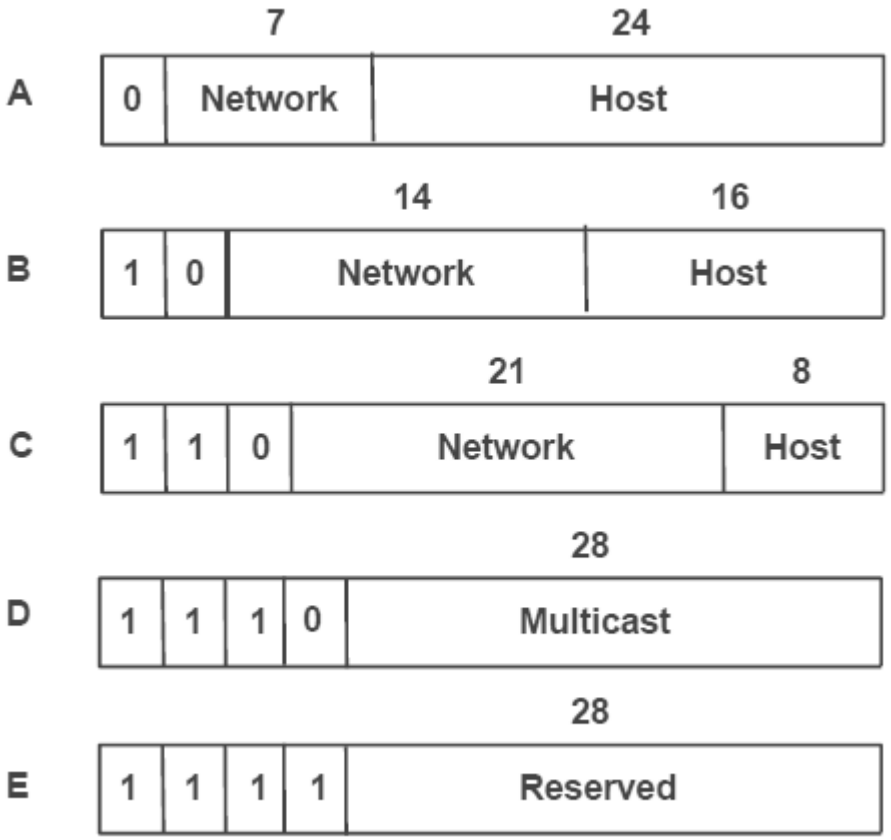
Formato dell'indirizzo IP

- I progettisti dell'IP scelsero indirizzi a 32 bit
- Allocati alcuni bit per il prefisso, altri per il suffisso
- Grandi prefissi, corti suffissi
  - Molte reti
  - Pochi host per rete
- Piccoli prefissi, grandi suffissi
  - Poche reti
  - Molti host per rete
- La varietà delle tecnologie necessita sia di reti piccole che grandi

Classi degli indirizzi IP

- I multipli formati di indirizzi IP permettono prefissi sia grandi che piccoli
- Ogni formato è chiamato classe di indirizzi
- La classe di un indirizzo è identificata dai primi 4 bit

Classi di indirizzi IP



Classi di indirizzi IP

- Le classi A, B e C sono classi primarie
  - Usate per l'indirizzamento di host ordinario
- Classe A
  - 128 ID di rete possibili (7 bit)
  - 4 milioni di ID di host per ID di rete (24 bit)
- Classe B
  - 16K ID di rete possibili (14 bit)
  - 64K ID host per ID di rete (16 bit)
- Classe C
  - 2 milioni di ID di rete possibili (21 bit)
  - 256 ID host per ID di rete (8 bit)

Classi di indirizzi IP

- La classe D è usata per il multicast, un formato limitato del broadcast
  - Gli host internet si uniscono ad un gruppo multicast
  - I pacchetti sono consegnati a tutti i membri del gruppo
  - I router gestiscono la consegna di un singolo pacchetto dalla sorgente ad ogni membro del gruppo multicast
  - Usata per mbone (multicast backbone)
- La classe E è riservata

Notazione decimale con punti

- Le classi A,B e C hanno una separazione tra prefisso e suffisso al confine del byte
- La notazione decimale a punti è una convenzione per rappresentare indirizzi internet a 32 bit in decimale
- Ogni byte dell'indirizzo è convertito in decimale e visualizzato separato da punti ("dots")

160.78.28.04

Notazione decimale con punti

- Netta separazione tra l'indirizzo della rete e l'indirizzo dell'host
- Le classi di indirizzo possono essere riconosciute dalla prima serie di numeri decimali

Class	Range of Values
A	0 through 127
B	128 through 191
C	192 through 223
D	224 through 239
E	240 through 255

Allocazione di indirizzi internet

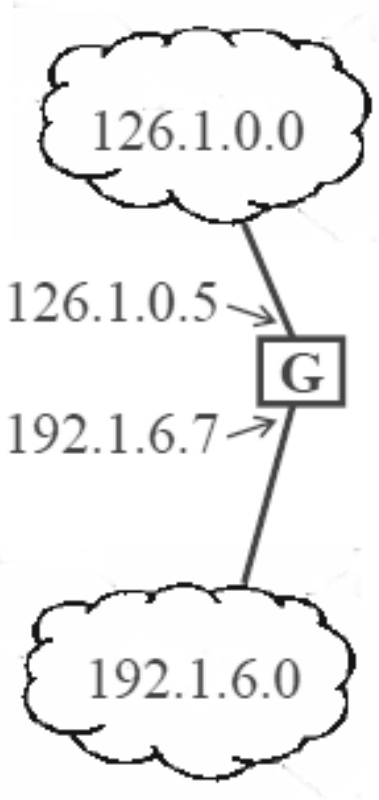
- Gli indirizzi su internet non sono usati in maniera efficiente
- Grandi organizzazioni non possono ottenere tutti gli indirizzi internet che necessitano
- Esempio: UPS necessita indirizzi per milioni di computer
- Soluzione
  - Creare internet private (intranet)
  - Allocare indirizzi per l'intero spazio di indirizzamento di 32 bit

Indirizzi IP speciali

Prefix	Suffix	Address Type	Purpose
All 0's	All 0's	Host	Host identification during bootstrap
-	All 0's	Network	Network identification
All 0's	-	Host	Host identification in the local network
-	All 1's	Broadcast	Broadcast to a specific network
-	All 0's	Berkeley Broadcast	Broadcast to a specific network
All 1's	All 1's	Broadcast	Broadcast in the local network
127	-	Loopback	Testing

Router è indirizzamenti IP

- I router hanno molteplici indirizzi IP
  - Uno per ogni interfaccia
- Gli indirizzi IP specificano un'interfaccia, o un punto di unione ad una rete, non un computer



Multi – Homed Hosts

- Gli host (che non reindirizzano i pacchetti) possono essere connessi a molteplici reti
- Può migliorare affidabilità e performance
- I multi-homed host hanno anche indirizzi IP multipli
  - Uno per ogni interfaccia

Consegna dei pacchetti agli indirizzi IP

- I software di computer e router utilizzano l'indirizzo IP di destinazione per inviare e gestire i pacchetti
- L'hardware fisico non comprende gli indirizzamenti IP
- Gli indirizzi IP nel passaggio successivo devono essere tradotti in indirizza hardware
- La traduzione degli indirizzi IP in indirizzi hardware è chiamata risoluzione dell'indirizzo (Address Resolution)

Tecniche di risoluzione degli indirizzi

- Table lookup
  - Le associazioni sono salvate in una tabella in memoria
  - Usata per WAN
- Close-form computation
  - Gli indirizzi hardware sono calcolati a partire dagli indirizzi IP usando operazioni booleane ed aritmetiche
  - Usato con reti configurabili
- Message exchange
  - I computer si scambiano messaggi attraverso la rete per risolvere gli indirizzi
  - Usato con hardware LAN ad indirizzo statico

Table lookup

- Tecniche di ricerca per la risoluzione di indirizzi
  - Ricerca sequenziale per piccole reti
  - Hashing o indirizzamento diretto per reti estese

IP Address	Hardware Address
160.78.28.1	0A:22:EE:82:32:90
160.78.28.2	0A:95:1C:32:45:1F
160.78.28.3	0A:41:3D:56:B2:FA
...	...

Close-form Computation

- Efficiente per reti con indirizzi configurabili
  - La porzione degli host dell'indirizzo IP può essere scelto per essere identico all'indirizzo hardware
  - Un indirizzo hardware di rete di classe C può essere calcolato con la funzione:

    hardware_address = ip_address & 0xFF

Message exchange

- Scambio di messaggi
  - Richiesta di specifici indirizzi IP
  - La risposta porta con sé indirizzi hardware
- Due schemi
  - Client – server
    - Uno o più server per risolvere gli indirizzi
    - I computer inviano richieste di risoluzione a questi indirizzi
  - Peer to peer
    - I computer inviano a tutti la richiesta di risoluzione
    - Ogni computer risponde alla richiesta di risoluzione del suo indirizzo

Address Resolution Protocol

- TCP/IP include un Address Resolution Protocol (ARP) (protocollo di risoluzione indirizzi)
  - Il messaggio di richiesta contiene l'indirizzo IP
  - Il messaggio di risposta contiene sia l'indirizzo IP che quello di rete
- I messaggi ARP sono incapsulati all'interno dei frame hardware
- I messaggi ARP sono riconosciuti controllando il campo del tipo nell'header del frame

Chaching address

- ARP mantiene una piccola tabella di corrispondenze in memoria per evitare overhead di invio di messaggi multipli
- Le corrispondenze degli indirizzi sono messe in cache
  - Quando un computer riceve un messaggio di risposta
  - Quando un computer riceve un messaggio di richiesta

Reverse Address Resolution Protocol

- TCP/IP include un Reverse Address Resolution Protocol (RARP) (protocollo di risoluzione inversa di indirizzi)
- RARP permette ad un host di conoscere il suo indirizzo IP
- Host
  - Invia una richiesta RARP contenente il suo indirizzo hardware ad un server
- Server
  - Ritorna una risposta RARP con l'indirizzo IP dell'host

Servizi connectionless

- Il servizio di consegna TCP/IP end-to-end è connectionless
- I protocolli di trasporto usano il loro servizio connectionless per fornire
  - Consegna dei dati connectionless (UDP)
  - Consegna dei dati connection-oriented (TCP)
- Estensione dell'astrazione LAN che unisce la raccolta di reti fisiche in un'unica rete virtuale
  - Indirizzamento universale
  - Dati consegnati in pacchetti (frame), ognuno con un header

