UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione

Protocolli: Internet Protocol

Luca Veltri
(mail.to: luca.veltri@unipr.it)

Corso di Reti di Telecomunicazioni A, a.a. 2007/2008
http://www.tlc.unipr.it/veltri

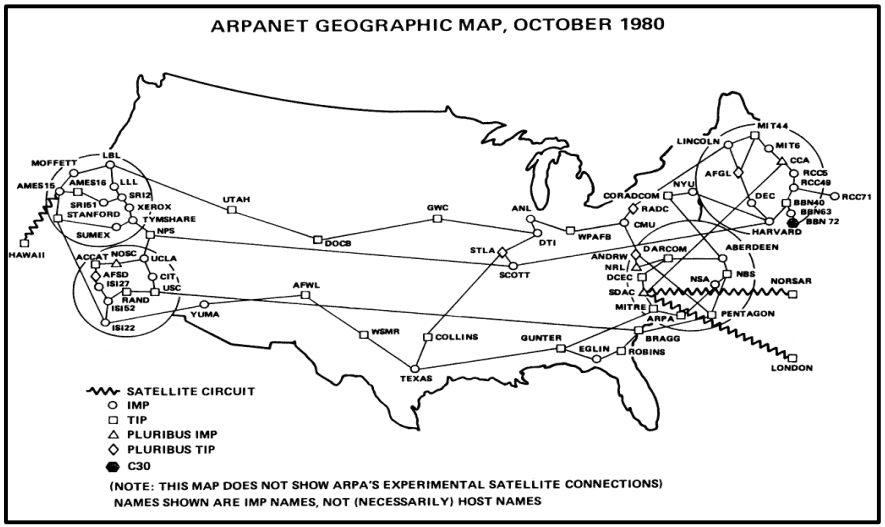
Sommario

- Introduzione ad Internet
- L'architettura TCP/IP
- Il protocollo IP
- Routing IP
- ARP
- ICMP
- DHCP
- Cenni su IPv6

Internet: storia

- Le origini di Internet si possono far risalire al progetto DARPA (Defense Advanced Research Project Agency) del Department of Defense (DOD) Americano (inizi anni 70')
- Necessità di interconnettere reti dei centri militari, universitari e di ricerca: definizione della rete ARPANET
- 1973 viene commissionato all'Università di Stanford il progetto di una suite di protocolli standard che garantissero connettività a livello di rete
- Verso la fine degli anni '70, tale sforzo portò al completamento dell'Internet Protocol Suite, di cui i due protocolli più noti sono il TCP e l'IP
  - **comunemente si fa riferimento ad essa con la sigla TCP/IP**
- RFC 791, "INTERNET PROTOCOL", Sept. 1981

ARPANET: 1980



Internet: storia (cont.)

- 1990: ARPANET cessa le sue attività
- 1990: Barners-Lee (CERN) definisce il WWW
- 1993: Andreessen (NCSA, Illinois) sviluppa il primo WWW browser
- Evoluzione:
  - **applicazioni e servizi principali:**
    - e-mail, ftp, telnet, news → www, e-mail, streaming, peer-to-peer
  - **velocità tipica delle portanti:**
    - 64 kbit/s → 2÷1000 Mbit/s
- Nuove problematiche:
  - **Qualità del servizio, multimedia, reti mobili**

Motivazioni del successo

- Sovvenzioni statali ($ 200 milioni nel periodo '86-'95)
- Assenza di vincoli architetturali forti: non richiede che tutti i sistemi siano basati sulla stessa architettura protocollare
  - **interconnessione di reti eterogenee**
- Modalità di trasferimento nello strato di rete senza connessione
  - **flessibilità rispetto a tecnologie di (sotto)rete anche molto diverse tra loro**
- Semplicità dei protocolli (inclusi quelli di gestione e controllo)
- Disponibilità immediata e gratuita del software, della documentazione tecnica e degli standards (anche nei primissimi stadi di sviluppo)
- Protocolli implementati in software
- Protocolli integrati nel sistema operativo UNIX
- Vasta disponibilità (spesso gratuita) di applicazioni (modello client/server e peer-to-peer)

Organi Regolatori

- ISOC (Internet SOCiety): Organo politico di rappresentanza di Internet
- IAB (Internet Architecture Board): Commissione di supervisione complessiva degli aspetti tecnici di Internet
- IETF (Internet Engineering Task Force): Comunità che specifica I protocolli di Internet ed emette documenti ad essa relativi. È diviso in Aree e Working Groups (WGs)
- IESG (Internet Engineering Steering Group): Organo di supervisione dell'IETF, costituito prevalentemente da IETF Area chairs
- IANA (Internet Assigned Number Authority): Autorità che disciplina l'uso di tutti i numeri, valori, costanti, well-known ports usati in Internet
- InterNIC (Internet Network Information Centre): Ente che assegna gli indirizzi IP ed i nomi di dominio

IETF

- L'organo di standardizzazione più importante per Internet dal punto di vista tecnico è l'IETF (Internet Engineering Task Force)
  - **definisce i protocolli riguardanti la rete Internet**
  - **gli standard prodotti vengono denominati RFC (Request For Comments) e numerati in ordine crescente**
  - **http:// www.ietf.org/**
- Processo di standardizzazione dell'IETF:
  - **Poche regole (*"Just Enough"*), flessibili, dinamiche e pragmatiche**
  - **Processo aperto a tutti i contributi**
  - **Nessuna votazione, bensì consenso**
  - **Prototipi disponibili prima (non dopo) la standardizzazione**
- Riassunti nel motto dell'IETF:
  - **"Rough consensus and running code!"**
    David D. Clark, MIT, in speech to IETF Plenary, ~1994.

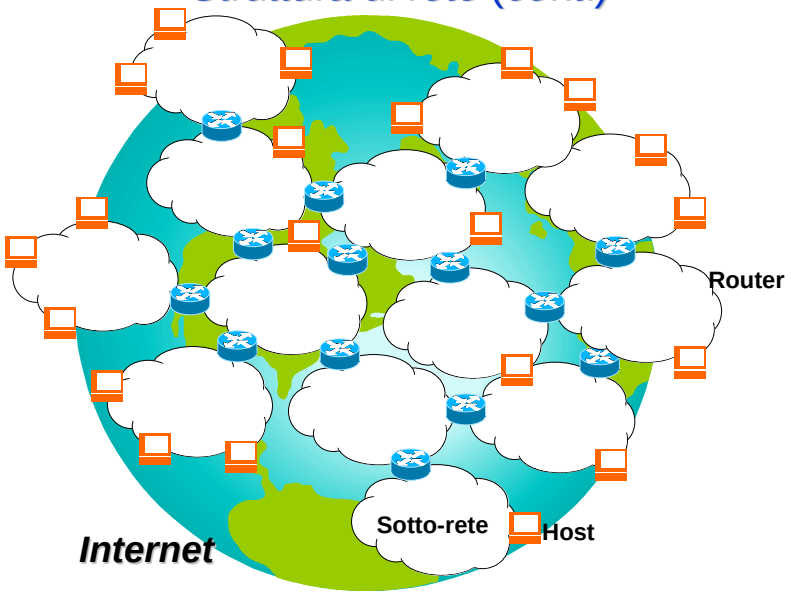
Struttura di rete

- Internet consiste di un insieme di reti interconnesse che possono essere considerate come un'unica entità
- Le reti sono collegate da apparati (nodi) di commutazione detti router, che hanno come funzione primaria quella di instradare i dati sulla base dell'indirizzo della rete destinataria
- La modalità di trasferimento nello strato di rete (IP) è senza connessione (CL)
  - **lo strato IP in genere non fornisce alcuna garanzia sulla qualità di servizio (grado di integrità informativa, ritardo di trasferimento, grado di trasparenza temporale, etc.)**
- La struttura di rete è non gerarchica

Struttura di rete (cont.)

- Il protocollo IP tratta tutte le sotto-reti in modo uguale
- Esempi di sotto-reti possono essere:
  - **una rete in area locale (e.g. Ethernet)**
  - **una rete in area metropolitana (e.g. anello SDH)**
  - **una rete geografica (e.g. rete PSTN/ISDN, o PLMN)**
  - **una connessione punto-punto dedicata**
  - **...**
- I protocolli TCP/IP (inteso come stack protocollare basato su IP)
  - **sono logicamente situati al di sopra di qualsivoglia altro protocollo di rete implementato all'interno delle singole sotto-reti (eventualmente duplicandone le funzioni)**
  - **sono in grado di operare su diverse piattaforme hardware (PC, PDA, Smartphone, Embedded PC, etc.) utilizzando svariati sistemi operativi (UNIX, Mac OS, MS-DOS, Windows, Linux, Symbian, etc.)**

Struttura di rete (cont.)



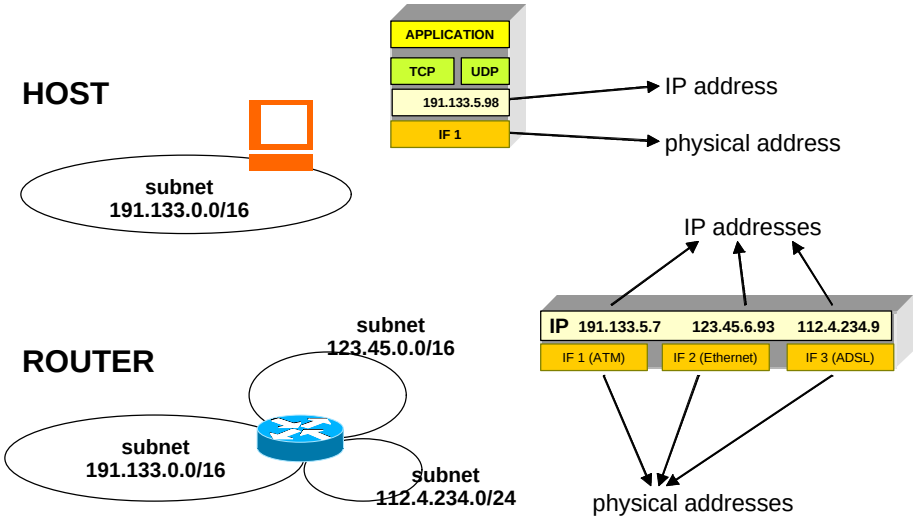
Tipi di reti sottostanti IP

- punto-punto
  - **le interfacce possono essere "unnumbered"**
  - **e.g.: linee dedicate o dial-up (PPP, SLIP)**
- multiaccesso con possibilità di broadcast
  - **più host possono comunicare direttamente senza passare per router intermedi**
  - **possibilità di broadcast**
  - **e.g. : LAN**
- multiaccesso senza possibilità di broadcast (Non Broadcast Multiple Access)
  - **più host possono comunicare direttamente senza passare per router intermedi**
  - **non c'è possibilità di broadcast**
  - **e.g. : X.25, Frame Relay, ATM, SDH, PSTN/ISDN, etc.**

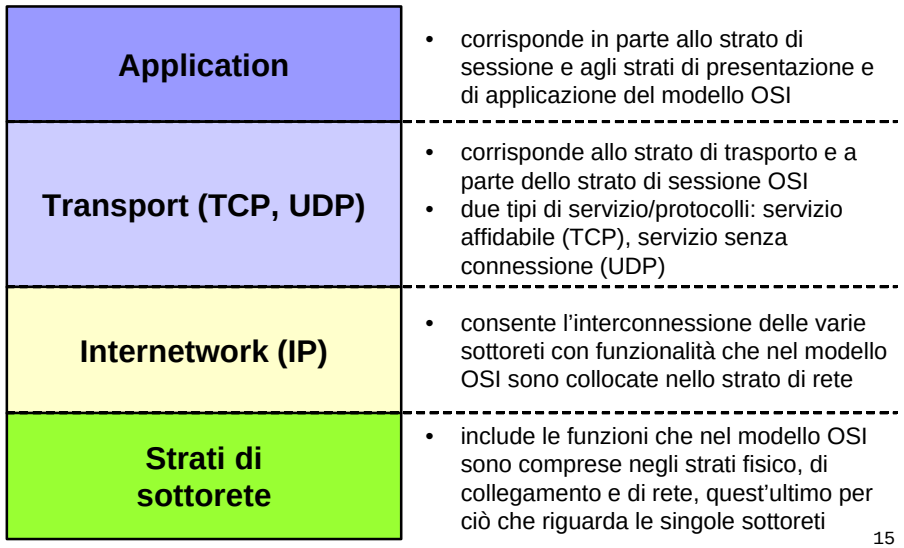
Hosts and Routers

- I nodi fondamentali all'interno di questa struttura sono gli hosts e i routers
  - **hosts:**
    - terminali IP
    - sono sorgente e destinazione di informazione, spesso hanno una sola interfaccia di rete e un indirizzo IP (ma in generale possono avere anche più di una interfaccia/indirizzo)
    - possono essere dei normali PC, workstation, palmari, telefoni cellulari o qualsiasi altro apparecchio connesso ad una rete IP
  - **routers:**
    - nodi di commutazione IP
    - in genere hanno due o più interfaccie di rete con corrispondenti indirizzi IP
    - inoltrano le unità informative IP da una rete ad un'altra (funzione di forwarding)
    - possono essere delle macchine dedicate (la maggior parte dei router commerciali) o con un OS aperto (e.g. Linux)

Hosts and Routers (cont.)