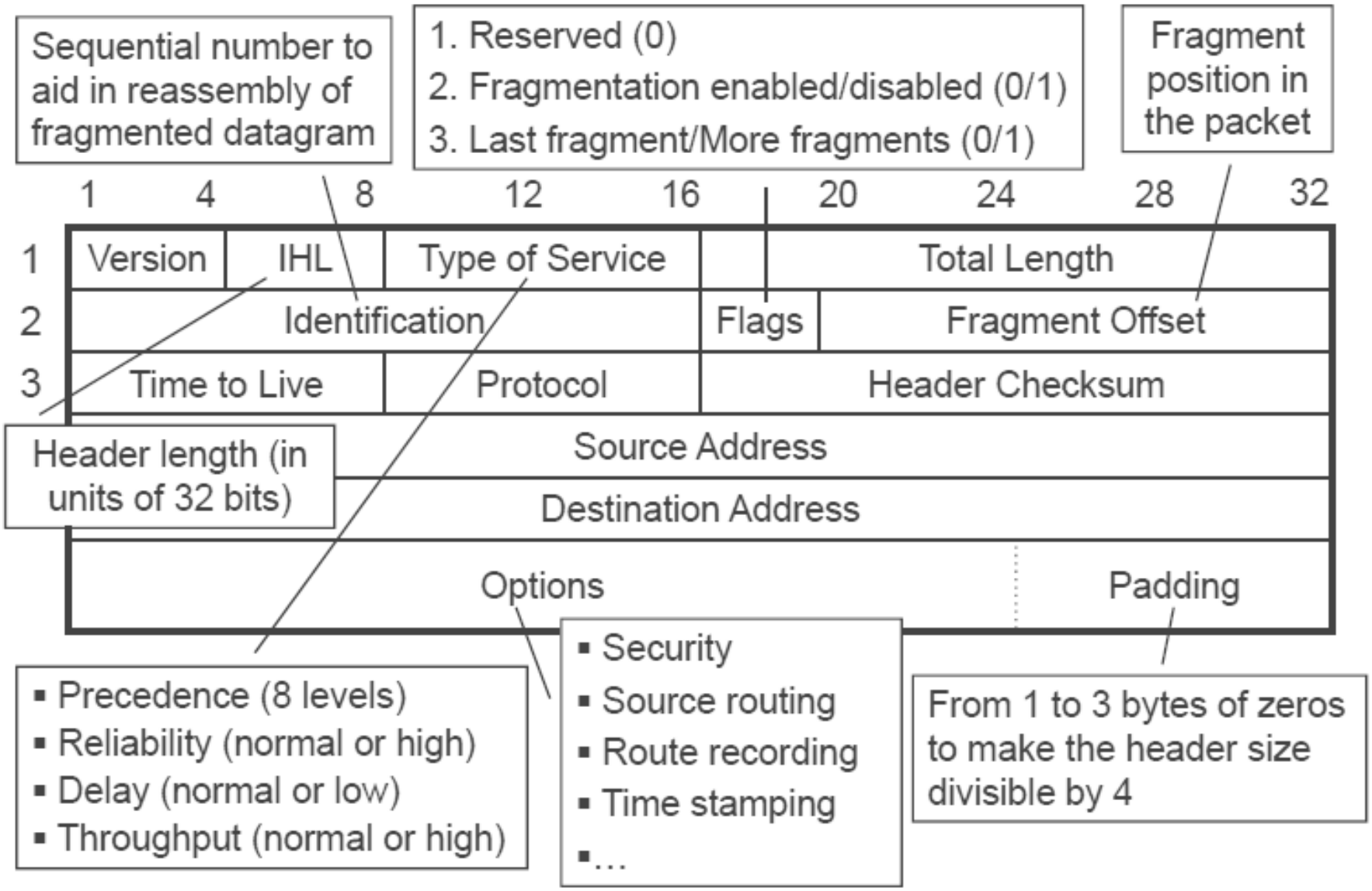
Datagrammi IP

- I pacchetti IP hanno lo stesso scopo in internet dei frame su una LAN
- I pacchetti IP sono chiamati datagrammi
- I router (formalmente gateway) instradano i pacchetti datagrammi tra le reti fisiche
- I pacchetti datagrammi hanno un formato uniforme, indipendente dall'hardware
- Sono incapsulati in frame hardware per la consegna attraverso ogni rete fisica

Formato dei datagrammi IP

- I pacchetti datagrammi sono composti da un'area di header ed un'area di dati
- I pacchetti datagrammi possono avere dimensioni differenti
  - L'area di header è di solito fissa (20 ottetti), ma può essere cambiata
  - L'area di dati può contenere da 1 a 64K ottetti
  - Di solito l'area di dati è maggiore di quella di header
- L'header contiene tutte le informazioni che servono per consegnare i pacchetti datagrammi al computer destinatario

Header del datagramma IP



Routing

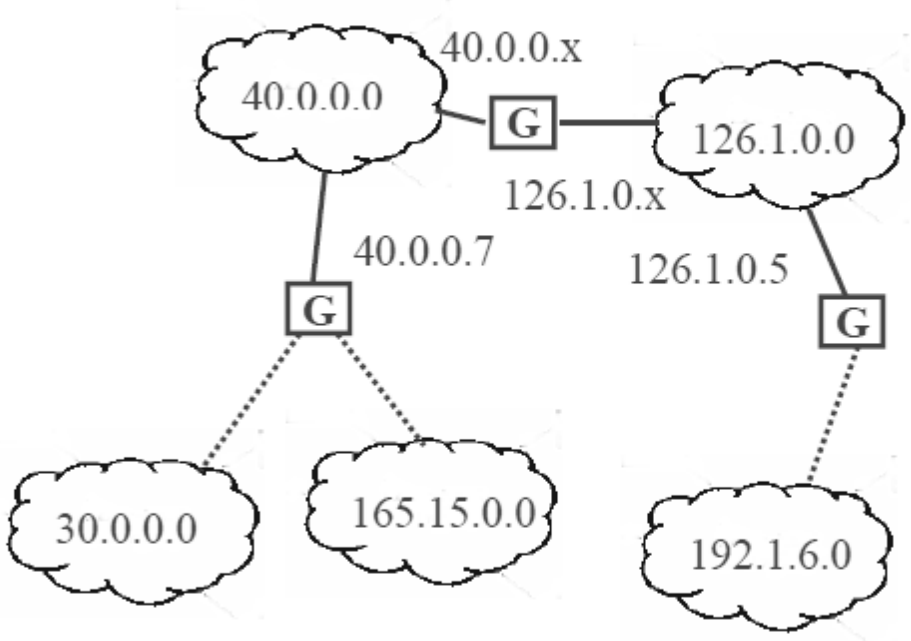
- Una “route” (strada) è l’informazione su come il traffico è rilanciato verso una locazione fisica o indirizzo
- I programmi applicativi o di gateway (router) instradano i pacchetti sulla porzione di rete destinataria…
- Le informazioni sul forwarding sono conservate nelle tabelle do routing
  - Inizializzate all’inizializzazione del sistema
  - Devono essere aggiornate quando la topologia della rete cambia
- Contengono la lista delle reti di destinazione ed il prossimo salto (next hop) per ogni destinazione
- Le tabelle di routing tengono una piccola lista di indirizzi IP di rete piuttosto che indirizzi IP completi

Tabella di routing

Network Address	Network Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	Direct Delivery
126.1.0.0	255.255.0.0	Direct Delivery
192.1.6.0	255.255.255.0	126.1.0.5
165.15.0.0	255.255.0.0	40.0.0.7

Tabella di routing

Network Address	Next Hop
30.0.0.0	40.0.0.7
40.0.0.0	Direct Delivery
126.1.0.0	Direct Delivery
192.1.6.0	126.1.0.5
165.15.0.0	40.0.0.7



Forwarding (inoltro) di datagrammi

- Per identificare la rete di destinazione
  - Applicare la maschera degli indirizza all'indirizzo di destinazione
  - Comparare agli indirizzi di rete nella tabella di routing
- Questo processo può essere espresso come

  if((Mask[i] & D) == Dest[i]) forward to NextHop[i]
- L'indirizzo di destinazione in un datagramma IP è sempre l'indirizzo della destinazione ultima
- I router cercano l'indirizzo di salto successivo ed inoltrano il datagramma
- L'indirizzo del salto successivo non compare mai in un datagramma IP

“Best-Effort delivery”

- IP fornisce un servizio equivalente alla LAN
- Non garantisce di prevenire
  - Pacchetti duplicati
  - Ritardi o consegne non ordinate
  - Corruzione di dati
  - Perdita di datagrammi
- L’affidabilità di consegna è fornita dalla strato di trasporto
- Lo strato di rete IP può trovare e riportare errori senza risolverli
  - Lo strato rete è centralizzato sulla consegna dei datagrammi
  - Allo strato applicativo non interessa la differenziazione tra problemi di consegna a livello di router intermedi

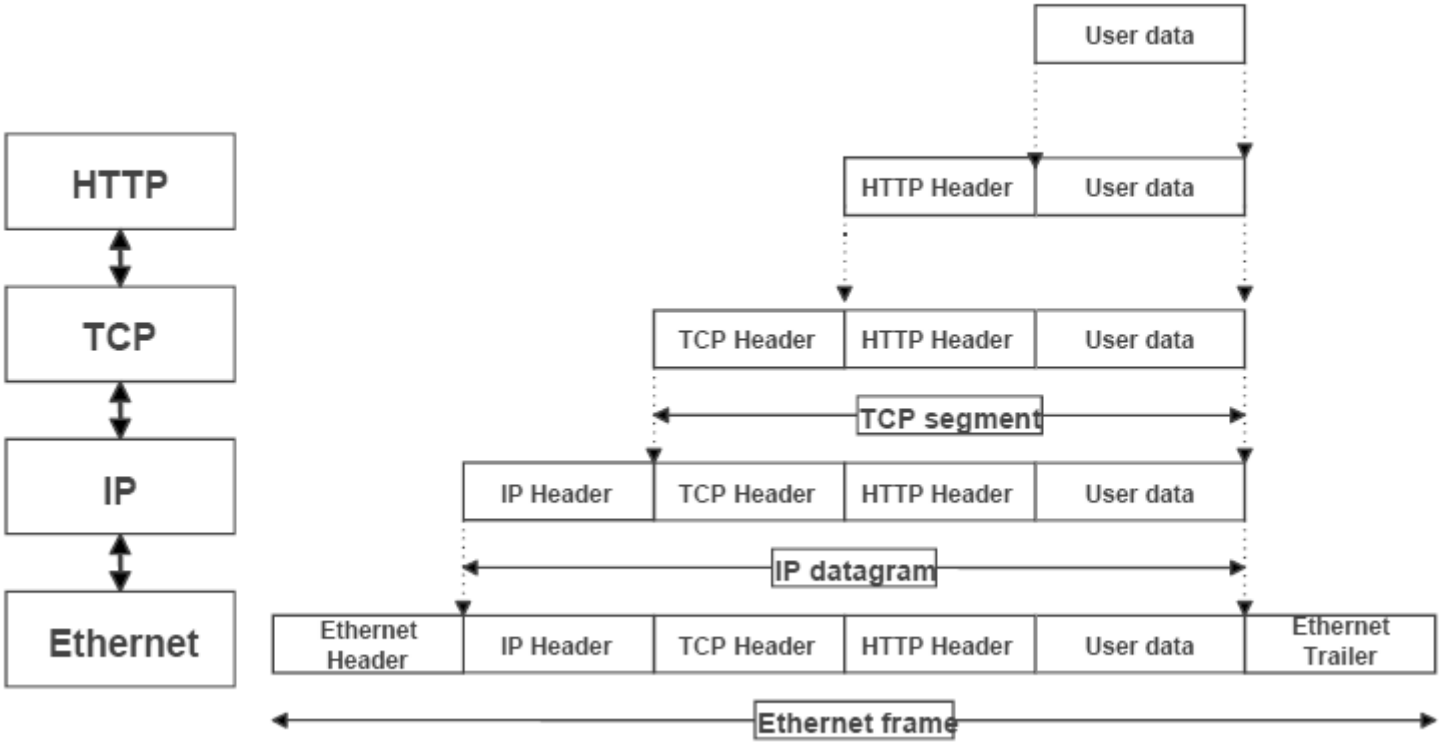
Trasmissione di datagrammi e frame

- Strato internet IP
  - Costruisce datagrammi
  - Determina il salto successivo
  - Si appoggia allo strato di interfaccia di rete
- Strato di interfaccia di rete IP
  - Collega l'indirizzo del salto successivo con il suo indirizzo hardware
  - Prepara i datagrammi per la trasmissione
- Tuttavia l'hardware accetta e consegna i pacchetti che aderiscono ad uno specifico formato del frame

incapsulazione

- Lo strato di interfaccia di rete IP incapsula i datagrammi come dati in frame hardware
  - L'hardware ignora il formato del datagramma IP
  - Tipi di frame sono specifici per il datagramma IP, così come gli altri (es. ARP)
- Lo stack del protocollo ricevente interpreta l'area dei dati basandosi sul tipo di frame

Incapsulamento



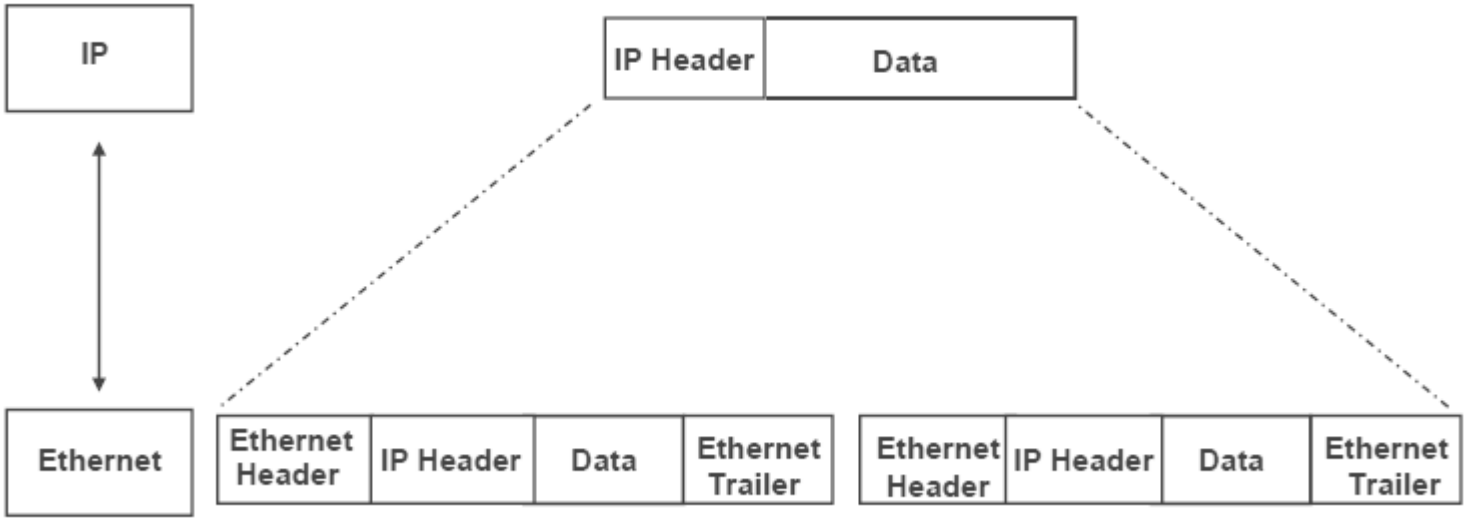
Massima unità di trasmissione

- Ogni specifica tecnologia hardware include la definizione delle dimensioni massime dell'area dati all'interno del frame
- È chiamata massima unità di trasmissione (MTU)
- Ogni datagramma in un frame hardware deve essere più piccolo dell'MTU di quell'hardware

frammentazione

- Una tecnica
  - Limitare la dimensione dei datagrammi alla più piccola MTU di ogni rete
- IP utilizza la frammentazione
  - I pacchetti datagrammi possono essere divisi in pezzi per entrare in reti con piccole MTU
- I router trovano i datagrammi più grandi dell'MTU della rete
  - Li dividono in pezzi
  - Ogni pezzo è più piccolo del limite massimo dell'MTU della rete

Frammentazione



Frammentazione

- Ogni frammento è un datagramma indipendente
  - Include tutti i campi header
  - I bit dell'header indicano che il datagramma è un frammento
  - Gli altri campi hanno informazioni per ricostruire il datagramma originale
    - L'offset del frammento fornisce la posizione originale del frammento
- Il router utilizzano l'MTU locale per calcolare la dimensione di ogni frammento
  - Mette una parte dei dati del datagramma originale in ogni frammento
  - Mette le altre informazioni nell'header

Riassemblamento di datagrammi

- La ricostruzione di datagrammi originali è detta riassemblamento
- La destinazione ultima opera il riassemblamento
  - Riduce l'ammontare di informazione di stato all'interno dei router
  - I router possono essere cambiati dinamicamente
- La destinazione esegue il riassemblamento usando
  - Il campo di identificazione
  - Il campo di offset del frammento

Perdita di frammenti

- IP può eliminare frammenti di un datagramma
  - La destinazione elimina l'intero datagramma
- La destinazione identifica frammenti persi
  - Imposta un timer quando il primo frammento arriva
  - Se il tempo scade prima che tutti i frammenti siano arrivati, il datagramma viene eliminato
- La sorgente (protocollo di strato applicativo) ritrasmette il datagramma se un acknowledgment (ack) non arriva

Frammentazione di un frammento

- I frammenti possono incontrare successivamente delle reti con MTU ancora inferiori
- Il router frammenta i frammenti per incontrare le dimensioni dell'MTU
- I sottoframmenti risultanti appaiono proprio come i frammenti originali (tranne che per la dimensione)
- Non c'è necessità di una gerarchia di riassemblamento
- I sottoframmenti includono la posizione originale all'interno del datagramma

Successo di IP

- La versione corrente di IP – versione 4 – ha 30 anni
- IPv4 ha mostrato grande abilità di spostarsi verso nuove tecnologie ed i principi base sono validi anche oggi
- IPv4 ha accomodato cambiamenti drammatici dal design originale
  - Molti nuovi tipi di hardware
  - Scalato da poche decine a qualche decina dei milioni di computer
  - Velocità da Kbps a Gbps
- IETF ha proposto una versione completamente nuova (IPv6) per indirizzare alcune piattaforme specifiche

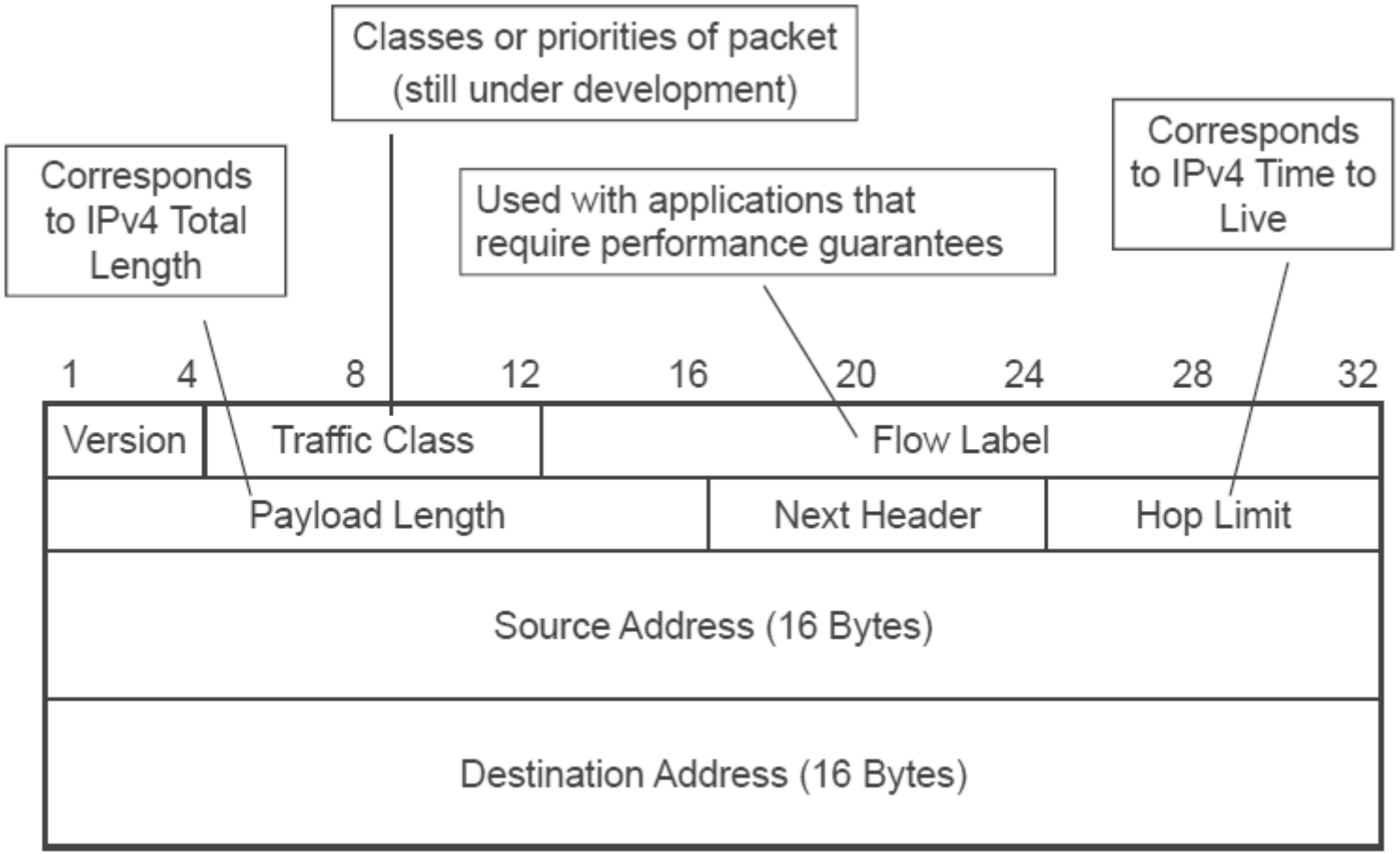
Motivo del cambiamento

- Spazio di indirizzi
  - Indirizzi a 32 bit permettono oltre un milione di reti
  - Molte delle quali sono di classe C, troppo piccole per molte organizzazioni
  - 2^{14} indirizzi di reti di classe B sono già in gran parte esauriti
- Tipo di servizio
  - Differenti applicazioni hanno differenti requisiti per l'affidabilità di consegna e per velocità
  - Gli attuali header dei datagrammi IP hanno campi che indicano il tipo del servizio
  - Il protocollo IP attuale non li utilizza
- multicast