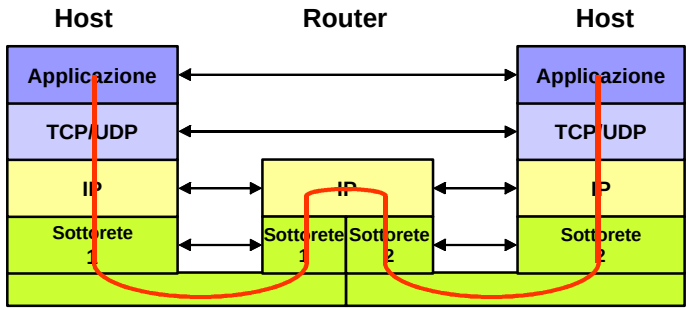


Architettura TCP/IP



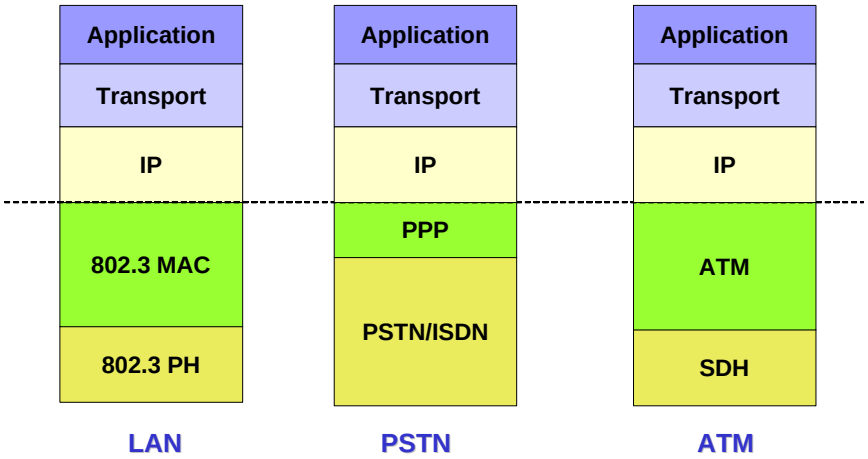
- corrisponde in parte allo strato di sessione e agli strati di presentazione e di applicazione del modello OSI
- corrisponde allo strato di trasporto e a parte dello strato di sessione OSI
- due tipi di servizio/protocolli: servizio affidabile (TCP), servizio senza connessione (UDP)
- consente l'interconnessione delle varie sottoreti con funzionalità che nel modello OSI sono collocate nello strato di rete
- include le funzioni che nel modello OSI sono comprese negli strati fisico, di collegamento e di rete, quest'ultimo per ciò che riguarda le singole sottoreti

Architettura TCP/IP



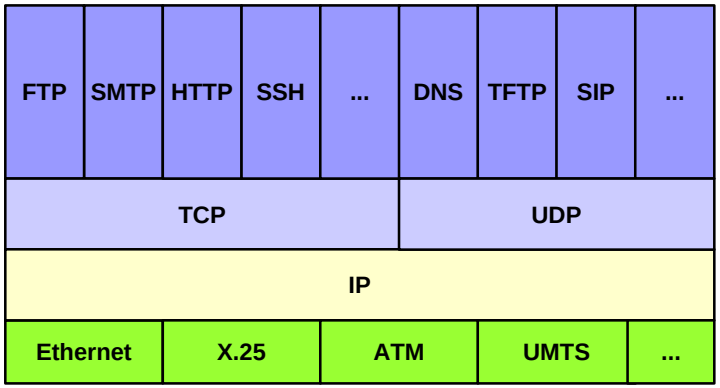
- I router implementano i protocolli IP, ICMP e i protocolli di routing

Architettura TCP/IP: Esempi

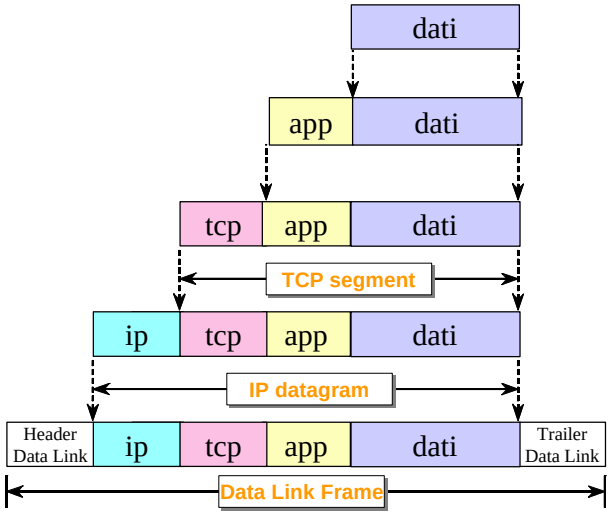


Architettura TCP/IP

- Esempio di pila dei protocolli Internet



Architettura TCP/IP: esempio di imbustamento



Architettura TCP/IP

- L'insieme di protocolli TCP/IP
  - **riesce a inter-connettere tutti i tipi di sotto-rete in quanto assume che le funzionalità degli strati sottostanti costituiscano solo una piattaforma per il trasferimento fisico**
  - **realizza tutte le funzioni tipiche per il trasporto dell'informazione: controllo di errore, indirizzamento, instradamento, frammentazione e aggregazione delle unità informative, inoltro in rete**
- Se alcune o tutte queste funzioni non erano state svolte da una particolare sotto-rete, TCP/IP le realizza; se erano già state volte le duplica, realizzandole nuovamente
- Ciò conduce ad eventuali duplicazioni di funzioni ma consente di non imporre alcun vincolo sulla tecnologia e sui protocolli delle sotto-reti di trasporto che interconnette (X.25, Frame Relay, ATM, LAN, MAN, ISDN, UMTS, etc.)

Architettura TCP/IP (cont.)

- Le prestazioni da estremo a estremo (velocità di trasmissione delle informazioni, grado di trasparenza temporale e di integrità informativa) sono fortemente legate alle caratteristiche delle sottoreti attraversate
- Il trasferimento delle unità informative può richiedere una frammentazione delle stesse laddove le dimensioni delle unità informative gestite dalle sotto-reti non coincidano con le dimensioni massime consentite

Internet Protocol (IP)

Internet Protocol (IP)

- "IP is the workhorse protocol of the TCP/IP protocol suite" (W. R. Stevens)
- Il protocollo IP (RFC 791, 919, 922, 950, 1349)
  - **è un protocollo di strato di rete (secondo il modello OSI)**
  - **opera con modalità di trasferimento connectionless (senza connessione), ovvero a datagramma**
    - Il termine connectionless significa che il protocollo IP non mantiene alcuna informazione di stato circa i pacchetti inoltrati; ciascun pacchetto è trattato independentemente da tutti gli altri
    - questo significa anche che i datagrammi IP possono essere consegnati fuori sequenza
  - **è di tipo NON affidabile e non fornisce alcuna garanzia sulla QoS (servizio "best effort")**
    - Il termine inaffidabile significa che non ci sono garanzie che un pacchetto IP giunga a destinazione, ne sui tempi di trasferimento

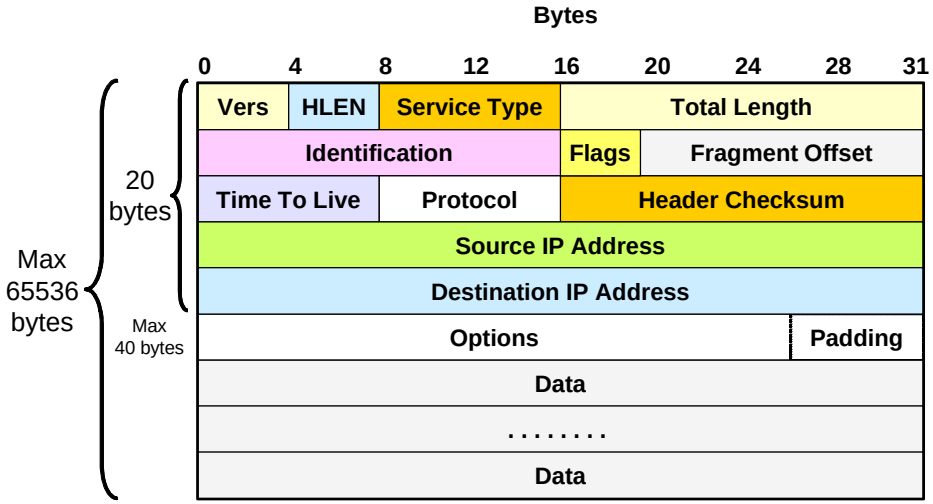
Internet Protocol (IP)

- Il protocollo IP esegue le seguenti principali funzioni:
  - **definisce l'unità base per il trasferimento dei dati (IP-PDU o datagramma)**
    - di lunghezza variabile (max 65536 ottetti)
  - **definisce lo schema di indirizzamento IP**
  - **definisce le modalità di instradamento dei datagrammi**
  - **esegue controllo di errore sull'intestazione IP (IP-PCI o IP header)**
  - **esegue, se necessario, la frammentazione e il ri-assemblaggio delle unità dati**

Internet Protocol (IP)

- Il protocollo IP in trasmissione
  - **riceve una unità dati dallo strato superiore (in genere lo strato di trasporto)**
  - **predispone l'opportuna intestazione (indirizzi src e dst, etc.)**
  - **sceglie il nodo successivo a cui consegnare il datagramma**
  - **eventualmente esegue frammentazione dello stesso**
  - **inoltra il datagramma attraverso l'opportuna interfaccia di rete**
- in ricezione
  - **riceve un datagramma dallo strato di sottorete**
  - **esamina l'intestazione e ne verifica la validità**
  - **verifica se il datagramma deve essere rilanciato**
  - **se sono dati locali, estrae il contenuto del datagramma e lo consegna all'opportuno protocollo di livello superiore**

Header IP



Header IP

- Vers (4 bits): versione del protocollo usata (attualmente IPv4)
- HLEN (4 bits): lunghezza dell'intestazione specificata in parole di 4 bytes (min 20 - max 60 bytes)
- TOS (Type Of Service): quando supportato dalla rete, permette di specificare un livello di qualità di servizio richiesto dall'utente (ad es. affidabilità o velocità di trasferimento)
  - **in passato non usato**
  - **ora utilizzato da reti a servizi differenziati (Differentiated Services)**
- Total length: (16 bits) specifica la lunghezza totale (inclusa l'intestazione) del datagramma, misurata in bytes (valore max: 2^{16}=65536 bytes)
- Identification: (16 bits) numero identificativo del datagramma; è ereditato dagli eventuali frammenti
- Flags: è un campo di 3 bits usato per la frammentazione: X, DF e MF
  - **X: non usato e posto a zero**
  - **DF: Don't Fragment; se 0 indica che il datagramma può essere frammentato, se 1 no**
  - **MF: More Fragment; se 0 indica che è l'ultimo frammento, se 1 che ci sono altri frammenti**

Header IP

- Fragment Offset: (13 bits); posizione del frammento all'interno del datagramma, espresso in unità di 8 bytes può numerare 8192 frammenti; se uno o più frammenti non viene ricevuto (a destinazione), verrà scartato l'intero datagramma
- Time to Live: (8 bits); indica il numero massimo di salti residui che il datagramma può effettuare in rete. E' aggiornato da ogni router attraversato
- Protocol: indica a quale protocollo dello stato superiore deve essere trasferito il contenuto informativo del datagramma (es. TCP=6, UDP=17, ICMP=1)
- Header Checksum (16 bits): controllo di errore sull'intestazione; calcolato come somma complemento a 1; se viene rivelato un errore il datagramma viene scartato
- Source Address: (32 bits); indirizzo dell'host sorgente
- Destin. Address: (32 bits); indirizzo dell'host destinazione IP (ovvero dell'host, non dell'utente finale)

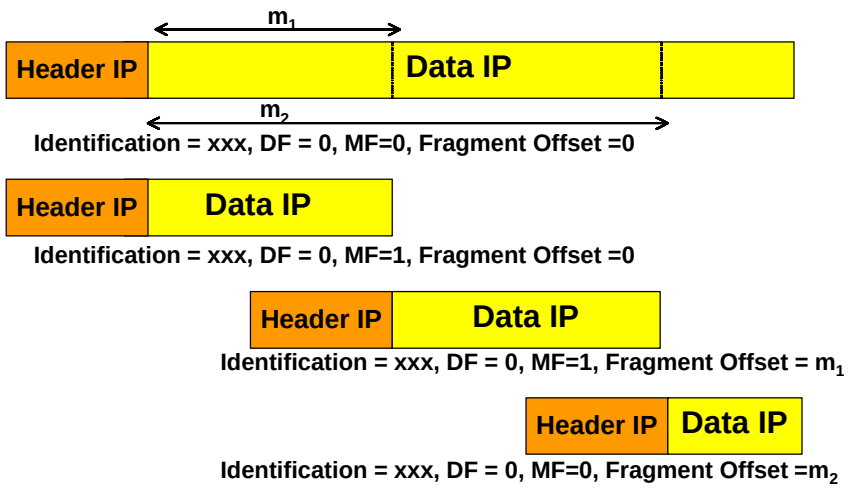
Header IP

- Options: campo di lunghezza variabile (multipli di 8 bit) che può essere omesso. È composto da tanti ottetti quante sono le opzioni implementate. Ad esempio:
  - **Record Route Option (RRO): consente al mittente di creare una lista vuota di indirizzi IP in modo che ogni nodo attraversato inserisce il suo indirizzo in questa lista**
  - **Source Route Option (strict o loose): consente al mittente di specificare i nodi attraverso i quali vuole che transiti il datagramma**
  - **Timestamp Option: come RRO con in più l'istante temporale in cui il datagramma attraversa i diversi nodi**
- Padding: rende la lunghezza dell'intestazione multiplo intero di 32 bit mediante introduzione di zeri

Frammentazione

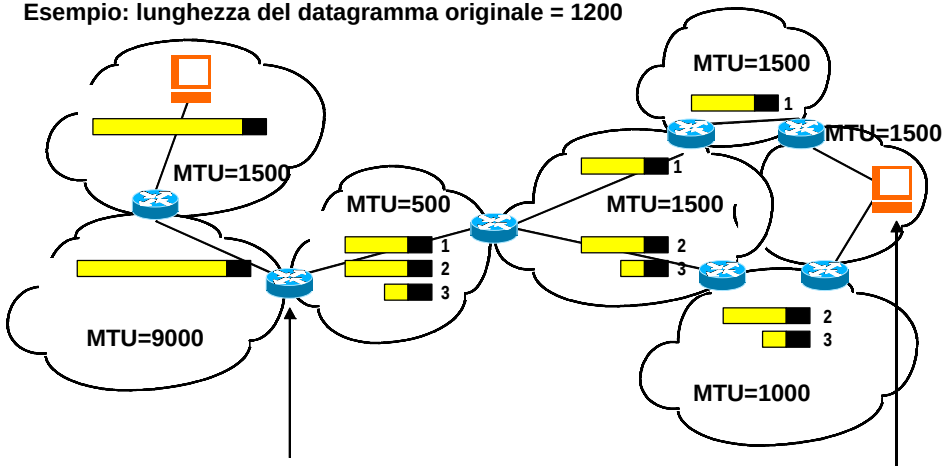
- Ogni rete fisica ha un valore massimo di lunghezza della propria unità informativa
  - **Maximum Transmission Unit - MTU**
- La frammentazione di un datagramma IP è necessaria se il valore della MTU nella sottorete fisica è inferiore alla lunghezza del datagramma
- La frammentazione è effettuata dal router/host prima del rilancio nella sottorete
- La ricomposizione del datagramma originale è effettuata dall'host di destinazione

Frammentazione



Frammentazione

Esempio: lunghezza del datagramma originale = 1200



Esempio di datagramma IP

rappresentazione esadecimale	*rappresentazione binaria*	
45 00 00 20	01000101 00000000 00000000 00100000	*Header IP*
fe be 00 00	11111110 10111110 00000000 00000000	
80 11 ca b7	10000000 00010001 11001010 10110111	
8d 89 2b 20	10001101 10001001 00101011 00100000	
8d 89 2b 24	10001101 10001001 00101011 00100100	
06 8c 52 4c	00000110 10001100 01010010 01001100	*dati*
00 0c 70 ce	00000000 00001100 01110000 11001110	
63 69 61 6f	01100011 01101001 01100001 01101111	

01000101 00000000 00000000 00100000 11111110 10111110 00000000 00000000 10000000 00010001 11001010 10110111 10001101 10001001 00101011 00100000 10001101 . . .