Nuove caratteristiche di IPv6

- Dimensione dell'indirizzo (da 32 a 128 bit)
- Header
  - L'header ha poche informazioni e dimensione fissata
  - Le altre informazioni sono contenute in header estesi
- Supporto per audio video
  - Etichette di flusso e qualità del servizio permettono alle applicazioni audio e video di stabilire le connessioni appropriate
- Estensibile
  - Nuove caratteristiche possono essere aggiunte facilmente
- Routing semplice
  - I router non gestiscono la frammentazione, il nuovo formato dell'header semplifica il routing

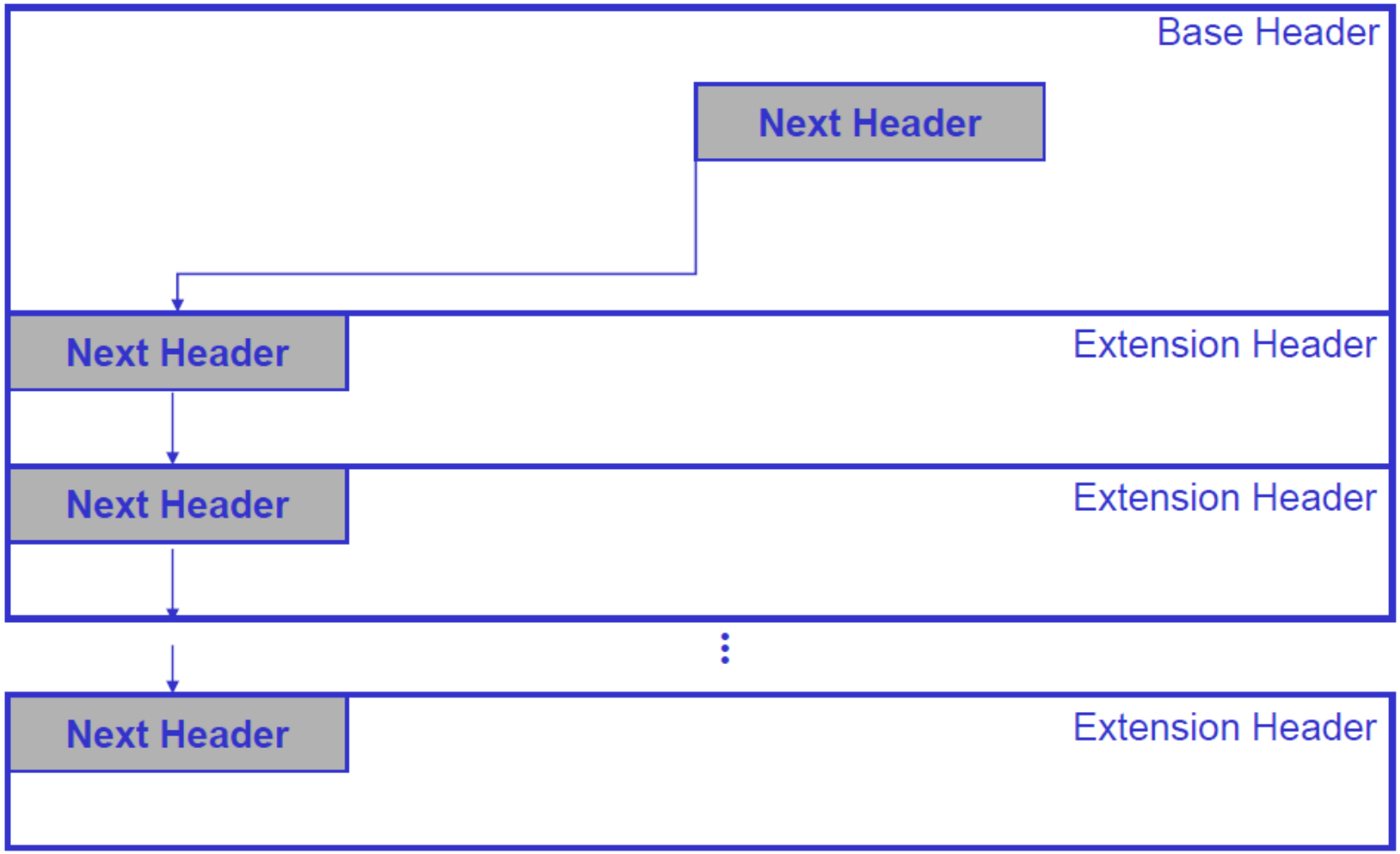
Header IPv6 di base



Header multipli

- Efficienza
  - Header larghi solo il necessario
- Flessibilità
  - Possibilità di aggiungere nuovi header per nuove funzionalità
- Sviluppo incrementale
  - Può aggiungere il trattamento di nuove funzionalità da testare
  - Gli altri router possono saltare questi header

Header multipli



Estensione degli header

- Routing header
- Fragmentation header
- Hop-by-Hop header
- Destinations Option Header
- Authentication Header
- Encrypted Security Payload Header

Frammentazione

- Le informazioni sulla frammentazione sono tenuti in header estesi separati
- Ogni frammento ha un header base e un header di frammentazione (inserito)
- L’intero datagramma (incluso l’header originale) può essere frammentato

Frammentazione e Path MTU

- La sorgente è responsabile della frammentazione
  - I router riducono i datagrammi più grandi degli MTU della rete
  - La sorgente deve frammentare i datagrammi per raggiungere la destinazione
- La sorgente determina il percorso MTU
  - MTU piccolo tra sorgente e destinazione
  - Frammenta i datagrammi per adattarli alla MTU
- Procede alla scoperta del percorso della MTU
  - La sorgente manda messaggi di dimensioni diverse finché la destinazione riesce a riceverli
  - Deve essere dinamica poiché il percorso può variare durante la trasmissione dei datagrammi

Indirizzamento IPv6

- Indirizzi a 128 bit
- Nessuna classe degli indirizzi
- Presenza di indirizzi speciali
  - Unicast
  - Multicast
  - Cluster

Tipi di indirizzi IPv6

- Unicast
  - Destinazione: singolo computer
- Multicast
  - Destinazioni multiple
  - Possibili in siti diversi
- Cluster
  - Insieme di computer con il medesimo prefisso
  - I datagrammi sono indirizzati lungo il percorso più breve e consegnati ad un solo computer del cluster

Codifica degli indirizzi IPv6

- Gli indirizzi a 128 bit in rappresentazione decimale richiederebbero 16 numeri

  105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

- Vengono raggruppati in gruppi di 16 bit in formato esadecimale

  69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF

- La zero-compression viene rappresentata con “::”

  FF0C:0:0:0:0:0:0:B1

  FF0C::B1

- Indirizzi IPv6 con 96 zeri iniziali vengono interpretati come indirizzi IPv4

Verso l'IPv6

- Cambio dei Domain Name Service per gestire gli indirizzi IPv6
- Cambio delle applicazioni
- Interoperabilità con gli indirizzi IPv4

Cambio delle applicazioni

- Applicazioni che non utilizzano la rete non devono essere cambiate
- Applicazioni che utilizzano la rete devono
  - Utilizzare nuovi tipi di record DNS per gli indirizzi IPv6
  - Utilizzare nuove API per le socket
- Approccio Bump-in-the-stack per la transizione
  - Introduce un modulo di interoperabilità come un “bump” nello stack della rete, tra gli strati Applicazione/Trasporto e IP
  - Permette alle applicazioni IPv4 di lavorare su reti IPv6

Interoperabilità con IPv4

- Non tutti i router possono essere aggiornati simultaneamente
- Come può la rete operare con router IPv4 e IPv6 mischiati?
- Due approcci proposti:
  - Stack doppio: alcuni router con doppio stack (v6,v4) possono tradurre i formati
  - Tunneling: IPv6 incapsulato come Payload nei datagrammi IPv4, attraverso router IPv4

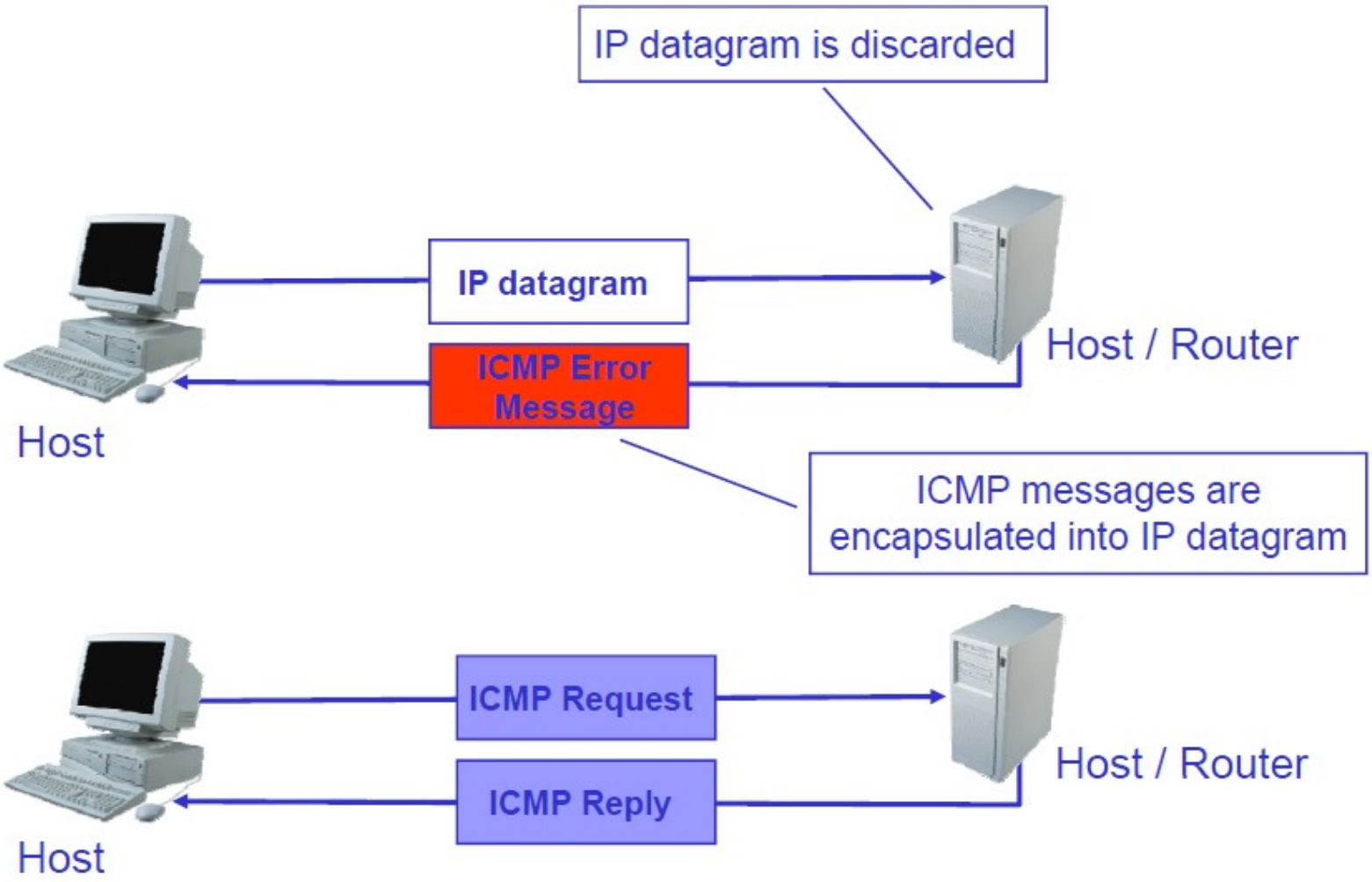
Scoperta degli errori e report

- Lo strato Internet può scoprire molti tipi di errori
  - Checksum (solo header!)
  - Time to Live scaduto
  - Reti senza percorso verso la destinazione
- IP fornisce una consegna migliore
  - IP scarta i pacchetti a datagramma con problemi

Internet Control Message Protocol (I**C**MP)

- ICMP è utilizzato per mostrare i problemi dei datagrammi IP su una rete IP
- ICMP può essere citato per dimostrare quando un particolare sistema finale non risponde, quando una rete IP non è raggiungibile, quando un nodo è in sovraccarico, quando si verifica un errore nel header di un pacchetto,…
- ICMP è utilizzato frequentemente dai gestori di rete per verificare il corretto funzionamento dei sistemi finali e l'instradamento corretto dei pacchetti da parte dei router verso le destinazioni specificate

Meccanismi del ICMP



Messaggi di errore frequenti

Name	Description
Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped
Redirect	Informs about an alternative route for the datagram and should result in a routing table update
Time exceeded	Sent when the TTL field has reached zero or when there is a timeout for the reassembly of segments
Parameter problem	Sent when the IP header is invalid or when an IP header option is missing
Network Unreachable	No routing table entry is available for the destination network
Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests
Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination
Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application
Fragmentation Needed	IP datagram must be fragmented, but the DF bit in the IP header is set

Messaggi informativi frequenti

Name	Description
Echo Request	Ask a machine if it is alive
Echo Reply	Reply to confirm that it is alive
Timestamp Request	Ask about the machine time (often used for synchronizing the clocks between two machine
Timestamp Reply	Replies with the machine time
Router Solicitation	Ask about router addresses sending the message to a router multicast address
Router Advertisement	Reply its address
Address Mask Request	Ask about the network mask to be used
Address Mask Reply	Reply with the network mask

ICMP e accessibilità

- I programmi di Ping testano l'accessibilità delle macchine
  - Mandano un datagramma UDP da B ad A ed A risponde a B
  - Utilizzano messaggi di richiesta ICMP e rispondono con dei messaggi di echo
  - Lo strato Internet include dei codici per rispondere ai messaggi di richiesta ICMP entranti

ICMP e scoperta del cammino

- I programmi traceroute usano dei pacchetti a datagramma verso delle non-existent port per trovare i cammini attraverso cui espandere l'anello di ricerca
- Mandano dei messaggi echo ICMP con un Time to Live incrementato
  - I router che decrementano il Time to Live a 0 mandano un messaggio ICMP di tempo scaduto, con il loro indirizzo come indirizzo sorgente
  - Prima, con il Time to Live 1, vanno nel primo router che scartano e mandano un messaggio di tempo scaduto
  - Poi, con il Time to Live 2, vanno nel secondo router
  - Continuano finché il messaggio non viene ricevuto a destinazione
- I traceroute devono tenere conto
  - Di vari ritardi nella rete
  - Del cambiamento dinamico dei percorsi

ICMP e scoperta del router

- Il router può rompersi, lasciando isolato dalla rete un host
- La procedura di scoperta dei router ICMP serve per trovare nuovi router
- L’host può trasmettere delle richieste al router per auto configurare il cammino predefinito
- L’host può trasmettere delle richieste se il router si rompe
- Il router può trasmettere degli avvisi di esistenza appena si connette

ICMP e scoperta del percorso MTU

- La frammentazione deve essere evitata, poiché abbassa le performance
- La sorgente determina il percorso con l'MTU di rete più breve tra sorgente e destinazione
  - La sorgente sonda il percorso utilizzando dei datagrammi IP con flag "don't fragment" attivo
  - Il router risponde con un messaggio ICMP frammentato
  - La sorgente manda delle sonde finché il destinatario riesce a ricevere

Assegnamento dinamico degli indirizzi IP

- L'assegnamento dinamico degli indirizzi IP è desiderabile per diverse ragioni:
  - Gli indirizzi IP sono assegnati a richiesta
  - Evita la configurazione manuale
  - Supporta la mobilità dei laptop
- RAPR fa questo:
  - Trasmette una richiesta per l'indirizzo IP, con annesso l'indirizzo MAC
  - Il server RAPR risponde con l'indirizzo IP
- Tuttavia assegna solamente l'indirizzo IP (non il router di default e la subnet mask)

Dynamic Host Configuration Protocol (DHCP)

- DHCP è il meccanismo migliore per l'assegnamento dinamico degli indirizzi IP
  - Supporta le allocazioni temporanee di indirizzi IP (lease)
  - Il client DHCP può acquisire dinamicamente tutti i parametri di configurazione IP necessari per operare

Ciclo di vita di un indirizzo IP

- Un client richiede un server DHCP tramite un messaggio “DHCP discovery”
- Uno o più server DHCP rispondono con un messaggio di offerta
- Il client chiede un indirizzo IP ad uno dei server DHCP
- Il server DHCP noleggia un indirizzo IP tramite un messaggio di ACK
- Quando il 50% del lease è scaduto, il client rinnova il lease con un messaggio di richiesta al DHCP
- Alla fine il client rilascia l’indirizzo IP con un messaggio di rilascio

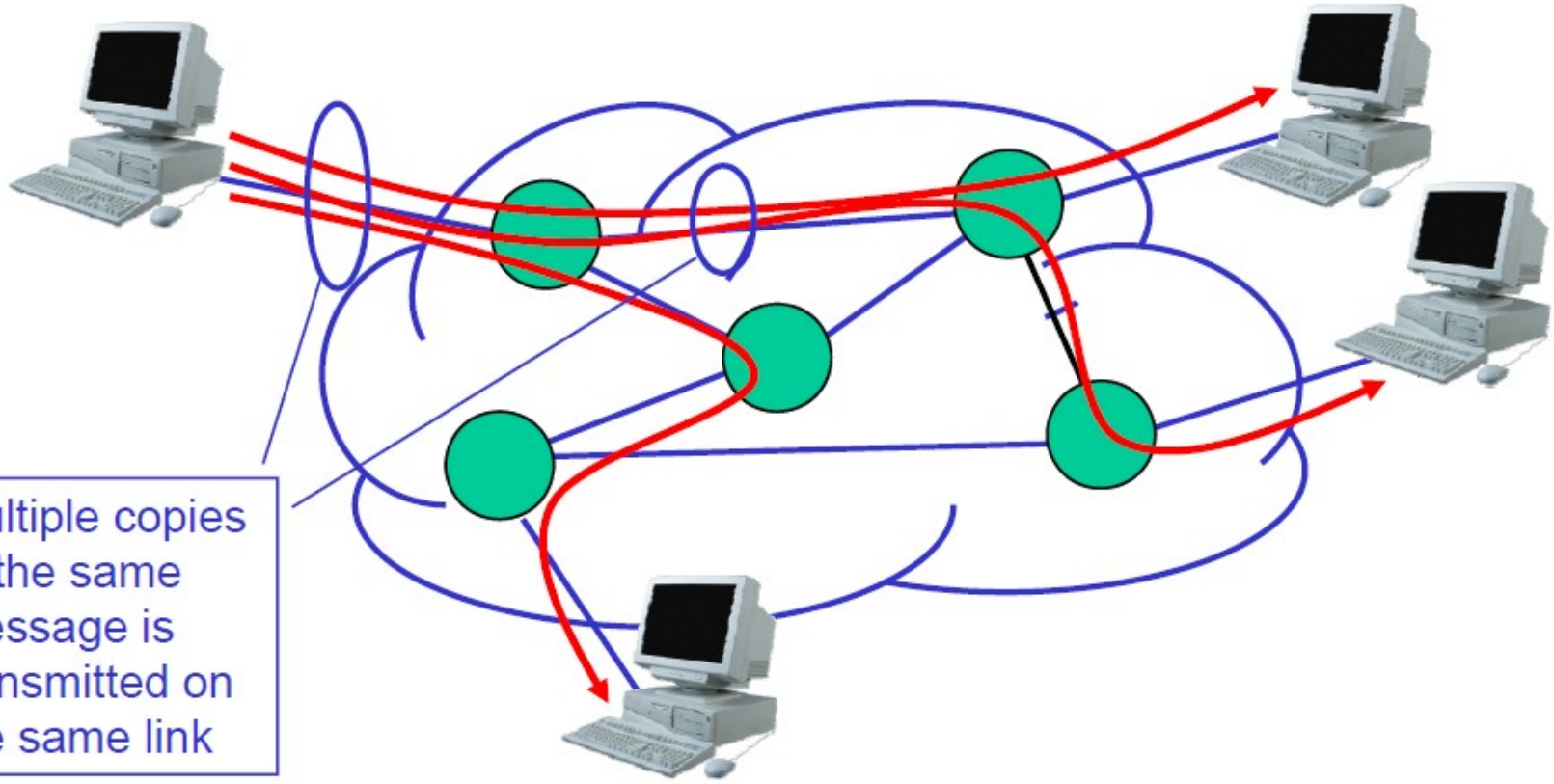
Applicazioni con molti ricevitori

- Molte applicazioni trasmettono lo stesso dato ad un dato istante a più ricevitori
  - Trasmissioni radio e video
  - Videoconferenze
  - Applicazioni distribuite
- Una rete deve avere dei meccanismi per supportare queste applicazioni in maniera efficiente