Indirizzamento IP

Schema di indirizzamento

- Internet consente ad ogni nodo connesso alla rete di comunicare con ogni altro nodo di Internet
- Al tal fine è necessario un metodo globale di identificazione e indirizzamento di tutti i nodi (host e router)
  - **lo schema di indirizzamento è indipendente da quello utilizzato dalle singole sottoreti sottostanti, che in genere possono essere diverse tra loro (Ethernet, X.25, rete telefonica etc.)**

Schema di indirizzamento

- Un indirizzo IP (IP Address) ha una lunghezza di 32 bits
- Identifica un nodo e non uno specifico utente; l'identificazione di un utente all'interno di un host è affidata ai protocolli di strato superiore (TCP o UDP)
- L'identificativo del IP-SAP è dato alla coppia *indirizzo_IP* + *protocol_id*
- Se un nodo è connesso a più di una rete avrà un indirizzo IP per ogni rete (interfaccia di rete); ciò si verifica nei:
  - **routers**
  - **multi-homed hosts**
- Gli indirizzi devono essere unici in tutta la rete (è possibili attribuire indirizzi arbitrari ad una sub-rete TCP/IP solo se questa non è connessa con altre reti)
- Lo schema di indirizzamento IP è stato progettato per consentire un efficiente instradamento
  - **era però stato pensato per una rete con dimensioni decisamente inferiori alle attuali**

Schema di indirizzamento

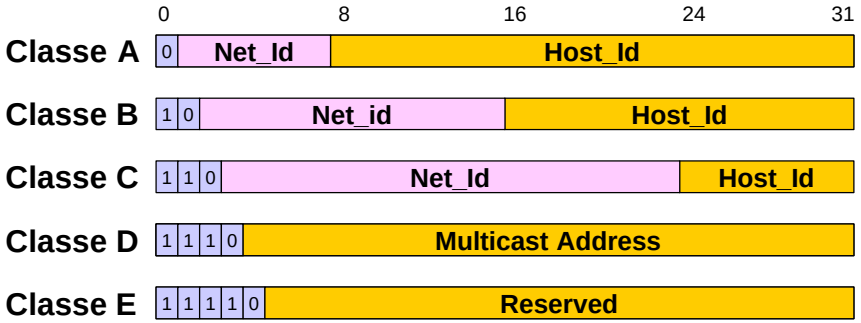
- Un indirizzo IP identifica sia l'host che la rete a cui l'host è connesso
  - **L'indirizzo di un host deve essere coerente con quello della rete in cui si trova**
  - **Se un host si muove da una rete, il suo indirizzo deve essere cambiato**
- In origine (1981, RFC 791) lo schema di indirizzamento era di tipo gerarchico a due soli livelli
  - **Indirizzi formati da due parti**
    - net_id: identificativo di rete o network prefix
    - host_id: identificativo dell'host all'interno della rete

IP_address = net_id + host_id

- La divisione tra *net_id* e *host_id* non è fissa
  - **originariamente determinata in modo univoco dai primi bit dell'indirizzo**
  - **attualmente un indirizzo è suddiviso in identificativo/prefisso di rete (network prefix) e identificativo dell'host, ma quando necessario la divisione viene indicata esplicitamente (tramite la netmask)**
- Il network prefix viene utilizzato principalmente per verificare l'appartenenza di un nodo ad una sottorete (e.g. per l'istradamento)

Schema di indirizzamento

- Gli indirizzi IP originariamente sono stati suddivisi in 5 classi (gruppi di indirizzi)

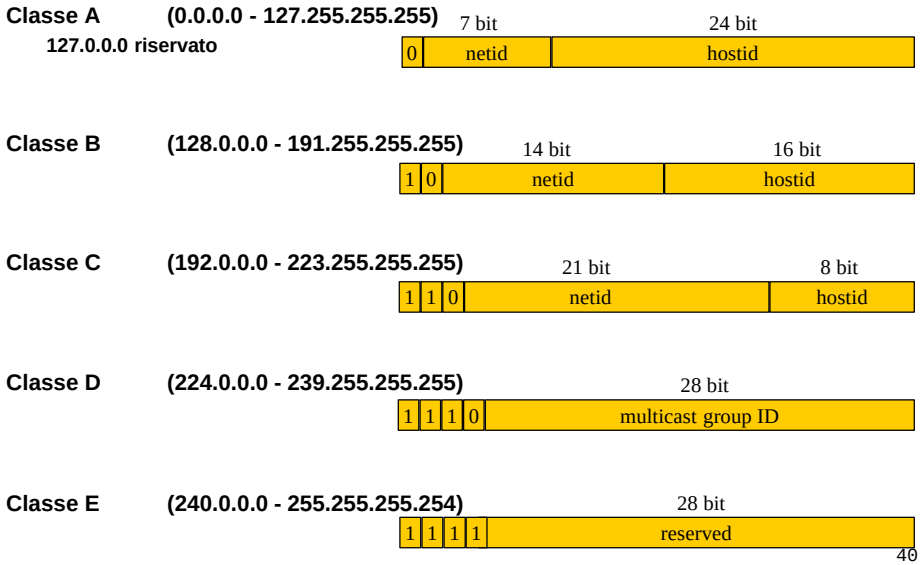


Schema di indirizzamento

- Classi di indirizzi IP

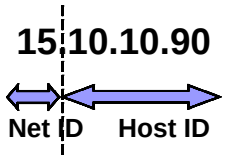
Classe	Bit iniziali	Net_Id	Host_Id	"Reti" disponibili	"Host" disponibili
A	0	7 bit	24 bit	128	16.777.216
B	10	14 bit	16 bit	16384	65.536
C	110	21 bit	8 bit	2.097.152	256
D	1110	Indirizzo multicast: 28 bit Indirizzi possibili: 268.435.456			
E	1111	Riservata per usi futuri: 28 bit Indirizzi possibili: 268.435.456			

Indirizzi IP

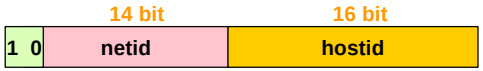


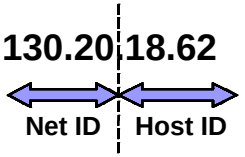
Indirizzi IP: esempi

- Esempio di indirizzo di classe A:

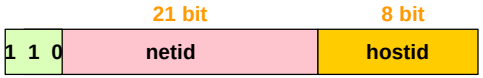


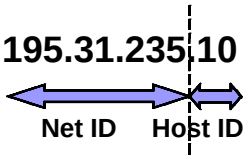
Esempio di indirizzo di classe B:





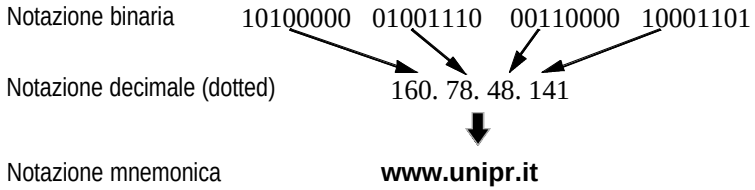
Esempio di indirizzo di classe C:





Schema di indirizzamento

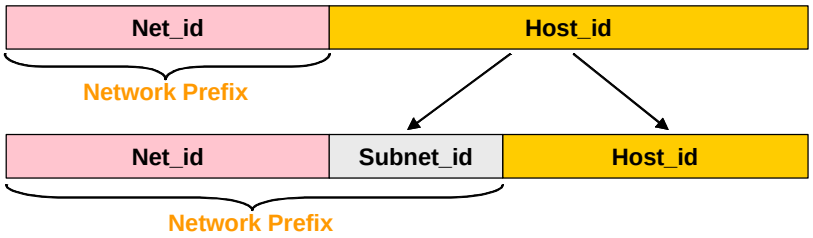
- Notazione numerica, “dotted” e “mnemonica”:



- Un opportuno protocollo applicativo (DNS) provvede a tradurre un indirizzo numerico in mnemonico e viceversa

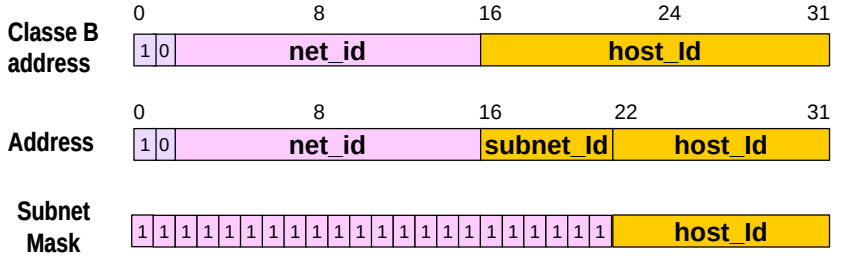
Schema di indirizzamento

- La struttura di indirizzamento a due livelli gerarchici era sufficiente nella fase iniziale di Internet
- Nel 1984 è stato aggiunto un terzo livello gerarchico
  - **il livello di sottorete (subnet)**
- Si utilizzano alcuni bit dell’host_id originario per codificare il subnet_id
  - **si riduce così la parte di host_id rimanente**



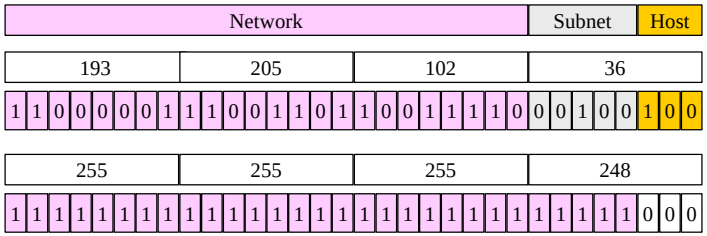
Subnetting

- Il campo subnet_id e il complessivo network prefix è identificato da una maschera denominata “subnet mask” o brevemente “netmask”
- Una subnet mask è una parola di 32 bit in cui
  - **i bit uguali a “1” identificano i bit del net_id e del subnet_id (network prefix)**
  - **i bit uguali a “0” identificano i bit dell’host_id**



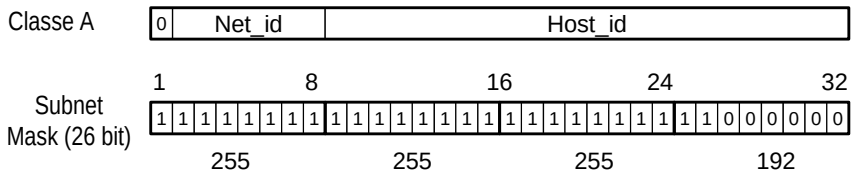
Subnetting

- Nel caso in cui il network prefix coincide con il net_id (no subnetting) si ha la "netmask naturale" (netmask implicita)
- Si parla di *subnetting* quando la nuova maschera un numero di bit a 1 maggiore rispetto alla maschera naturale
- Grazie al *subnetting* aumentano gli indirizzi di rete a disposizione e migliora la gestione degli indirizzi
- Esempio:



Subnetting statico

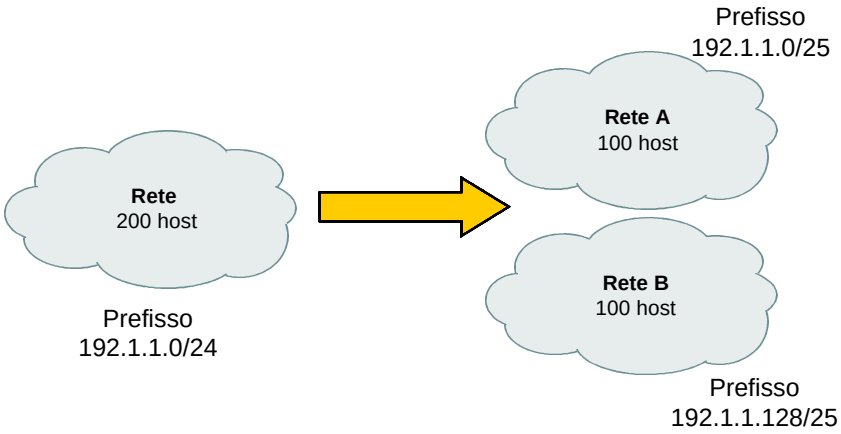
- Tutte le subnet a partire dalla stessa rete hanno la stessa maschera
- Esempio:



- **numero massimo di sottoreti possibili = 2^{18} = 226.144**
- **numero massimo di host per sottorete = 2^{6} = 64**

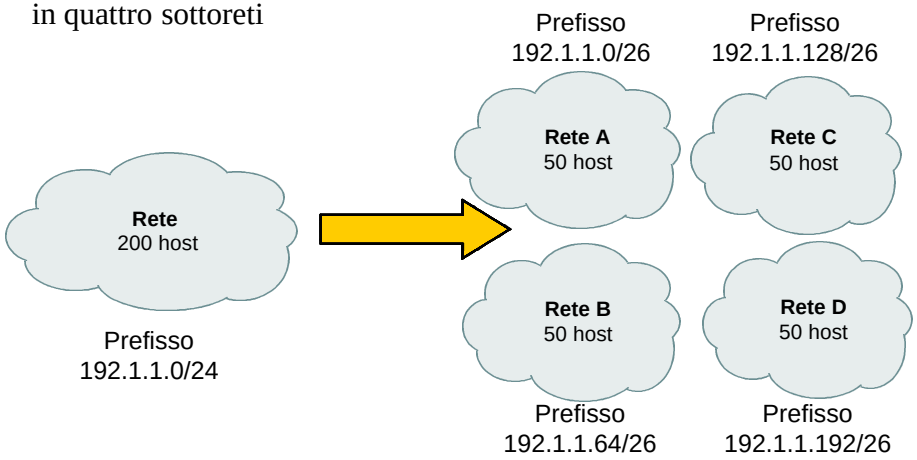
Subnetting statico: Esempio 1

- Subnetting di una rete di classe C in due sottoreti



Subnetting statico: Esempio 2

Subnetting di una rete di classe C in quattro sottoreti

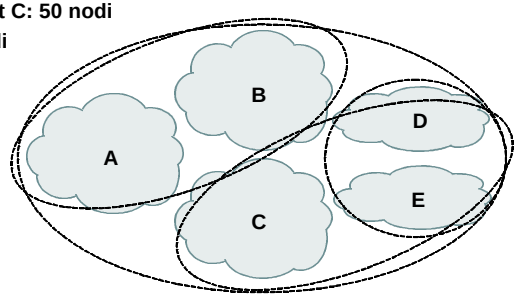


Subnetting a lunghezza variabile

- Le sottoreti di una rete usano maschere diverse
- Consente di gestire sottoreti di dimensione diversa
  - **differente numero max di nodi in ogni sottrete**
- Esempio
  - **rete di classe C (256 indirizzi)**
    - 1 rete con 128 indirizzi
    - 1 rete con 64 indirizzi
    - 2 reti con 32 indirizzi

Subnetting a lunghezza variabile: Esempio

- A partire da un indirizzo di classe B
  - **165.214.0.0**
- Ricavare 5 sottoreti del tipo
  - **Subnet A, Subnet B, Subnet C: 50 nodi**
  - **Subnet D, Subnet E: 20 nodi**



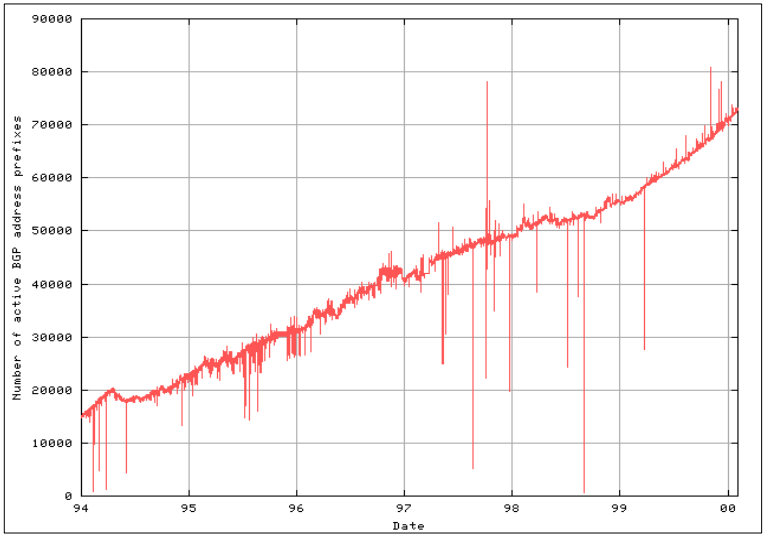
- subnetting
  - **4 sottoreti con 64 indirizzi ciascuna (Host_id: 6 bit) (subnet mask 255.255.255.192)**
  - **1 sottorete divisa ulteriormente in due sottoreti con 32 indirizzi ciascuna (Host_id: 5 bit) (subnet mask 255.255.255.224)**