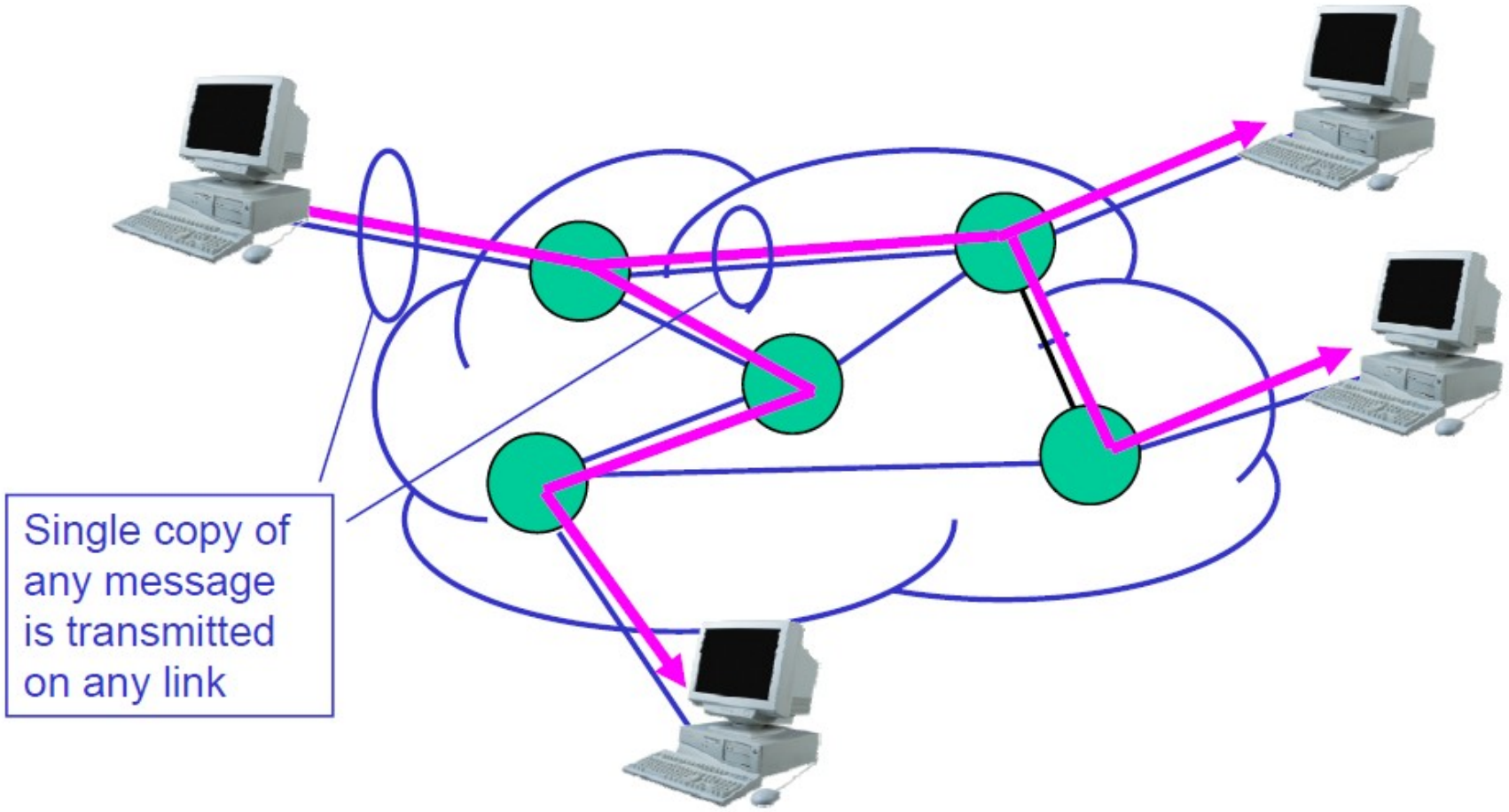
Gruppo Multicast

- L’insieme dei ricevitori di una trasmissione multicast è chiamato Gruppo Multicast
  - Un gruppo multicast è identificato da un indirizzo multicast
- Un utente che vuole ricevere una trasmissione multicast si unisce al corrispondente gruppo, e ne diviene membro
- Dopo che un utente si è unito, la rete costruisce i percorsi di instradamento necessari affinché l’utente riceva i dati spediti al gruppo multicast

Multicasting senza supporto di rete



Multicasting con supporto di rete



Internet Group Management Protocol (I**G**MP)

- IGMP gestisce i gruppi multicast
- L'host manda un report IGMP quando un'applicazione si unisce ad un gruppo multicast
- Il router manda una query IGMP ad intervalli regolari
- L'host che diventa multicast deve rispondere alla query
- L'host non deve uscire esplicitamente dal gruppo quando si disconnette

Routing Information Protocol (RIP)

- RIP è un semplice protocollo interno al dominio
  - È un implementazione lineare dell'algoritmo di routing Distance Vector
    - Ogni router annuncia il proprio vettore di distanza ogni 30 sec (o quando la propria tabella di routing cambia) a tutti i propri vicini
    - RIP utilizza sempre 1 come metrica di collegamento
    - Il conteggio massimo degli hop è 15, 16 equivale ad infinito (∞)
    - I percorsi sono settati come irraggiungibili (16) dopo 3 minuti se non vengono aggiornati

Open Shortest Path First (OSPF)

- OSPF gestisce l'instradamento in una internet
  - Utilizza l'algoritmo di routing Link State
    - Ogni router mantiene una lista dello stato dei collegamenti locali della rete
    - Trasmette degli aggiornamenti di stato
    - I messaggi creano un traffico insignificante
  - Topologia salvata come grafo diretto
    - Vertici o nodi (routers o reti)
    - Lati (connette routers o reti)

Resource ReSerVation Protocol (RSVP)

- RSVP permette alle applicazioni unicast e multicast di riservare risorse nei router per migliorare la qualità del servizio (QoS)
  - Le applicazioni fanno delle prenotazioni
  - Se il router non incontra una richiesta, la corrispondente applicazione viene informata
  - Le applicazioni devono periodicamente rinnovare le loro richieste durante la trasmissione

Protocolli di trasporto

- Il protocollo Internet (IP) fornisce un servizio di datagramma inaffidabile tra gli host
- I protocolli di trasporto forniscono un meccanismo di consegna end-to-end tra i terminali della connessione, che siano processi di sistema o applicazioni
- User Datagram Protocol (UDP) fornisce un servizio a datagramma
- Transport Control Protocol (TCP) fornisce un sistema di trasporto affidabile

Selezione del numero di porta

- Computer comunicanti devono accordarsi su un numero di porta comune
  - Il server apre determinate porte ed attende dei messaggi
  - Il client sceglie delle porte locali e manda un messaggio sulla porta selezionata
- I servizi forniti dai computer utilizzano delle porte riservate, ben definite
  - ECHO
  - TELNET
  - FTP
- Gli altri servizi utilizzano delle porte assegnate dinamicamente

Porte assegnate

Port	Scope
0	Not Used
1-255	Reserved ports for well-known services
256-1023	Other reserved ports
1024-65535	User-defined server ports

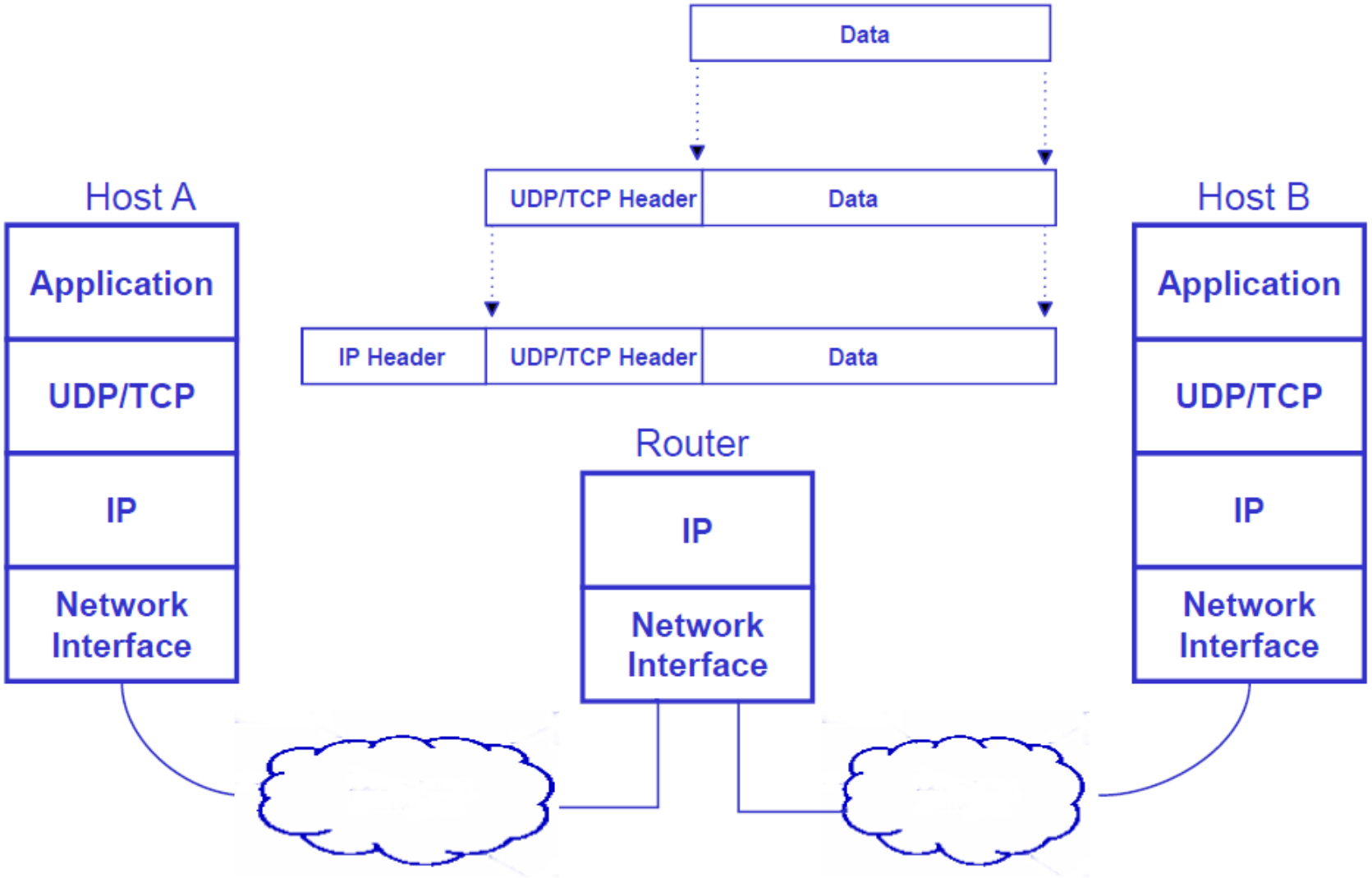
Porte Well-Known

Port	Name	Description
7	echo	Echo input back to sender
9	discard	Discard input
11	systat	System statistics
13	daytime	Time of day (ASCII)
17	quote	Quote of the day
19	chargen	Character generator
37	time	System time (seconds since 1970)
53	domain	DNS
69	tftp	Trivial File Transfer Protocol (TFTP)
123	ntp	Network Time Protocol (NTP)
161	snmp	Simple Network Management Protocol (SNMP)

Utilizzo di IP per la consegna dei dati

- UDP e TCP utilizzano IP per la consegna dei dati
- I punti finali sono identificati dalle porte
  - Consentono connessioni multiple allo stesso host
  - Le porte dovrebbero essere assegnate ad un'applicazione o ad un processo di sistema
- IP tratta UDP/TCP come dati e non interpreta il contenuto del messaggio