Netmask: valori leciti

- Per come è stata definita una netmask, i suoi 4 byte possono assumere solo i seguenti valori decimali

decimale	*binario*	*# di host_id (se ultimo byte)*
128	1000 0000	(128)
192	1100 0000	(64)
224	1110 0000	(32)
240	1111 0000	(16)
248	1111 1000	(8)
252	1111 1100	(4)
254	1111 1110	(2)
255	1111 1111	(1)

Esplosione delle tabelle di routing



http://www.telstra.net/ops/bgptable.html

Esaurimento degli indirizzi IP

- Il progressivo esaurimento degli indirizzi IP unitamente alla rapida crescita delle dimensioni delle tabelle di routing ha spinto l'IETF (*Internet Engineering Task Force*) ad intraprendere delle azioni preventive
- Tali misure preventive possono essere raggruppate nelle seguenti categorie:
  - **Assegnazione razionale degli indirizzi IP**
  - ***Classless InterDomain Routing* (CIDR)**
  - **Indirizzi privati e *Network Address Translation* (NAT)**
  - **IP versione 6 (IPv6)**

Classless Inter Domain Routing

- Nel 1996 erano stati assegnati
  - **100 % degli indirizzi di classe A**
  - **61.95 % degli indirizzi di classe B (rischio esaurimento)**
  - **36.44 % degli indirizzi di classe C**
- CIDR è stato ideato per
  - **affrontare l'esaurimento dello spazio di indirizzamento di IP (raddoppio degli host ogni anno)**
  - **diminuire la complessità delle tabelle di instradamento nei router**
  - **velocizzare le operazioni di instradamento nei router**
- CIDR tende ad eliminare la divisione in classi di indirizzi anche nei router più interni alla rete Internet
- CIDR è basato sulla tecnica *Supernetting*

Supernetting

- Strategia di assegnazione di indirizzi IP in modo aggregato e gerarchico
- Più indirizzi di rete assegnati ad un ISP (Internet Service Provider) vengono presi contigui, in modo da poter essere rappresentati e pubblicizzati tramite un unico indirizzo aggregato
  - **esempio,**
    - le 4 reti: 193.200.16.0/24, 193.200.17.0/24, 193.200.18.0/24, 193.200.19.0/24
    - possono essere viste come una unica rete (aggregata) con indirizzo: 193.200.16.0/22

Classless Inter Domain Routing

- Nuova strategia di assegnazione degli indirizzi
  - **la metà superiore della classe A (da 64 a 127) è stata riservata per usi futuri**
  - **un indirizzo di classe B è assegnati solo se la rete ha**
    - almeno 32 sotto-reti
    - oltre 4096 host complessivi
  - **gli indirizzi della metà inferiore della classe C (da 192.0.0 a 207.255.255) sono divisi in otto blocchi assegnati ciascuno ad una autorità geografica**
    - gli indirizzi della metà superiore della classe C (da 208.0.0 a 223.255.255) non sono assegnati
  - **ad una rete che non soddisfa i requisiti per la classe B è assegnato un certo numero di blocchi contigui di indirizzi di classe C**
    - la rete è caratterizzata da un unico *prefisso* (insieme dei bit più significativi)
    - la rete sarà individuata nei router solo dal *prefisso*

Classless Inter Domain Routing

- Pianificazione geografica degli indirizzi di classe C

Multiregional	**192.0.0**	÷	**193.255.255**
Europe	**194.0.0**	÷	**195.255.255**
Others	**196.0.0**	÷	**197.255.255**
North America	**198.0.0**	÷	**199.255.255**
Central/South America	**200.0.0**	÷	**201.255.255**
Pacific Rim	**202.0.0**	÷	**203.255.255**
Others	**204.0.0**	÷	**205.255.255**
Others	**206.0.0**	÷	**207.255.255**

- Tutte le reti appartenenti ad una regione geografica sono identificate dagli stessi 7 bit di prefisso
  - **Esempio: Europa**
    - da 194 = 11000010 0 a 195 = 11000011 1

Classless Inter Domain Routing

- Esempio 1
  - **Ad un grande Internet Service Provider (ISP) sono assegnati 2048 blocchi di indirizzi di classe C**
    - da 198.24.0.0 (11000110.00011000.00000000.0)
    - a 198.31.255.0 (11000110.00011111.11111111.0)
  - **CIDR mask per il grande ISP = 198.24.0.0/13**
  - **Un piccolo ISP locale richiede al grande ISP 16 blocchi di indirizzi di classe C**
    - da 198.24.16.0 (11000110.00011000.00010000.0)
    - a 198.24.31.0 (11000110.00011000.00011111.0)
  - **CIDR mask per il piccolo ISP locale = 198.24.16.0/20**

Classless Inter Domain Routing

- Esempio 2
  - **Ad una organizzazione sono assegnati 2048 indirizzi di classe C**
    - da 194.32.136.0 (11000010.00100000. 10001000.0)
    - a 194.32.143.0 (11000010. 00100000.10001111.0)
  - **CIDR mask per il grande ISP = 198.32.136.0/21**

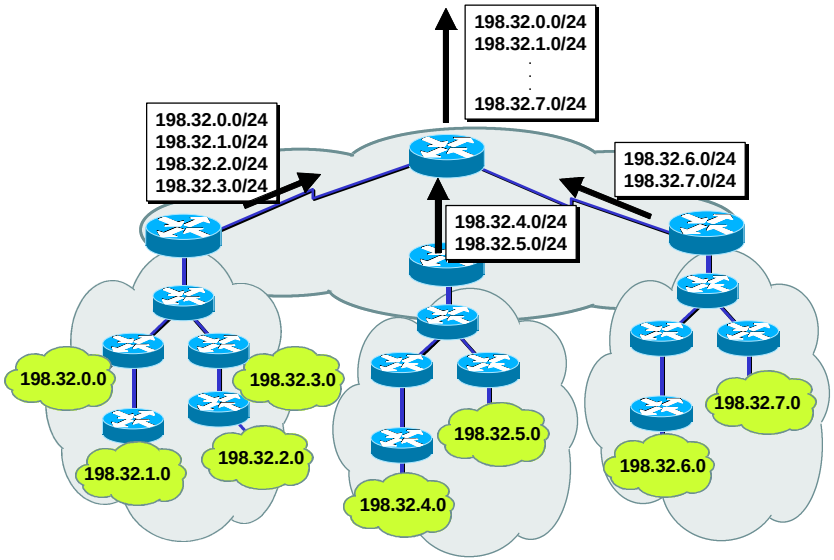
Classless Inter Domain Routing

- Da un indirizzo IP a 32 bit e dalla relativa maschera di rete a 32 bit si individua il prefisso con una operazione di AND
- In una routing table un blocco di indirizzi può essere rappresentato da un unico elemento (di lunghezza variabile) corrispondente al prefisso (Supernetting)

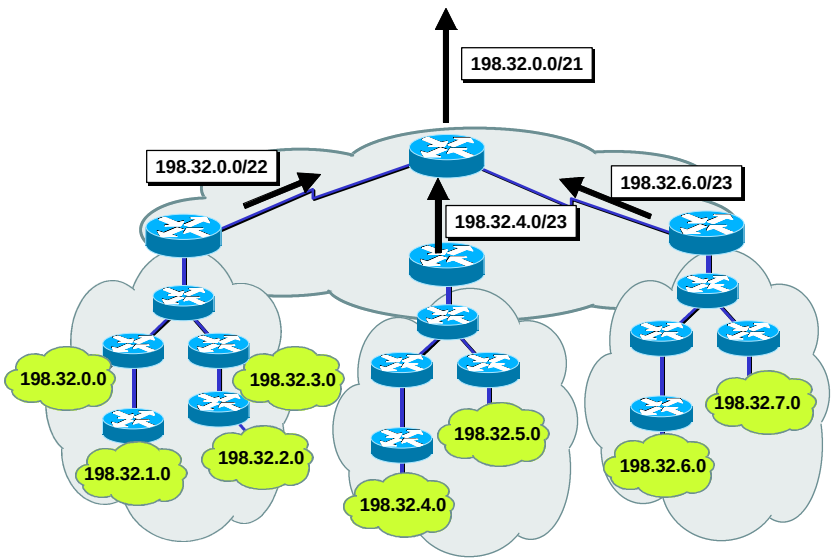
```
11000000 00100000 10001000 00000000 = 192.32.136.0 (class C address)
11111111 11111111 11111000 00000000   255.255.248.0 (network mask)
=================================== logical_AND
11000000 00100000 10001             = 192.32.136 (IP prefix)

11000000 00100000 10001111 00000000 = 192.32.143.0 (class C address)
11111111 11111111 11111000 00000000   255.255.248.0 (network mask)
=================================== logical_AND
11000000 00100000 10001             = 192.32.136 (same IP prefix)
```

- Viene scelto l'instradamento verso la direzione corrispondente al prefisso di lunghezza maggiore (Longest Prefix Matching)

Esempio di Routing Tables senza CIDR



Esempio di Routing Tables senza CIDR



Indirizzi IP particolari

All 0s		**This host[1]**
All 0s	Host	**Host on this net[1]**
All 1s		**Limited broadcast (local net) [2]**
Net	All 0s	**Network address**
Net	All 1s	**Directed broadcast for net [2]**
127	Anything (often 1)	**Loopback[3]**

[1] Utilizzabile solo come indirizzo sorgente(usato al bootstrap)
[2] Può essere usato solo come indirizzo destinazione
[3] Non deve essere propagato dai nodi sulla rete

Indirizzi privati

- The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets [RFC 1918]:

  10.0.0.0 - 10.255.255.255 (10/8 prefix)

  172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

  192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

- In pre-CIDR notation:
  - **The first block is a single class A network number,**
  - **the second block is a set of 16 contiguous class B network numbers,**
  - **the third block is a set of 256 contiguous class C network numbers.**

Indirizzi privati

- Ogni rete può utilizzare al suo interni qualsiasi indirizzo appartenente a questi insiemi
- I router della rete pubblica non rilanciano pacchetti con indirzzo di destinazione privato
  - **I router di bordo della rete che usa indirizzi privati non propagheranno all'esterno tramite protocolli di rouing informazioni di istradamento relativi alle sottoreti con indirizzi privati**
- Un host con un indirizzo privato non ha la possibilità di connettersi alla rete IP pubblica (Internet) direttamente tramite IP
  - **un host con un indirizzo privato può però comunicare con host pubblici tramite rilancio effettuato a livello applicativo**
    - "Application Level Gateway (Proxy)"
  - **un ulteriore meccanismo che permette di interconnettere due reti con indirizzamento differente (e.g. privato-pubblico) è il NAT (vedi seguito)**

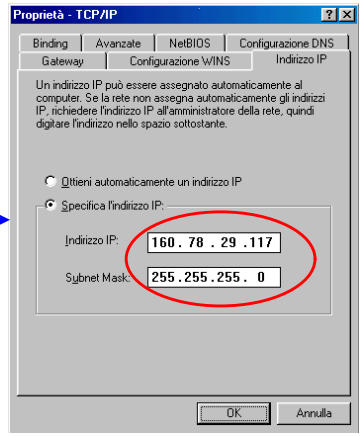
Configurazione di un nodo IP

Configurazione di un nodo Unix/Linux

- Ifconfig
  - **mostra / configura le interfacce di rete**
- route
  - **mostra / manipola la tabella di routing IP (print, add, delete)**
- arp
  - **manipola la cache ARP del sistema**
- nslookup
  - **effettua interrogazioni al DNS**
- netstat
  - **mostra connessioni di rete, tabelle di routing, statistiche sulle interfacce, connessioni masquerade e messaggi netlink**

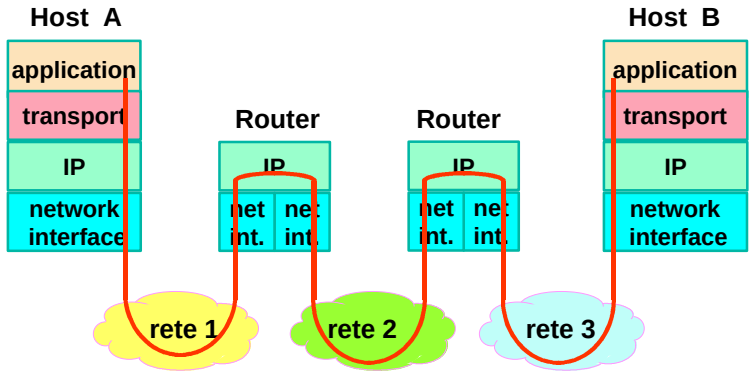
Configurazione di un nodo windows

- Ipconfig
  - **mostra le configurazioni IP di tutte le interfacce di rete**
- winipcfg (win98/ME)
  - **tool grafico per visualizzare le impostazioni di rete**
- netsh (win2000/XP)
  - **tool per modificare le impostazioni di rete**
- control panel / network / TCP/IP
  - **impostazioni di rete (win98)**
- route
- arp
- nslookup
  - **(winNT, windows2000/XP)**
- netstat



Routing IP

Routing IP



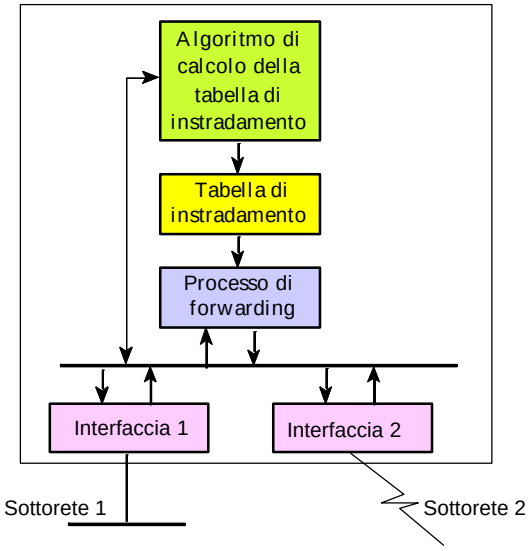
Router

- I router hanno il compito di instradare i pacchetti IP attraverso la rete
  - **permettono di far comunicare host che non sono connessi direttamente alla stessa sottorete IP, facendo transitare i datagrammi IP da una sottorete ad un'altra**
    - ricevono i datagrammi IP da un'interfaccia di ingresso e li inoltrano su una opportuna interfaccia di uscita

- Si distinguono dagli Host perchè:
  - **Inoltrano i datagrammi IP diretti ad altri nodi**

- In genere:
  - **hanno più di un'interfaccia (e in genere un indirizzo IP per ogni interfaccia)**
  - **possono utilizzare "protocolli di routing" per aggiornare dinamicamente le proprie tabelle di routing**

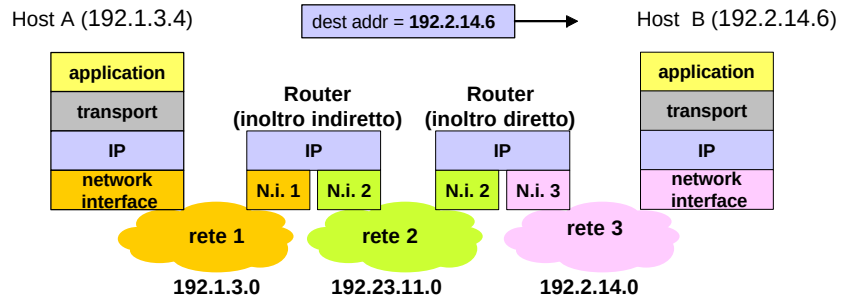
Architettura di un Router



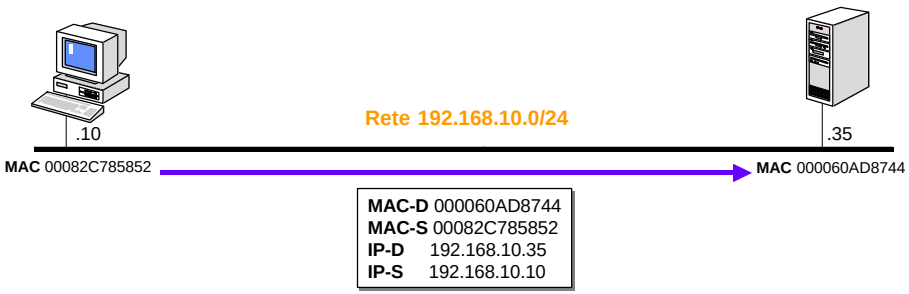
Instradamento (1/3)

- dato un datagramma IP in uscita da un nodo (host o router), si possono distinguere due casi di instradamento:
  - **instradamento diretto:**
    - l'host destinazione è nella stessa sottorete dove si trova il nodo che sta instradando il datagramma IP
  - **instradamento indiretto:**
    - l'host destinazione non si trova in nessuna delle sottoreti a cui è connesso il nodo che sta instradando il pacchetto
    - il datagramma viene consegnato ad un next hop router che avrà il compito di far proseguire il datagramma verso l'host destinazione
    - il datagramma passa da un nodo ad un altro finché raggiunge un nodo (router) connesso alla stessa sotterete in cui si trova l'host di destinazione
    - a questo punto il datagramma viene instradato direttamente al (host) destinatario (instradamento diretto)

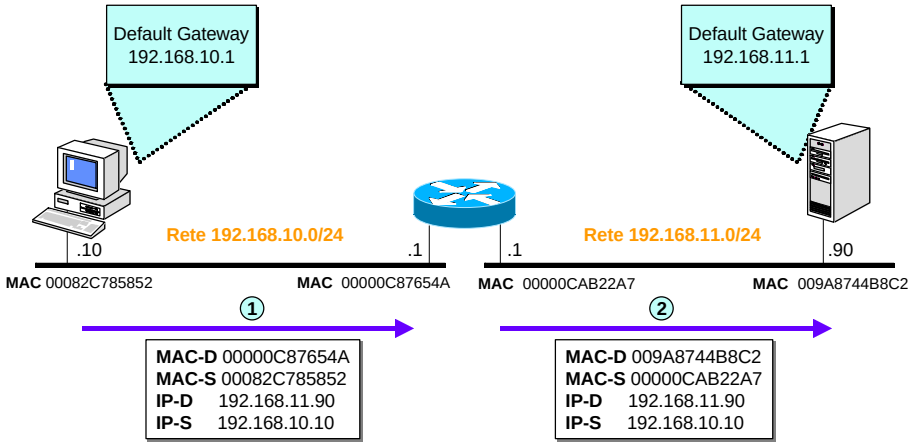
Instradamento (2/3)



Forwarding diretto: Esempio



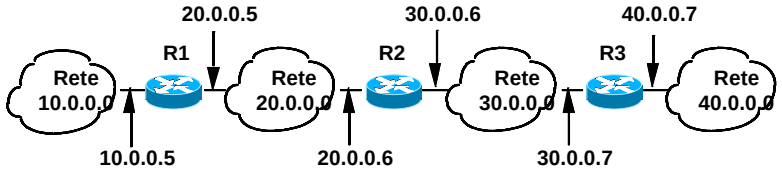
Forwarding indiretto: Esempio



Instradamento (3/3)

- La decisione riguardo quale “next-hop node” utilizzare per instradare il datagramma viene presa in base ad una tabella di instradamento (routing table)
- La routing table di un nodo (host o router) specifica solo un passo lungo il cammino verso l’host di destinazione
  - **Un host/router non conosce il cammino completo, ma solo il passo successivo verso la destinazione**
- La RT contiene le coppie (dest , next-hop)
  - **dest : indirizzo della rete di destinazione**
  - **next-hop : indirizzo del prossimo router verso la rete di destinazione**
- I nodi devono conoscere l’indirizzo del next-hop router
- Nota: nel caso di instradamento diretto l’indirizzo di destinazione apparterrà ad una delle sottoreti a cui il nodo è direttamente connesso

Tabelle di instradamento (1/4)



Routing Table di R2	
Net_Id	Router_Id
20.0.0.0	Instradamento diretto
30.0.0.0	Instradamento diretto
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

Tabelle di instradamento (2/4)

- L’informazione comunemente contenuta in ogni riga di una tabella di instradamento è:
  - **Dest net address:** rete di destinazione
  - **Subnet Mask:** porzione dell’indirizzo IP indicante il prefisso di rete
  - **Next Hop:** IP address del router successivo verso la destinazione
  - **Interface:** identificatore della porta fisica dove trovare il next hop
  - **Metric:** peso assegnato al cammino
- La coppia dest_net_addr + subnet_mask
  - **serve per identificare la possibile sottorete/host di destinazione**
- La coppia next_hop + interface
  - **serve per determinare univocamente dove instradare il datagramma**
- Se ci sono più righe che corrispondono, viene scelta quella con network prefix (netmask) più lungo
  - **longest prefix matching**

Tabelle di instradamento (3/4)

- Esempio di una tabella di instradamento di un host

windows:

```
Indirizzo rete            Maschera Indirizzo gateway   Interfac.  Metric
        0.0.0.0          0.0.0.0     150.100.33.1    150.100.33.18   1
      127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1   1
    150.100.33.0    255.255.255.0    150.100.33.18    150.100.33.18   1
   150.100.33.18  255.255.255.255        127.0.0.1        127.0.0.1   1
 150.100.255.255  255.255.255.255    150.100.33.18    150.100.33.18   1
      224.0.0.0        224.0.0.0    150.100.33.18    150.100.33.18   1
255.255.255.255  255.255.255.255    150.100.33.18    150.100.33.18   1
```

linux:

```
Destination     Gateway         Genmask         Flags   MSS Window Iface
150.100.33.0    *               255.255.255.0   U      1500 0      eth0
127.0.0.0       *               255.0.0.0       U      3584 0      lo
default         150.100.33.1    0.0.0.0         UG     1500 0      eth0
```

Tabelle di instradamento (4/4)

- Esempio di una tabella di instradamento di un router (linux)

```
Destination     Gateway         Genmask         Flags   MSS Iface
150.100.33.0    *               255.255.255.0   U      1500 eth0
150.100.34.0    *               255.255.255.0   U      1500 eth1
150.100.35.0    *               255.255.255.0   U      1500 eth2
127.0.0.0       *               255.0.0.0       U      3584 lo
default         150.100.35.1    0.0.0.0         UG     1500 eth2
```


Longest Prefix Matching

- Instradamento di 2 datagrammi
  - **indirizzo dest. 198.15.7.3**
  - **indirizzo dest. 198.15.7.4**
- Matching:
  - **198.15.7.3**
    - R1: matching prefisso 16
    - R7: matching prefisso 24
    - R4: matching prefisso 32
  - **198.15.7.4**
    - R1: matching prefisso 16
    - R7: matching prefisso 24
    - R4: no matching
- Scelta instradamento:
  - **198.15.7.3 ⇒ R4**
  - **198.15.7.4 ⇒ R7**

Tabella di instradamento

Prefix	Next hop
198.15.0.0/16	**R1**
198.15.7.0/24	**R7**
198.15.7.3/32	**R4**

Tabelle di instradamento: Esempio di CIDR (1/3)

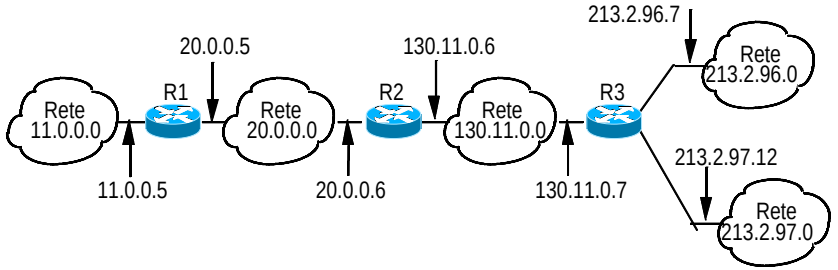


Tabella di instradamento di R2

Dest network	*Subnet mask*	*Next hop*
20.0.0.0	255.0.0.0	diretto
130.11.0.0	255. 255.0.0	diretto
11.0.0.0	255.0.0.0	20.0.0.5
213.2.96.0	255. 255.255.0	130.11.0.7
213.2.97.0	255. 255.255.0	130.11.0.7

Tabelle di instradamento: Esempio di CIDR (2/3)

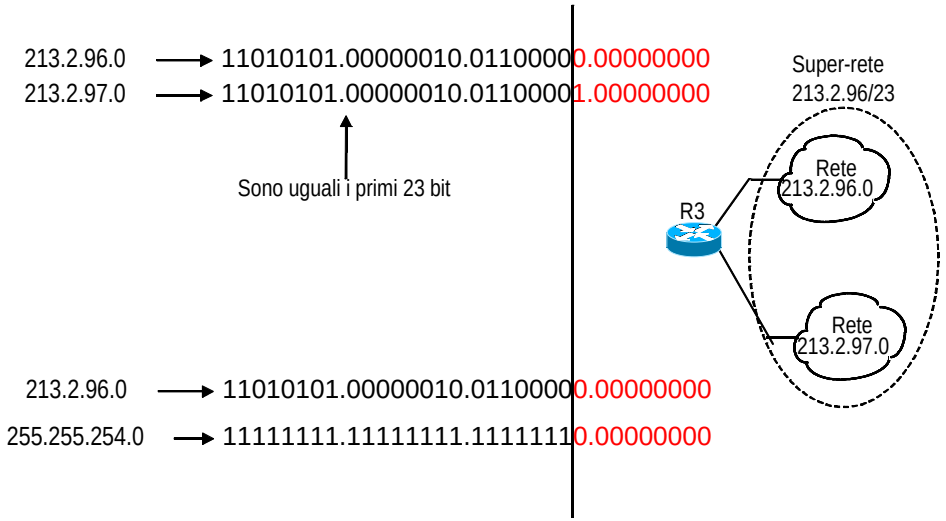


Tabelle di instradamento: Esempio di CIDR (3/3)

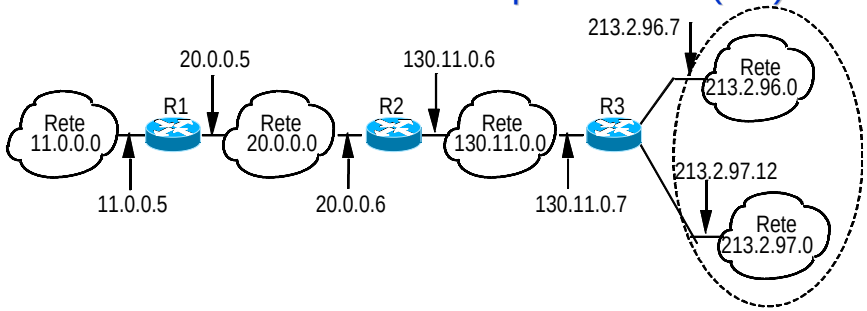


Tabella di instradamento di R2

Dest network	*Subnet mask*	*Next hop*
20.0.0.0	255.0.0.0	diretto
130.11.0.0	255. 255.0.0	diretto
11.0.0.0	255.0.0.0	20.0.0.5
213.2.96.0	255. 255.254.0	130.11.0.7

Tabelle di instradamento

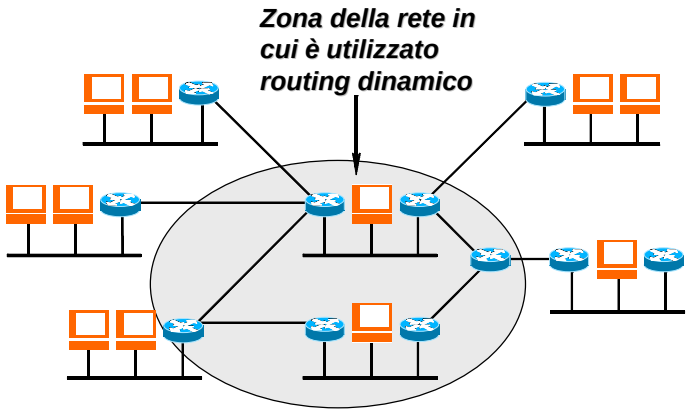
- Al fine di
  - **nascondere il più possibile i dettagli inerenti la rete,**
  - **mantenere piccole le tabelle di instradamento, e**
  - **consentire un instradamento efficiente,**

  le tabelle contengono (in genere) solo informazioni sulle reti di destinazione e non sui singoli nodi
- Spesso nelle RT è presente come possibile target di rete di destinazione anche l'indirizzo della massima super-rete 0.0.0.0/0 (ovvero net 0.0.0.0 e mask 0.0.0.0)
  - **questo indirizzo di rete include ogni possibile indirizzo di destinazione**
  - **il router next-hop relativo a questa paticolare super-rete viene detto router (o gateway) di default**
  - **in questo modo si può evitare di includere esplicitamente nella RT tutte le possibili reti di destinazioni**
  - **tutto ciò vale sia per le RT degli host che dei router**
  - **In base al Longest Prefix Matching, se per un datagramma non viene trovata nella RT una strada diversa allora viene instradato verso il "router di default" (se presente nella tabella di routing)**