Consegna UDP/TCP



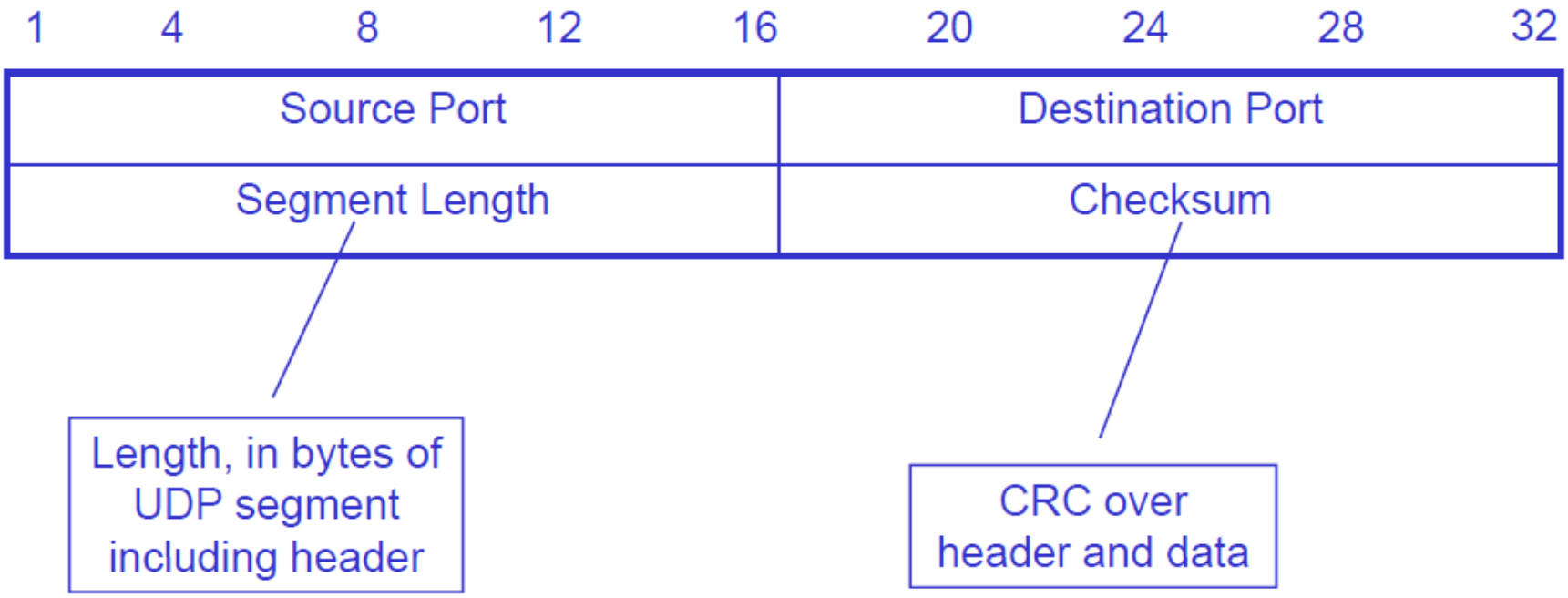
User Datagram Protocol (UDP)

- UDP consegna dei messaggi indipendenti, chiamati pacchetti o datagrammi, tra le applicazioni del host
- Principali caratteristiche:
  - Consegna inaffidabile
    - I datagrammi possono essere persi
    - Consegnati fuori ordine
  - Il checksum (opzionale) garantisce l'integrità dei dati

UDP

- Generalmente, i terminali del UDP sono chiamati porte
- Ogni trasmissione dati UDP identifica l'indirizzo e la porta di destinazione e sorgente del messaggio
- Le porta sorgente e di destinazione possono essere differenti

Header UDP


1
4
8
12
16
20
24
28
32
Source Port
Destination Port
Segment Length
Checksum
Length, in bytes of UDP segment including header
CRC over header and data

Transmission Control Protocol (TCP)

- TCP è il protocollo di trasporto più utilizzato
- Fornisce una consegna affidabile dei dati utilizzando la consegna inaffidabile dei datagrammi
- Compensa le perdite, i ritardi, le duplicazioni e problemi simili
- La consegna affidabile è un modello di alto livello per la costruzione di applicazioni

Caratteristiche di TCP

- Connection Oriented
  - Le applicazioni richiedono una connessione con la destinazione e poi utilizzano la connessione per trasferire i dati
- Punto-Punto
  - Una connessione TCP ha due punti terminali
- Affidabilità
  - TCP garantisce che i dati vengano consegnati senza perdite, duplicazioni od errori di trasmissione
- Full duplex
  - I punti terminali di una connessione TCP possono scambiarsi i dati in entrambe le direzioni simultaneamente

Caratteristiche di TCP

- Interfaccia a flusso
  - Le applicazioni consegnano i dati al TCP come un flusso continuo di dati, senza delimitazioni di record
  - TCP non fornisce garanzie che i dati vengano ricevuti negli stessi blocchi in cui sono stati trasmessi
- Installazione della connessione affidabile
  - Three-Way Handshake garantisce un'installazione affidabile e sincronizzata tra i punti terminali
- Arresto della connessione affidabile
  - TCP garantisce la consegna di tutti i dati dopo che i terminali si spengono

Tecniche di consegna affidabile tramite TCP

- Pacchetti persi
- Pacchetti duplicati
- Pacchetti in ritardo
- Dati corrotti
- Errori nella velocità di trasmissione
- Congestione
- Riavvii del sistema

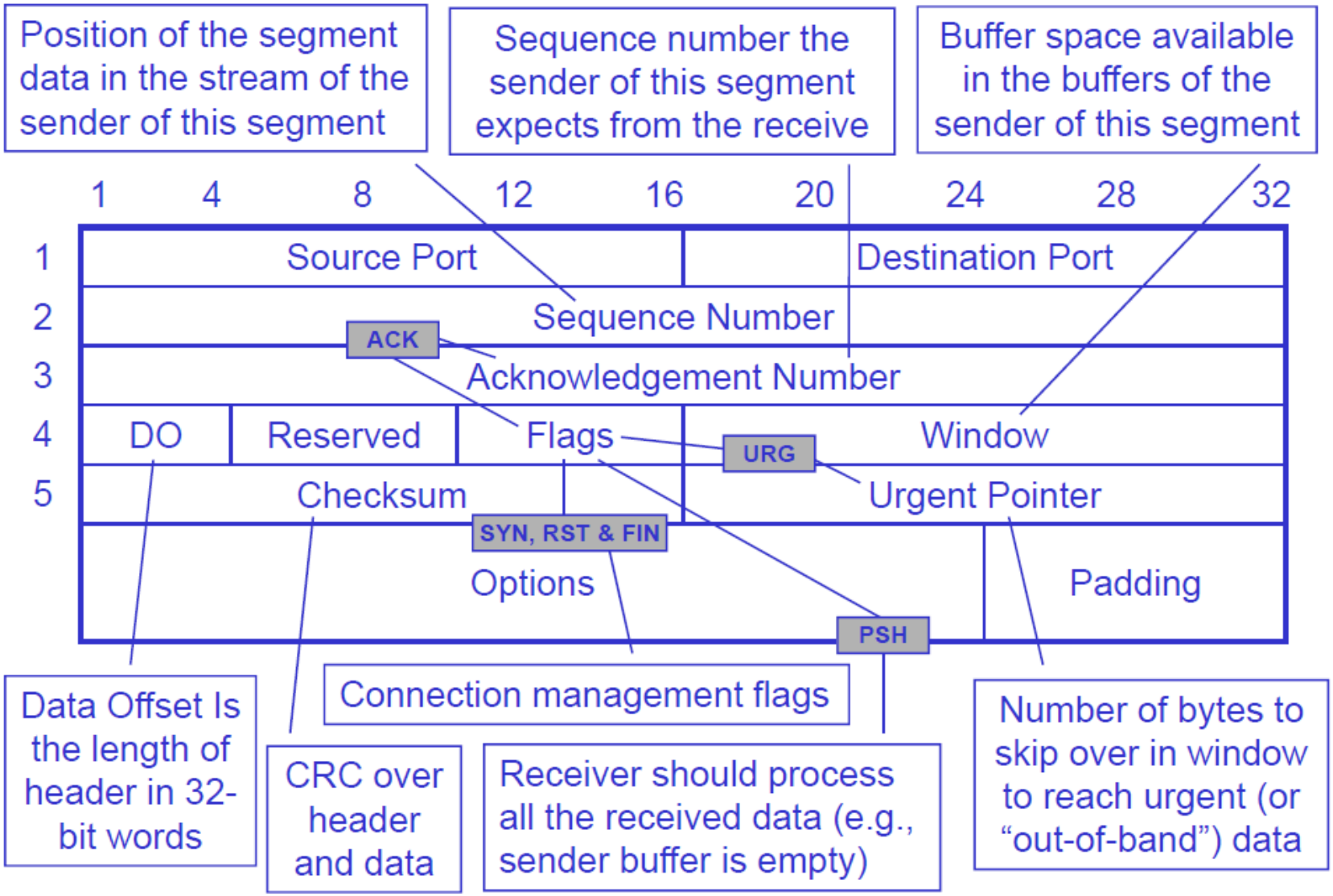
Pacchetti persi

- TCP utilizza ACK positivi con ritrasmissione per realizzare una consegna dei dati affidabile
- Ricevitore
  - Manda degli ACK al mittente come verifica di corretta ricezione dei dati
- Mittente
  - Imposta dei timer per trasmettere i dati
  - Se il timer scade prima che l'ACK arrivi ritrasmette i dati, attivando un nuovo timer

Segmenti TCP e numeri di sequenza

- Le applicazioni consegnano dei pacchi di dati larghi a piacere al TCP come un flusso
- Il flusso originale è numerato per bytes
- Il mittente spezza il flusso in segmenti
  - Ogni segmento finisce in un datagramma IP
  - Il segmento contiene un numero di sequenza
- Il ricevitore manda un segmento formato dai numeri di sequenza dei dati ricevuti
  - Un ACK può assicurare più segmenti

Header TCP


Position of the segment data in the stream of the sender of this segment
Sequence number the sender of this segment expects from the receive
Buffer space available in the buffers of the sender of this segment
1 4 8 12 16 20 24 28 32
1
2
3
4
5
Source Port
Destination Port
Sequence Number
ACK
Acknowledgement Number
DO
Reserved
Flags
URG
Window
Checksum
Urgent Pointer
SYN, RST & FIN
Options
Padding
PSH
Data Offset Is the length of header in 32-bit words
CRC over header and data
Connection management flags
Receiver should process all the received data (e.g., sender buffer is empty)
Number of bytes to skip over in window to reach urgent (or "out-of-band") data

Timeout

- Un timeout non appropriato può portare a performance basse:
  - Troppo lungo
    - Il mittente attende più del necessario prima di ritrasmettere
  - Troppo breve
    - Il mittente genera del traffico non necessario
- Il timeout deve essere differente per ogni connessione e settato dinamicamente
  - Host sulla stessa LAN devono avere timeout breve rispetto ad host a 20 hop di distanza
  - Il tempo di consegna attraverso internet dovrebbe cambiare fuori flusso
    - Il timeout deve seguire i cambiamenti

Fissare un valore per il timeout

- Il timeout deve essere basato su un round trip time (RTT)
  - Il mittente non può conoscere l'RTT di ogni pacchetto a priori
  - Il mittente fissa il timeout di ritrasmissione (RTO) basandosi sugli RTT precedenti
- Un metodo specifico è quello chiamato Algoritmo Adattativo di Ritrasmissione

$$RTT_{new} = \alpha \bullet RTT_{old} + (1 - \alpha) \bullet RTT_{sample}$$

$$RTO = \beta \bullet RTT_{new}$$

Misura del RTT

- L'RTT viene misurato osservando le differenze tra il tempo di trasmissione e quello di arrivo del ACK
- Tuttavia, gli ACK non portano informazioni su quali pacchetti sono conosciuti
- Il mittente non può determinare se l'ACK è relativo alla trasmissione originale o ad una ritrasmissione
  - Decide per la trasmissione originale sovrastimando l'RTT
  - Decide per la ritrasmissione sottostimando l'RTT