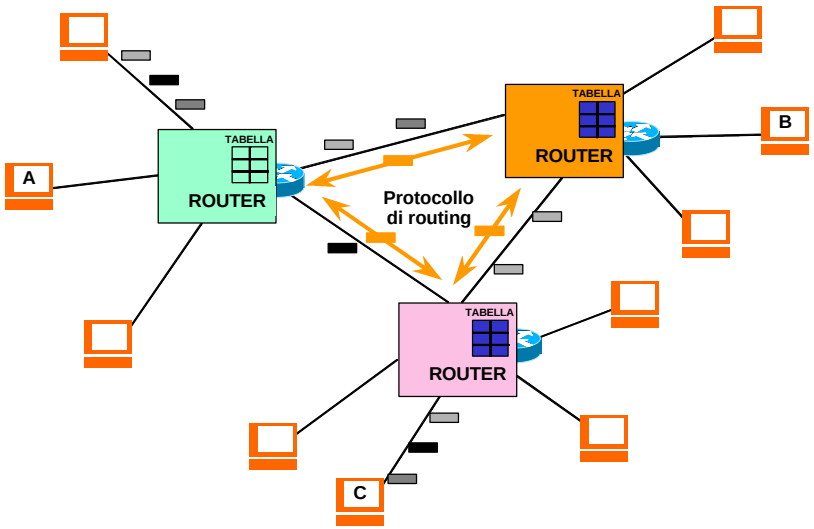
Tabelle di instradamento

- In base alle modalità con cui vengono create/aggiornate le tabelle di instradamento nei router si distinguono due tipi di instradamento (routing):
- routing statico
  - **le tabelle vengono create/aggiornate staticamente e non sono funzione dello stato della rete**
  - **le tabelle vengono create/aggiornate dal gestore**
    - il gestore ha un totale controllo dei flussi di traffico
    - deve intervenire manualmente per riconfigurare la rete
  - **utilizzato ad es.**
    - nella parte non magliata di reti IP
    - negli host, che in genere vengono configurati in base alle seguenti informazioni: indirizzo IP, net mask, default "gateway"
- routing dinamico
  - **Le tabelle vengono calcolate con appositi algoritmi (di routing) e aggiornate periodicamente al variare dello stato della rete attraverso opportuni protocolli di routing**

Routing Statico e Dinamico



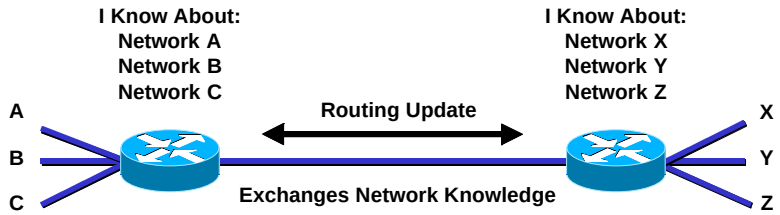
Routing Dinamico



Routing protocols

Routing Dinamico

- Ogni router calcola le sue tabelle dialogando con gli altri router
- Tale dialogo avviene tramite dei protocolli (livello 3 o superiore) detti protocolli di routing
- I protocolli di routing sono utilizzati dai router per determinare il percorso per raggiungere le reti non direttamente connesse
- Esistono diversi protocolli di routing, ciascuno con caratteristiche più o meno attraenti: RIP, *EIGRP (CISCO),* OSPF



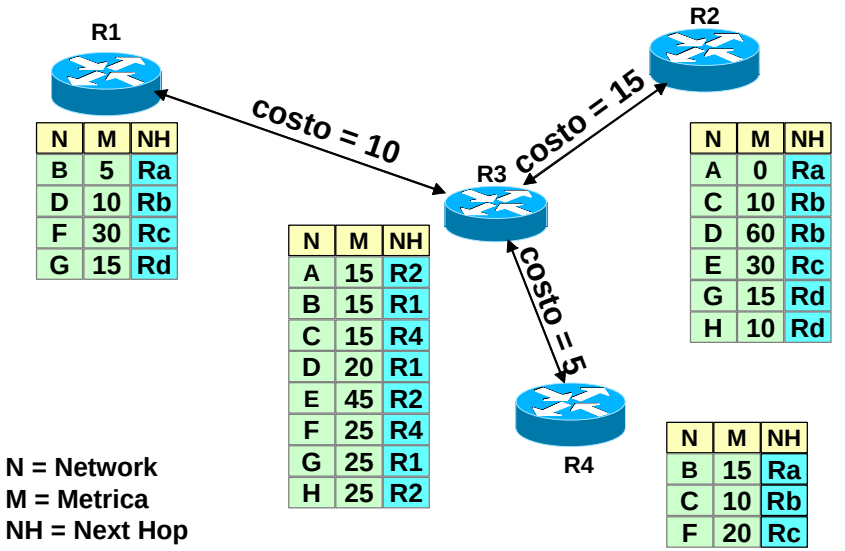
Routing Dinamico

- Esistono due approcci principali al routing distribuito:
  - **Algoritmi Distance Vector**
    - più semplici
    - impegnano meno risorse sul router
    - meno efficenti
    - adatti a reti piccole
  - **Algoritmi Link State**
    - molto più complessi
    - molto più efficenti
    - impegnano più risorse
    - adatti a reti grandi

Distance Vector

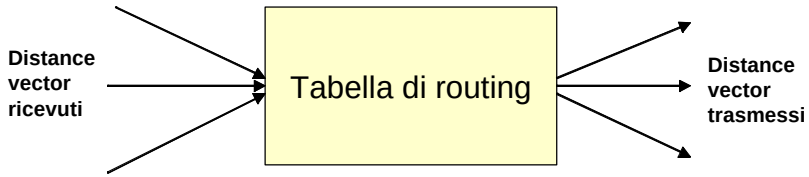
- Noto anche come algoritmo di Bellman-Ford
- Ogni nodo mantiene un database con le distanze minime tra sé stesso e tutte le possibili destinazioni
- Ogni nodo, quando modifica le proprie tabelle di instradamento, invia ai nodi adiacenti un distance vector
- Il distance vector è un insieme di coppie
  - **[indirizzo - distanza]**
- Quando un nodo riceve un distance vector da un nodo adiacente, ricalcola la tabella delle distanze minime; se ci sono modifiche invia il suo nuovo distance vector (aggiornato) ai nodi adiacenti
- La distanza è espressa tramite metriche classiche quali numero di hops e costo

Distance Vector



N = Network
M = Metrica
NH = Next Hop

Distance Vector



Distance Vector: caratteristiche

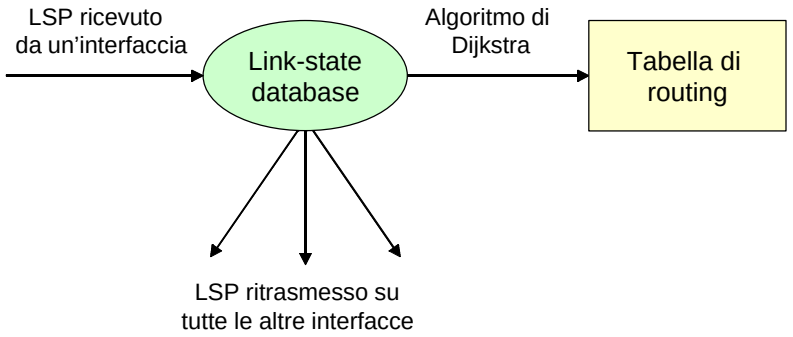
- Vantaggi:
  - **Molto semplice da implementare**
- Svantaggi
  - **Possono innescarsi dei loop a causa di particolari variazioni della topologia**
  - **Converge alla velocità del link più lento e del router più lento**
  - **Difficile capirne e prevederne il comportamento su reti grandi: nessun nodo ha una mappa della rete!**
  - **L'implementazione di meccanismi migliorativi appesantisce notevolmente il protocollo**

Link State

- Ogni router impara il suo ambito locale: linee e nodi adiacenti
- Trasmette queste informazioni a tutti gli altri router della rete tramite un Link State Packet (LSP)
- Tutti i router, memorizzando i LSP trasmessi dagli altri router, si costruiscono una mappa della rete
- Ogni router calcola indipendentemente le sue tabelle di instradamento applicando alla mappa della rete l'algoritmo di Dijkstra o SPF (Shortest Path First)
- La complessità è E log N
  - **E è il numero di link, N è il numero di nodi**

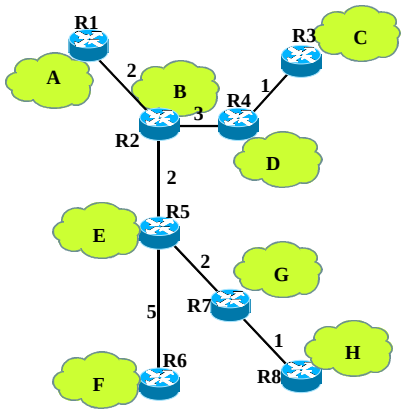
Link State: operazione di un router

- Il LSP è trasmesso in flooding su tutti i link del router
- I LSP memorizzati formano una mappa completa della rete
  - **Link State Database**



Link State: tabella di routing

- Ogni router calcola indipendentemente le sue tabelle di routing applicando alla mappa della rete l'algoritmo di Dijkstra o SPF (Shortest Path First)



Nodo	*LS Packet*
R1	B(2)
R2	A(2) D(3) E(2)
R3	D(1)
R4	B(3) C(1)
R5	B(2) F(5) G(2)
R6	E(5)
R7	E(2) H(1)
R8	G(1)

Tabella di routing di R2

A	R1
C	R4
D	R4
E	R5
F	R5
G	R5
H	R5

LSP Flooding

- I LSP vengono trasmessi in flooding su tutti i link del router che li ha originati
- Un router che riceve un LSP lo ritrasmette in flooding solo se esso ha modificato il LSP database del router stesso (selective flooding)
- All'atto del ricevimento di un LSP un router compie le seguenti azioni:
  - **se non ha mai ricevuto LSP da quel mittente o se il num di sequenza del LSP è maggiore di quello del LSP memorizzato nel database, allora memorizza il pacchetto nel database e lo ritrasmette in flooding su tutte le linee eccetto quella da cui l'ha ricevuto;**
  - **se il LSP ricevuto ha lo stesso numero di sequenza di quello posseduto, allora non viene fatto nulla;**
  - **se il LSP è più vecchio di quello posseduto, cioè è obsoleto, allora il router ricevente trasmette il LSP aggiornato al router mittente**
- Questo meccanismo serve a fare in modo che i LSP database di tutti i router si mantengano perfettamente allineati e coerenti, condizione indispensabile per un corretto instradamento

Link State: caratteristiche

- Vantaggi:
  - **Può gestire reti di grandi dimensioni**
  - **Ha una convergenza rapida**
  - **Difficilmente genera loop, e comunque è in grado di identificarli e interromperli facilmente**
  - **Facile da capire: ogni nodo ha la mappa della rete**
- Svantaggi:
  - **Più complesso da realizzare**
- È utilizzato nel protocollo OSPF

Distance Vector vs. Link State

- Nel LS i router cooperano per mantenere aggiornata la mappa della rete, poi ogni router calcola il proprio spanning tree autonomamente; nel DV i router cooperano per calcolare direttamente le tabelle di instradamento
- L'algoritmo LS può gestire reti di grandi dimensioni (10000 nodi), il DV generalmente non supera i 1000
- LS ha convergenza rapida, difficilmente genera loop, e comunque è in grado di identificarli e interromperli facilmente; ed è facile da capire e prevedere poiché ogni nodo contiene l'intera mappa della rete

Protocolli di routing

	Algoritmo	Protocollo
Link State	Dijkstra SPF	OSPF
Distance Vector	Bellman-Ford	RIP IGRP (Cisco)

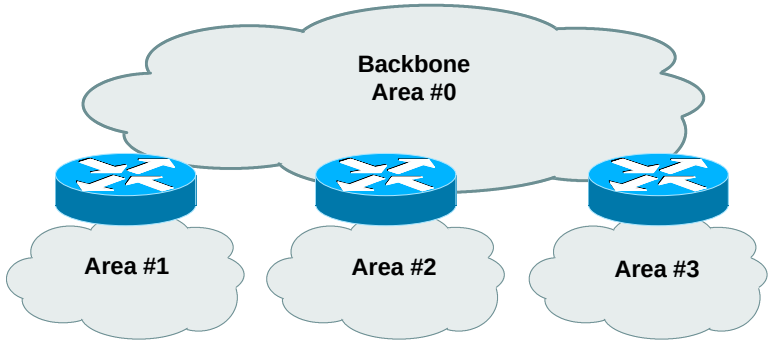
RIP

- Sviluppato dalla Xerox per XNS
- Nel 1982 il RIP è stato adattato per il TCP/IP con lo UNIX BSD
- Si tratta di un protocollo di routing intradominio basato su un algoritmo di tipo distance vector
- Definito dall'IETF nello RFC 1058 (1988) e nello RFC 1388 (1993)
- Metrica di costo: basata su hop count
  - **Il RIP permette un massimo di 15 hop, superati i quali il percorso viene ritenuto irrealizzabile**
- Messaggi di update: inviati ogni 30 s
  - **In caso di link failure o modifica di topologia l'update avviene immediatamente**
- Memorizzazione in tabella del solo percorso migliore verso la destinazione
- Usato dal demone “routed” in UNIX

OSPF

- Protocollo di tipo link state
- Definito dall'IETF:
  - **RFC 1247 (1991)**
  - **RFC 1583 (1994) - OSPFv2**
- OSPF ha il concetto di gerarchia
  - **un AS (dominio OSPF) è suddiviso in aree**
  - **le aree contengono un gruppo di reti contigue**
  - **le aree sono indicate da un area-id su 32 bit**
    - deve essere specificato per ogni interfaccia
  - **quando un AS ha più di un'area deve esistere una backbone area con area-id = 0**

OSPF: aree



- La topologia di un'area è invisibile all'esterno dell'area
- Riduzione del traffico di routing

OSPF: metrica

- Il costo (o metrica) di un'interfaccia può essere legato alla larghezza di banda ad essa associata
  - **costo inversamente proporzionale alla banda**
    - costo = 10^8/(bandwidth in bps)

Protocolli di routing: confronto

	OSPF	RIP
Scalabilità	Buona	Bassa
Banda	Bassa	Alta
Memoria	Alta	Bassa
CPU	Alta	Bassa
Convergenza	Veloce	Lenta
Configurazione	Moderata	Facile

Sistemi autonomi

- Si definisce come sistema autonomo (*Autonomous System* - AS) un insieme di hosts, routers e reti fisiche controllate da una singola autorità amministrativa; ogni AS è identificato da un numero assegnato dal NIC
- Ogni AS è libero di scegliere i criteri di determinazione delle strade al suo interno
- Ogni AS deve però affidare in modo specifico ad uno o più routers il compito di comunicare al mondo esterno le informazioni di routing al suo interno
- Le informazioni di instradamento riguardanti le strade all'interno di un sistema autonomo sono gestite tra i router del AS per mezzo degli Interior Gateway Protocols (IGP)
- Le informazioni di instradamento riguardanti strade che coinvolgono più di un sistema autonomo sono scambiate mediante gli Exterior Gateway Protocols (EGP) tra i *core routers*

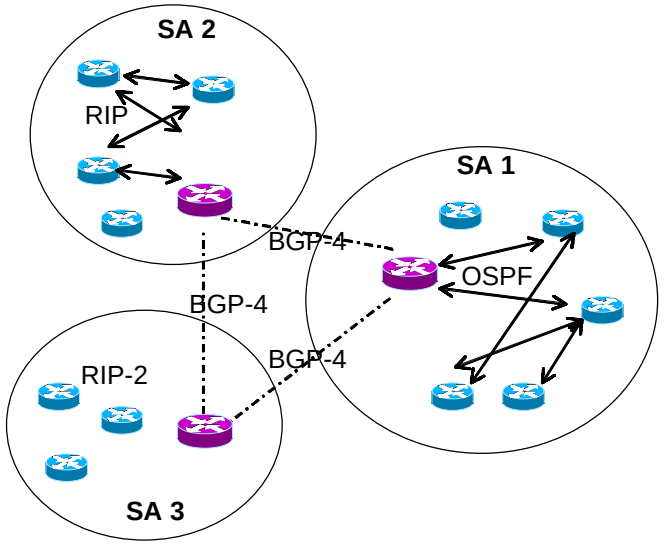
Interior and Exterior Gateway Protocols

- I protocolli di instradamento all'interno di un AS sono detti Interior Gateway Protocols (IGP)
  - **Routing Information Protocol (RIP)**
  - **Open Shotest Path First (OSPF)**
- Le informazioni di instradamento che coinvolgono più di un sistema autonomo sono gestite mediante gli Exterior Gateway Protocols (EGP)
  - **Border Gateway Protocol (BGP)**

Interior and Exterior Gateway Protocols

- Un IGP ha il compito di
  - **individuare i router adiacenti nello stesso AS**
  - **raccogliere e distribuire a tutti i router i dati sulla topologia di un AS e sul costo di attraversamento dei rami**
  - **comunicare tempestivamente eventuali variazioni del costo di attraversamento dei rami di un AS**
- Un EGP ha il compito di
  - **individuazione dei router adiacenti di altri AS con cui scambiare le informazioni di instradamento**
  - **verifica continua della funzionalità dei router interlocutori**
  - **scambio periodico di informazioni di raggiungibilità delle reti**

IGP & EGP



Il protocollo ICMP

ICMP (Internet Control Message Protocol)

- ICMP (Internet Control Message Protocol) (RFC 792, 950)
- Utilizzato per la trasmissione dei messaggi di errore e di controllo relativi al protocollo IP
  - **errori di instradamento, TTL scaduto, congestione, etc**
- I messaggi vengono manipolati dal software IP, non dagli applicativi utente
- ICMP può quindi essere considerato un sub-strato di IP (visto che serve a trasportare messaggi tra due entità IP) ma è funzionalmente al di sopra di IP (visto che i suoi messaggi governano il funzionamento di IP)
- ICMP è una parte integrante di IP è deve essere incluso in ogni implementazione di IP
- Un messaggio ICMP è incapsulato nella parte dati di un datagramma IP

ICMP

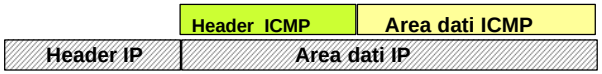
- ICMP ha lo scopo esclusivo di notificare errori all'host di origine
  - **ICMP non specifica le azioni che devono essere prese per rimediare ai malfunzionamenti**
  - **spetta all'host di origine decidere le azioni da intraprendere per correggere il problema**
- I messaggi di ICMP viaggiano come comuni datagrammi, anch'essi possono essere soggetti ad errore e contribuire alla congestione di rete
- La procedura di gestione dei datagrammi prevede un'unica differenza tra i datagrammi che trasportano i messaggi ICMP e gli altri:
  - **non vengono generati messaggi ICMP in seguito ad errori causati da datagrammi che trasportano messaggi ICMP**
    - ciò serve ad evitare messaggi di errore relativi a messaggi di errore.
- Ogni messaggio ICMP è in relazione ad uno specifico datagramma
- Un messaggio di errore ICMP contiene quindi anche una parte del datagramma che ha generato l'errore (Intest. IP + primi 8 ottetti dei dati IP, i quali contengono le porte TCP o UDP do sorgente e destinazione)

ICMP

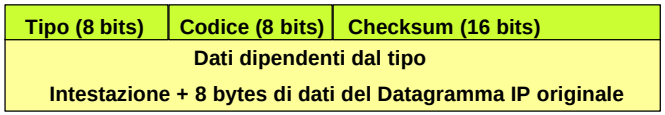
- Esempi:
  - **Source Quench: inviato dal destinatario, interrompe l'emissione di datagrammi del mittente;**
  - **Redirect: il destinatario segnala al mittente di re-instradare il datagramma verso un altro host;**
  - **Echo: controlla se un possibile destinatario è attivo,**
  - **Destination Unreacheable: notifica il mittente della non-raggiungibilità di un host**

ICMP

- Un messaggio ICMP si riferisce ad uno specifico datagramma
- Un messaggio ICMP contiene l'indicazione del particolare datagramma IP che ha generato l'errore
  - **nel caso di frammentazione, un messaggio ICMP viene emesso solo per il frammento 0**
- Incapsulamento di un messaggio ICMP



- Formato messaggio ICMP



ICMP: tipi di messaggio

Tipo	Descrizione
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	Echo Request
11	Time Exceeded for a Datagram
12	Parameter Problem for a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

ICMP: codici

Codici per messaggio 'destinazione irraggiungibile' (tipo 3)

0	Rete irragiungibile
1	Host irragiungibile
2	Protocollo irragiungibile
3	Porta irragiungibile
4	Frammentazione necessaria e DF settato
5	Fallimento routing sorgente
6	Rete destinazione sconosciuta
7	Host destinazione sconosciuto
8	Host sorgente isolato
9	Comunicazione con rete destinazione proibita amministrativamente
10	Comunicazione con host destinazione proibita amministrativamente
11	Rete irragiungibile per il tipo di servizio
12	Host irragiungibile per il tipo di servizio

ICMP

- Redirect message
  - **se è emesso da un router significa che i successivi datagrammi emessi dall'host verso la rete dovranno essere indirizzati verso il router indicato nel messaggio ICMP**
  - **causa una modifica della tabella di instradamento dell'host sorgente**
- Source quench
  - **se è emesso da un router intermedio indica che il router non ha buffer sufficiente per memorizzare il datagramma**
  - **se è emesso dall'host di destinazione indica che il datagramma non è stato processato dall'host**
  - **il messaggio è utilizzato dal TCP**
- Time exceeded
  - **indica che il TTL si è esaurito**

ICMP

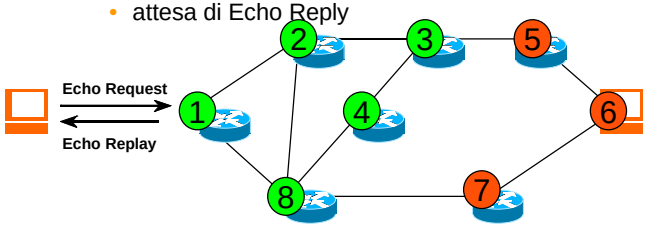
- Echo e Echo replay
  - **sono utilizzati per stabilire l'attività di un elemento di un host**
- Destination unreachable
  - **indica che l'instradamento di un datagramma non è stato completato**
- Time Stamp Request e Time Stamp Replay
  - **sono utilizzati per effettuare misure di prestazioni (es. ritardi di transito)**
- Address mask request e Address mask replay
  - **sono usati per determinare la maschera della sotto-rete a cui è connesso un host**
  - **sono usati da host molto semplici (diskless) dopo aver individuato il proprio indirizzo con il protocollo RARP**

Applicazioni dell'ICMP

- Ping
  - **è utilizzata per verificare**
    - l'istallazione della pila TCP/IP
    - l'attività di un host
    - il tempo di transito tra host sorgente e host destinazione
  - **utilizza i messaggi ICMP Echo e Echo Replay**
- Traceroute
  - **determina la sequenza di router attraversati da un datagramma tra l'host sorgente e l'host destinazione**
  - **utilizza in successione datagrammi con TTL=1 ,2, 3, ...**
  - **la sequenza di router viene individuata poichè questi il primo router risponderà con invieranno in successione i messaggi ICMP Time Exceeded**

Ping

- PING
  - **diagnosi di raggiungibilità**
    - generazione di pacchetti di Echo Request verso "Echo Server"
    - attesa di Echo Reply



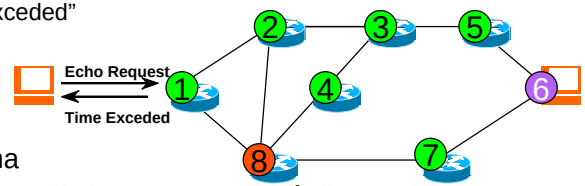
- Problema
  - **scarsa capacità diagnostica**
    - **cosa significa se 5,6 e 7 non rispondono al PING ?**
    - **ci sono decine di possibili cause**
    - **si può migliorare facendo PING da sorgenti diverse**

Ping

```
[user]$ ping pinco.pallino.net

PING pinco.pallino.net (193.200.242.5): 56 data bytes
64 bytes from 193.200.242.5: icmp_seq=0 ttl=248 time=111.4 ms
64 bytes from 193.200.242.5: icmp_seq=1 ttl=248 time=90.2 ms
64 bytes from 193.200.242.5: icmp_seq=2 ttl=248 time=116.2 ms
64 bytes from 193.200.242.5: icmp_seq=3 ttl=248 time=80.6 ms
64 bytes from 193.200.242.5: icmp_seq=4 ttl=248 time=80.1 ms
64 bytes from 193.200.242.5: icmp_seq=5 ttl=248 time=537.4 ms

--- pinco.pallino.net ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 80.1/169.3/537.4 ms
```

Traceroute

- TraceRoute
  - ➢ **identificazione dei percorsi sulla rete**
    - generazione di più pacchetti successivi di Echo Request
      - – TTL inizia da 1 e viene incrementato di 1 ad ogni successivo Echo Request
    - ogni pacchetto percorre un passo in più rispetto al precedente
    - osservazione dell'indirizzo sorgente dei pacchetti di "Time Exceded"



- Problema
  - ä **come per il ping scarsa capacità diagnostica**
    - ⋆ **Esempio: cosa succede se il percorso dei pacchetti nelle due direzioni è diverso (Es. 1,2,3,5,6,5,3,4,8,1) ed il nodo 8 è guasto ?**

Traceroute

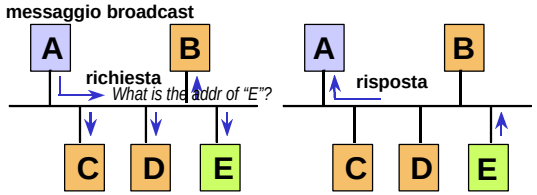
```
traceroute to www.stanford.edu (171.64.14.203), 30 hops max, 40 byte
packets
 1  151.100.238.1 (151.100.238.1)  2678.773 ms
 2  rc-uniromaI.rm.garr.net (193.206.131.49)  1859.746 ms
 3  rt-rc-2.rm.garr.net (193.206.134.165)  788.237 ms
 4  mi-rm-1.garr.net (193.206.134.17)  766.614 ms
 5  ny-mi.garr.net (212.1.200.17)  894.860 ms
 6  Abilene-DANTE.abilene.ucaid.edu (212.1.200.222)  1118.096 ms
 7  clev-nycm.abilene.ucaid.edu (198.32.8.29)  970.481 ms
 8  ipls-clev.abilene.ucaid.edu (198.32.8.25)  1161.797 ms
 9  kscy-ipls.abilene.ucaid.edu (198.32.8.5)  967.958 ms
10  denv-kscy.abilene.ucaid.edu (198.32.8.13)  1200.059 ms
11  scrm-denv.abilene.ucaid.edu (198.32.8.1)  985.121 ms
12  BERK--abilene.POS.calren2.net (198.32.249.41)  1166.336 ms
13  SUNV--BERK.POS.calren2.net (198.32.249.14)  1087.366 ms
14  STAN--SUNV.POS.calren2.net (198.32.249.74)  962.810 ms
15  i2-gateway.Stanford.EDU (171.64.1.214)  566.572 ms
16  Core3-gateway.Stanford.EDU (171.64.1.222)  215.399 ms
17  sweet-gateway.Stanford.EDU (171.64.3.110)  215.441 ms
18  www1.Stanford.EDU (171.64.14.203)  215.697 ms
```


Address Resolution Protocol (ARP)

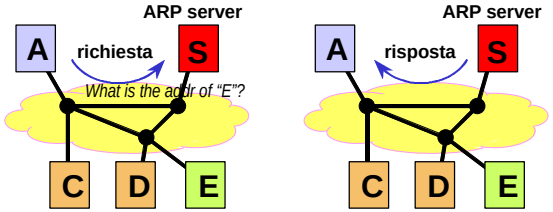
Risoluzione degli indirizzi

- Per effettuare il forwarding diretto è necessario associare l'indirizzo IP del destinatario e indirizzo fisico corrispondente.
- Mapping statico
  - ➢ **la tabella di associazione viene predisposta staticamente (ad esempio rete X.25, ISDN, etc.)**
- Mapping dinamico
  - ➢ **la tabella viene costruita dinamicamente attraverso un protocollo ARP (Address Resolution Protocol) RFC826**
    - broadcast (sulle LAN)
    - ARP-Server (su reti Non Broadcast)

- broadcast (sulle LAN)



- ARP-Server (su reti Non Broadcast)

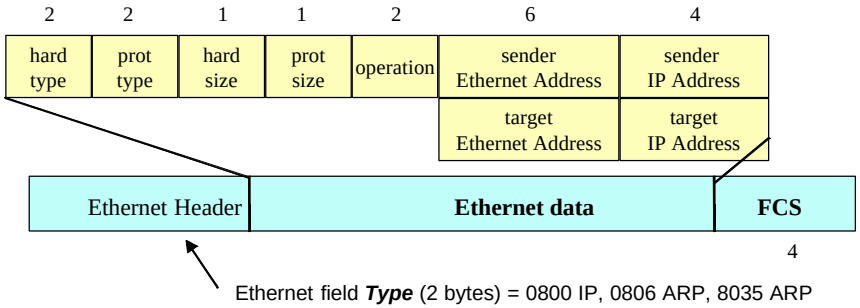


ARP

- Il protocollo ARP (Address Resolution Protocol) fornisce un meccanismo dinamico di associazione fra indirizzi MAC ed indirizzi IP
- Viene utilizzato ogni qual volta un nodo di una LAN debba inviare un pacchetto ad un altro nodo della stessa LAN di cui però conosca solo l'indirizzo IP

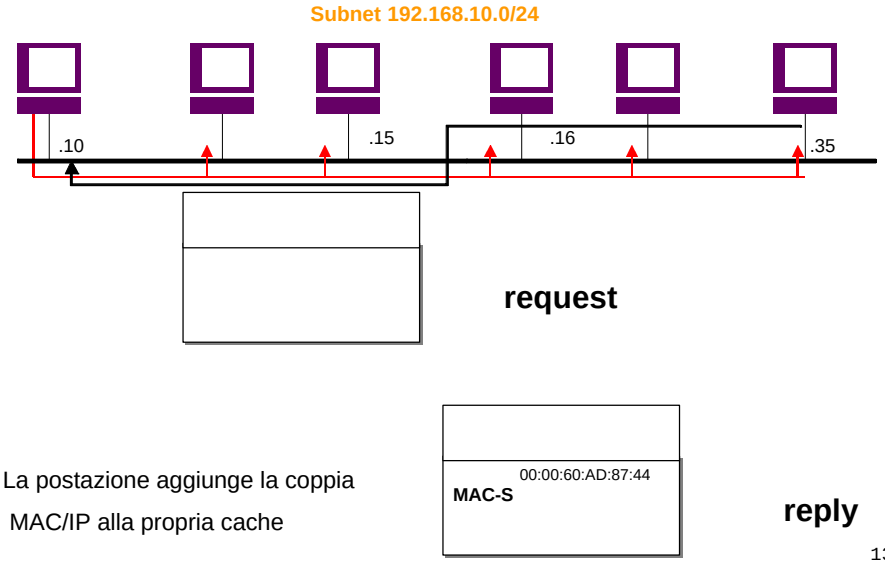
ARP

- Il formato dei pacchetti è identico per ARP e RARP
- ARP/RARP si appoggiano direttamente sullo strato MAC (non su IP). Ciò significa che un opportuno campo nell'intestazione della MAC-PDU indica se il contenuto deve essere consegnato a ARP,RARP o IP.