Algoritmo di Karn

- L’algoritmo di Karn specifica che il mittente ignora l’RTT per i segmenti ritrasmessi
- L’algoritmo di Karn specifica che l’RTO è separato dal RTT quando avviene una ritrasmissione
- L’RTO raddoppia per ogni nuovo messaggio finché non arriva un ACK senza ritrasmissione

Sliding Window TCP

- TCP usa la sliding window per il controllo di flusso
- Quando un segmento arriva, il ricevitore manda un ACK specificando lo spazio rimanente nel buffer
  - Lo spazio disponibile nel buffer è detto window
  - Le sue notifiche sono dette window advertisement
- Il mittente può trasmettere qualsiasi byte, in qualsiasi spazio del segmento, tra l'ultimo byte conosciuto e all'interno della dimensione della window

Sindrome della finestra sciocca (Silly Window Syndrome)

- In alcune circostanze la sliding window può consentire la trasmissione di molti piccoli segmenti
- Il ricevitore avverte la finestra piccola se
  - La propria finestra è piena
  - L'applicazione ricevente consuma pochi bytes di dati
- Il mittente immediatamente manda dei piccoli segmenti per adattare la window
  - Inefficiente in processi temporizzati
- Soluzioni
  - Il ricevitore ritarda l'annuncio della nuova finestra
  - Il mittente ritarda l'invio dei dati quando la window è piccola

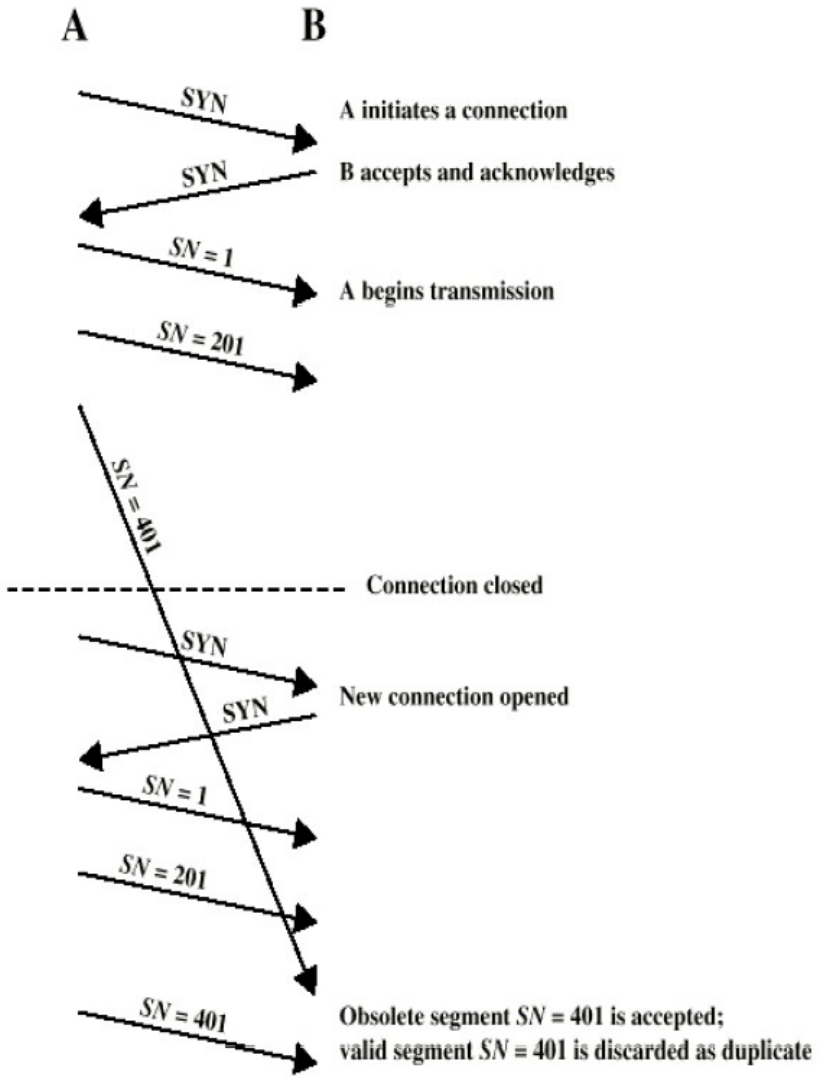
Gestione della connessione

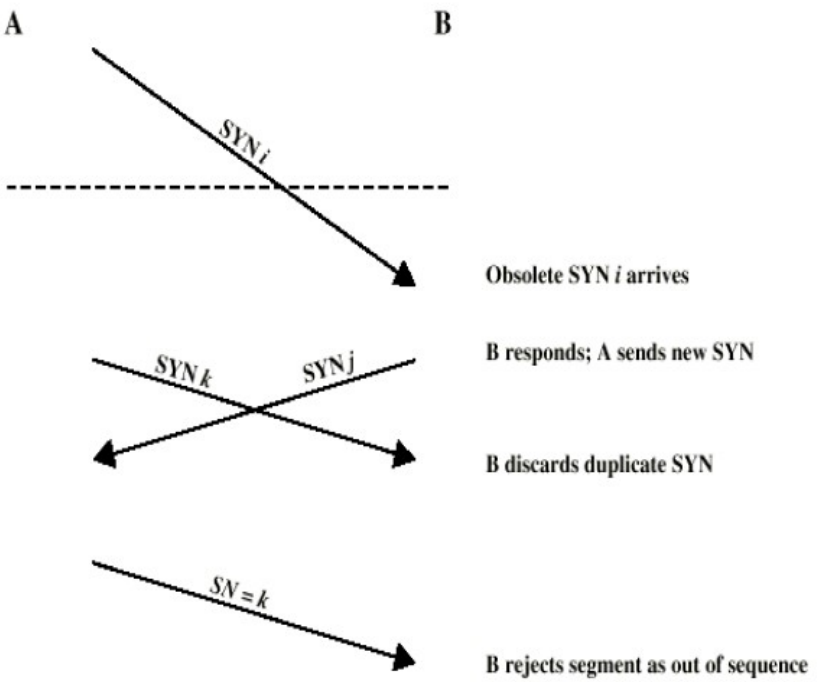
- L’installazione e l’abbattimento della connessione è basato sullo scambio di due tipi di segmenti
  - L’installazione della connessione è basata su segmenti di sincronizzazione (SYN)
  - L’abbattimento della connessione è basata su segmenti di finalizzazione (FIN)

Two-Way Handshake

- Un protocollo di installazione di una connessione utilizzabile è il Two-Way Handshake
  - A manda SYN, B replica con SYN
  - La perdita di SYN viene gestita con la ritrasmissione
    - Può portare a SYN duplicati
  - Si ignorano i SYN duplicati una volta connessi
- Segmenti persi o ritardati possono causare problemi alla connessione
  - Segmenti da una vecchia connessione
  - Segmento di partenza vecchio

Two-Way Handshake

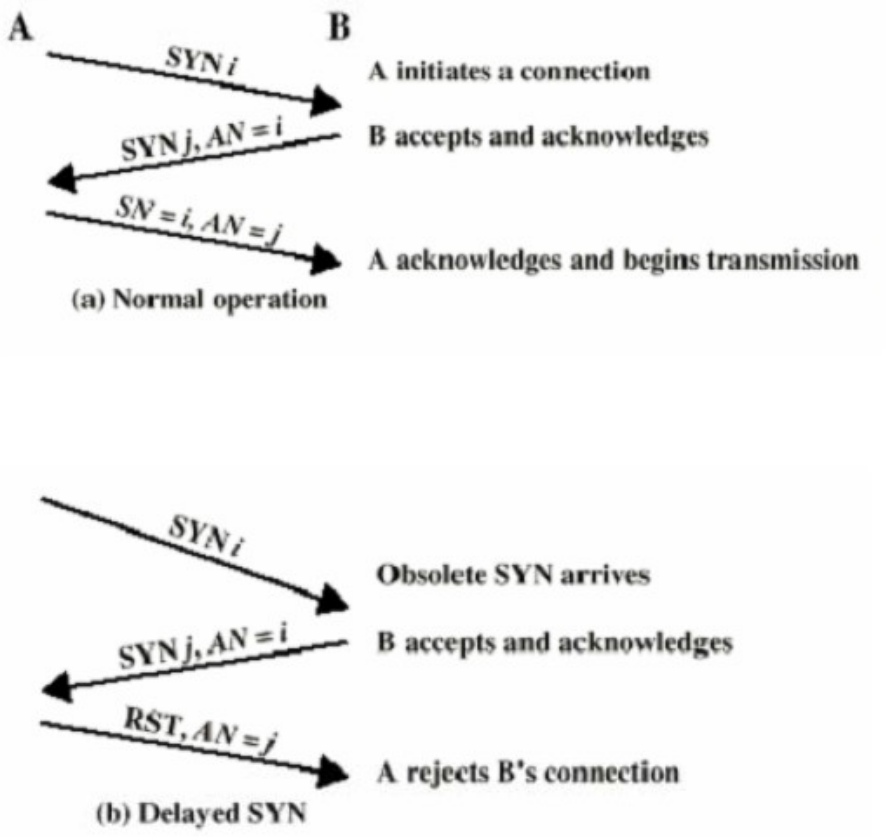


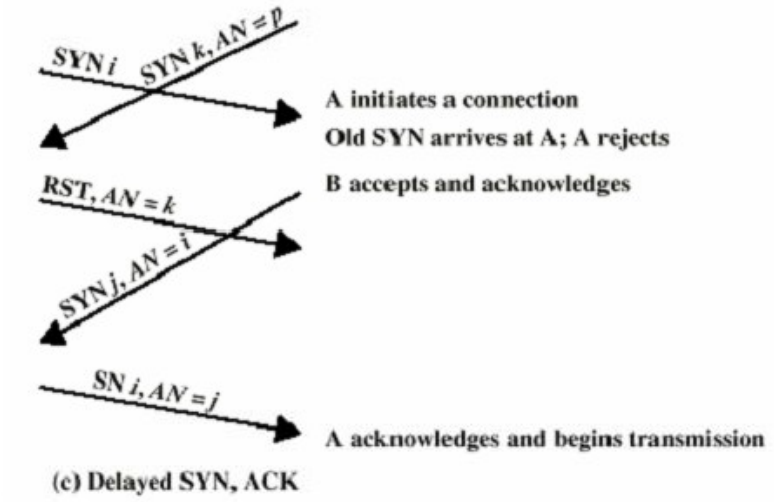


Three-Way Handshake

- TCP usa Three-Way Handshake per l'installazione e l'abbattimento di connessioni affidabili
- Handshake è basato su tre passi
  - Host 1 manda un segmento con i bit SYN/FIN settati ed un numero di sequenza random
  - Host 2 risponde con un segmento con i bit SYN/FIN settati, ACK per Host 1
  - Host 1 risponde con un ACK

Three-Way Handshake





Controllo di congestione

- Un traffico eccessivo può causare la perdita dei pacchetti
  - I protocolli di trasporto rispondono con una ritrasmissione
  - Ritrasmissioni massicce possono causare un crollo dovuto a congestione
- TCP interpreta la perdita di pacchetti come un indicatore di congestione
- Il mittente usa il controllo di congestione TCP e la trasmissione lenta di pacchetti
  - Manda un singolo pacchetto
  - Se ACK torna senza perdite, manda due pacchetti