ARP prevede caching delle informazioni
il comando `arp -a` vpermette di visualizza il contenuto della cache

ARP



Configuazione automatica di un nodo IP: da RARP a DHCP e PPP

RARP

- RARP (Reverse Address Resolution Protocol) (RFC 903):
  - **dato un indirizzo di scheda di rete, permette di ricavare il corrispondente indirizzo IP**
  - **si utilizza(va) per le workstation diskless per effettuare il bootstrap tramite immagine su server remoto**
  - **utilizza un RARP server**
  - **l'host emette un pacchetto RARP con indirizzo di sottorete (Ethernet) broadcast con il quale richiede il proprio indirizzo IP in base al proprio indirizzo di scheda di rete (Ethernet)**
  - **il server RARP riceve la richiesta, consulta un file di configurazione e risponde con l'indirizzo IP corrispondente all'indirizzo della scheda di rete del richiedente**
  - **svantaggi:**
    - l'applicazione server deve operare a livello di protocollo di sotto-rete
    - permette di acquisire solo l'indirizzo IP
    - il server deve essere nella stessa sotto-rete

BOOTP

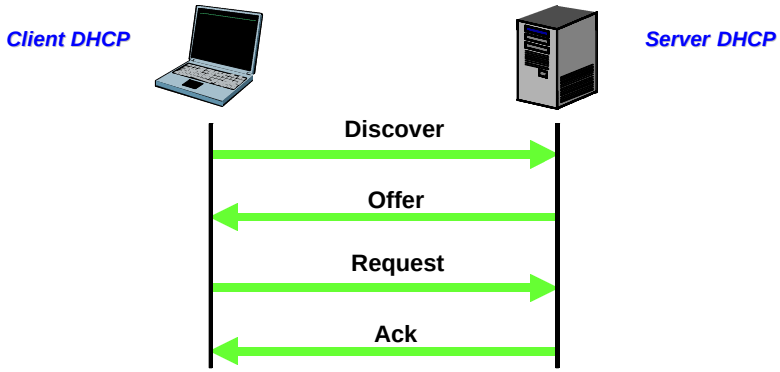
- BOOTP (BOOTstrap Protocol) (RFC 951, 1048, 1084)
  - **permette di acquisire all'avvio (bootstrap) informazioni di configurazione quali: (proprio IP address, indirizzo di un router, indirizzo di un server,...)**
  - **è adatto per host senza disco rigido**
  - **vengono scambiati messaggi (UDP) tra l'host e il BOOTP server utilizzando il limited broadcast address (255.255.255.255) come destinazione**
  - **il server risponde ad una richiesta e, in base al client identifier specificato dall'host richiedente, fornisce: l'indirizzo IP dell'host, l'indirizzo IP di un router, l'indirizzo IP di un server ecc.**
  - **lo svantaggio principale è la staticità; ovvero:**
    - richiede l'inserimento delle informazioni nel file di configurazione
    - non può essere usato per assegnare dinamicamente gli indirizzi IP a domanda (mappaggio statico)

Dynamic Host Configuration Protocol

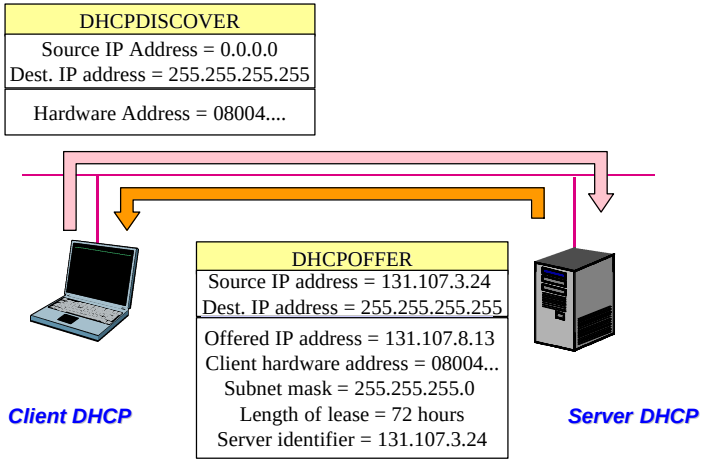
- DHCP (RFC 2131) è un'estensione di BOOTP che permette di:
  - **assegnare dinamicamente gli indirizzi IP**
  - **ricevere altre informazioni di configurazione (esempio: subnet mask)**
- DHCP è utile quando:
  - **i computer si connettono e disconnettono frequentemente**
  - **il numero di computer supera il numero di indirizzi disponibili nella sottorete**
  - **si vuole rendere automatica l'assegnazione degli indirizzi IP**
- DHCP permette tre tipi di configurazione: manuale, automatica e dinamica
- in configurazione dinamica un DHCP server assegna un IP address (tra un insieme di indirizzi disponibili) ad un host che ne effettua richiesta per un tempo limitato

Dynamic Host Configuration Protocol

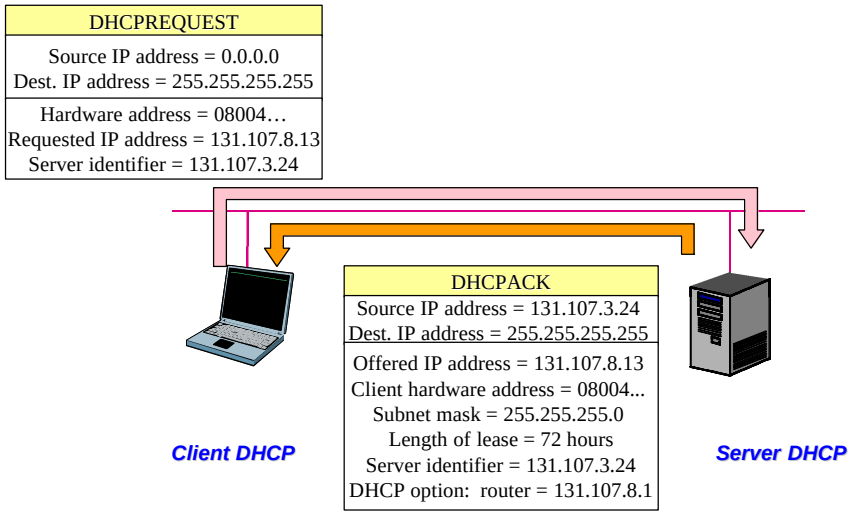
- DHCP utilizza un processo in quattro fasi per configurare un client
  - **discover**
  - **offer**
  - **request**
  - **ack**



DHCP: Discover e Offer



DHCP: Request e Ack



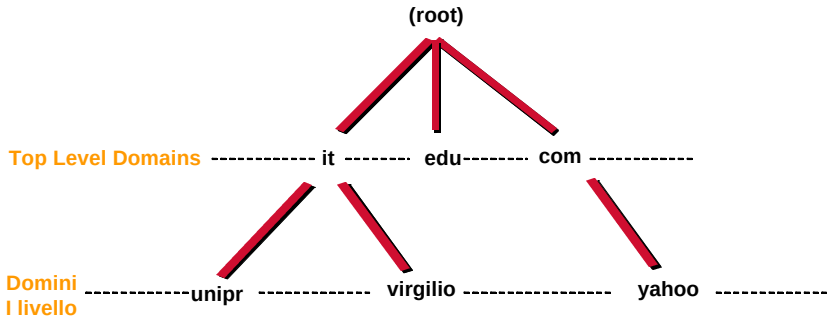
Point to Point Protocol

- PPP (Point to Point Protocol) è definito nell'RFC1661
- è un protocollo di livello 2 (Data Link) per collegamenti punto-punto
  - **attualmente il protocollo di livello 2 più usato in Internet per collegamenti punto-punto**
- oltre alle normali funzioni di Data Link (delimitazione di trama, controllo e recupero di errore, ecc) permette di:
  - **supportare differenti protocolli di livello 3 (tra cui IP)**
  - **negoziare informazioni di configurazione di livello 3 (nel caso di IP: host_address, default router/gateway, DNS)**

Risoluzione degli indirizzi (DNS)

Domain Name System (DNS)

- In Internet i nomi sono organizzati gerarchicamente in Domini
  - **I nomi sono costituiti da stringhe separate da "."**
  - **La parte più significativa è a destra**

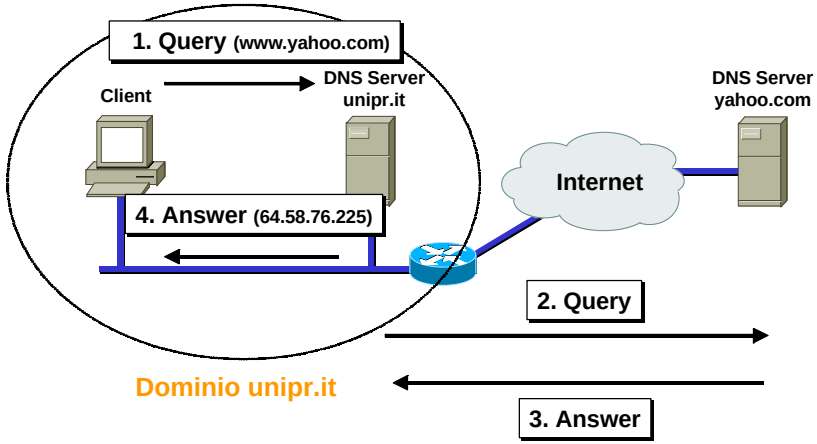


DNS (Domain Name System)

- **Top level domains**

com	**Organizzazioni commerciali (hp.com, sun.com ...)**
edu	**Organizzazioni educative (berkeley.edu, purdue.edu ...)**
gov	**Organizzazioni governative (nasa.gov, nsf.gov ...)**
mil	**Organizzazioni militari (army.mil, navy.mil ...)**
net	**Organizzazione di gestione reti (nsf.net ...)**
org	**Organizzazioni non commerciali (eff.org ...)**
int	**Organizzazioni internazionali (nato.int ...)**
	Codice di due caratteri per indicare una nazione

Risoluzione dei nomi



Root Name Server

- query per un nome

seguenti operazioni:

- ¶ **verifica nella cache se è presente il nome da risolvere. La cache contiene infatti i record dei nomi risolti più di recente**
- · **invia la query ad uno dei root name server specificati in un file denominato cache file**

- Nel secondo caso la query viene ripetuta sino a raggiungere un DNS server responsabile per il dominio richiesto

Cenni a IPv6

Perchè IPv6

- Esaurimento dello spazio di indirizzamento IPv4
- Esplosione delle tabelle di instradamento sui router
- Servizi nuovi e/o più efficenti
  - **Soluzione di networking "plug&play"**
  - **Qualità del Servizio**
  - **Sicurezza**
  - **Mobilità**
  - **Multicast**

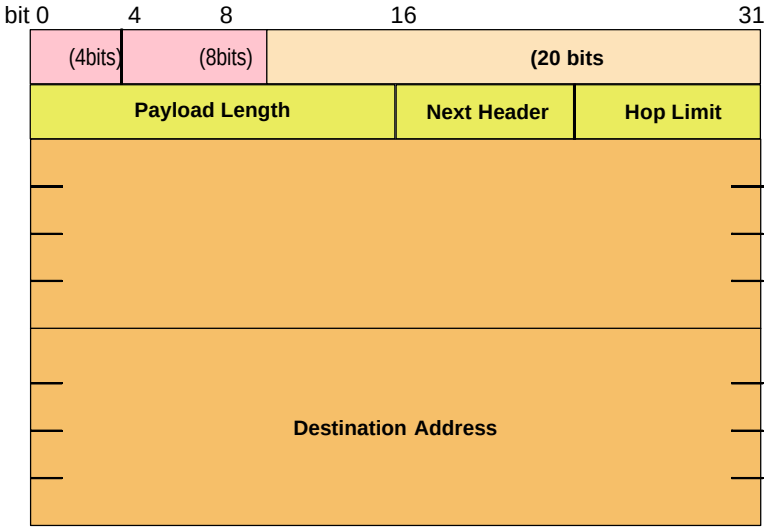
Indirizzi IP: quanti?

- Quanti nodi?
  - **terminali IP classici**
    - la crescita è probabilmente quella degli ultimi anni
  - **Altri apparati però potranno avere un indirizzo Internet:**
    - telefoni cellulari
    - agende elettroniche
    - carte di credito
    - elettrodomestici/casalinghi
    - apparati elettromedicali
    - dispositivi elettrici in genere

- Indirizzi IPv6 di 128 bit
  - **Con 128 bit si hanno a disposizione: 655.570.973.348.866.943.898.599 indirizzi/m^2**

  (Superificie della terra: 511.263.971.197.990 mq)

Header di IPv6



Header IPv6/IPv4

- Semplificazioni:
  - **l'header IPv6 ha lunghezza fissa (40 byte)**
    - le opzioni non sono più trasportate all'interno dell'header IP
      - questa funzione viene svolta dagli extension header di IPv6
  - **è stato rimosso il campo IP Header Length (IHL)**
    - non più necessario in quanto l'header IPv6 ha lunghezza fissa
  - **è stato rimosso il campo Header Checksum**
    - quasi tutti i protocolli di livello data link comprendono già il calcolo e la verifica di un checksum
  - **non esiste più la procedura di segmentazione hop-by-hop**
    - di conseguenza sono stati rimossi i campi Identification, Flags e Fragment Offset
  - **è stato rimosso il campo Type Of Service (TOS)**
- Nuovi campi:
  - **Flow Label**
  - **Class**

Sintassi degli indirizzi IPv6

Per rappresentare formalmente gli indirizzi IPv6 si è scelto di

I blocchi sono separati mediante il carattere ":" e vengono rappresentati in notazione esadecimale

- **3FFE:1001:7654:3220:FEDC:BA98:789A:32AC**
- :

  si possono omettere gli zeri iniziali di ogni blocco

  3ffe:1001:1:100:a00:20ff:fe83:5531
  - **con "::"**
    -

La transizione ad IPv6

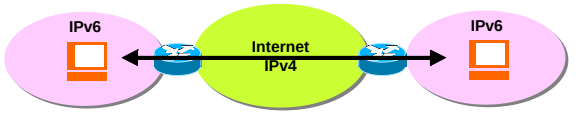
-

compatibilità con la base istallata IPv4

Durante la fase di transizione sono necessari meccanismi per:

- **Permettere il colloquio tra nuovi host**

Realizzare connettività tra isole IPv6 utilizzando l'infrastruttura IPv4



- Inoltre, reti IPv6 verranno utilizzate per intercconnettere reti IPv4 (e.g. backbone UMTS)

La transizione ad IPv6

- Lo sviluppo della rete IPv6 avverrà in modalità sovrapposta
  - **Dual stacked nodes**
    - i nodi implementano entrambe le pile protocollari IPv4 e IPv6
  - **Tunneling**
    - il traffico IPv6 viene trasportato da IPv4 mediante tunnel
- E tramite meccanismi di traduzione
  - **protocol translation**
    - il traffico IPv6 viene tradotto in IPv4 e viceversa