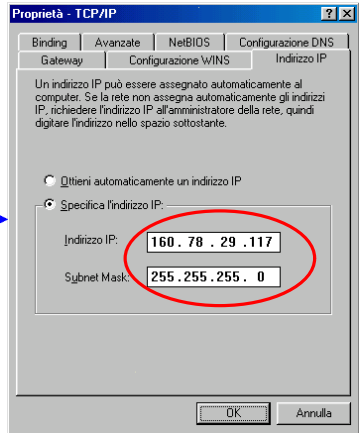
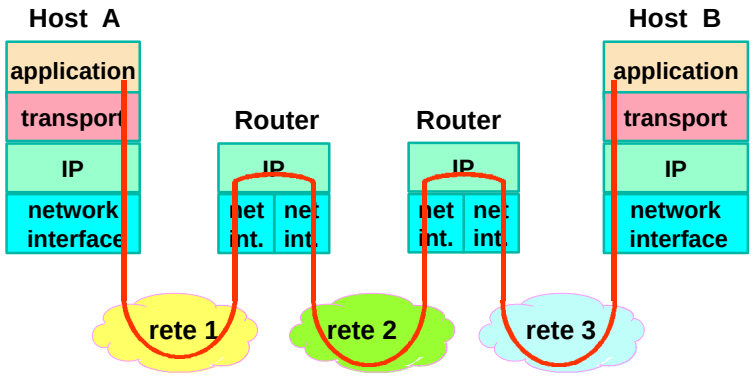
Configurazione di un nodo windows

- 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

Instradamento IP



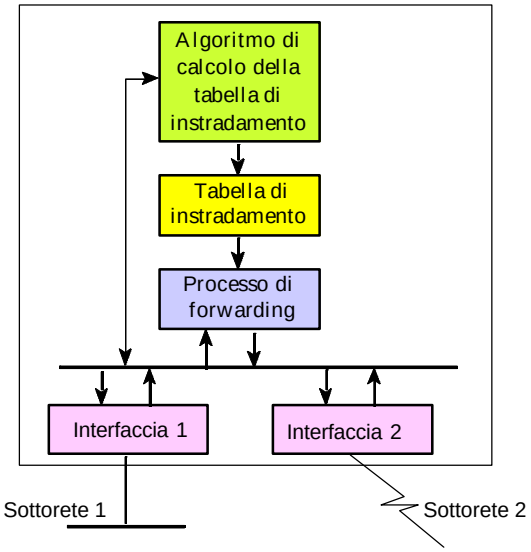
Router

- 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)**
  - **utilizzano "protocolli di routing"**

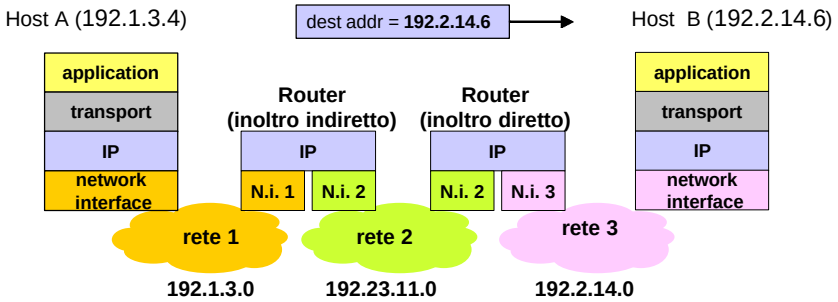
Architettura di un Router



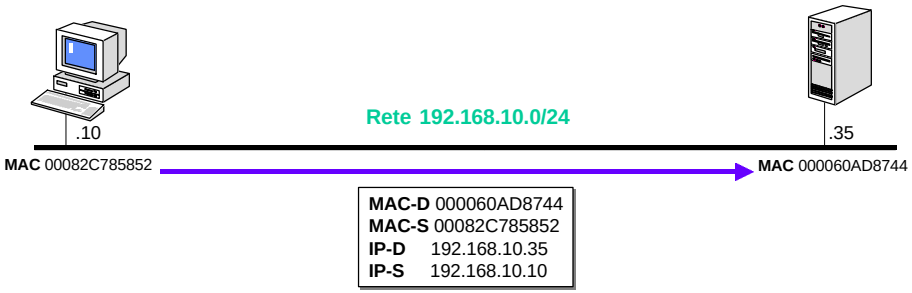
Instradamento (1/3)

- 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)

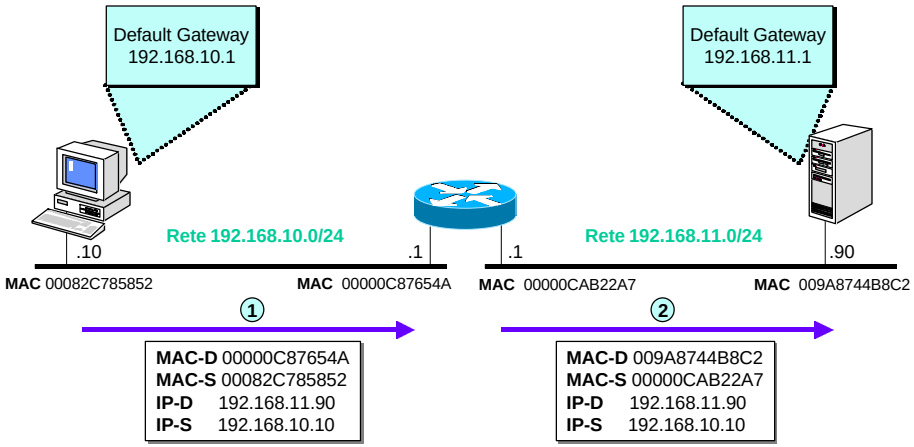
Instradamento (2/3)



Forwarding diretto: esempio



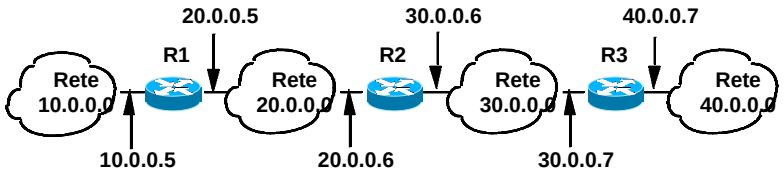
Forwarding indiretto: esempio



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
```


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

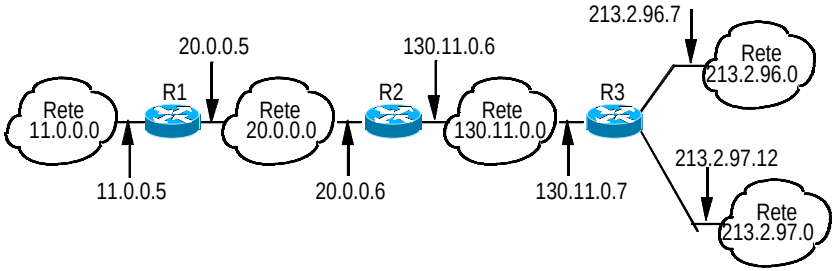


Tabella di instradamento di R2

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)

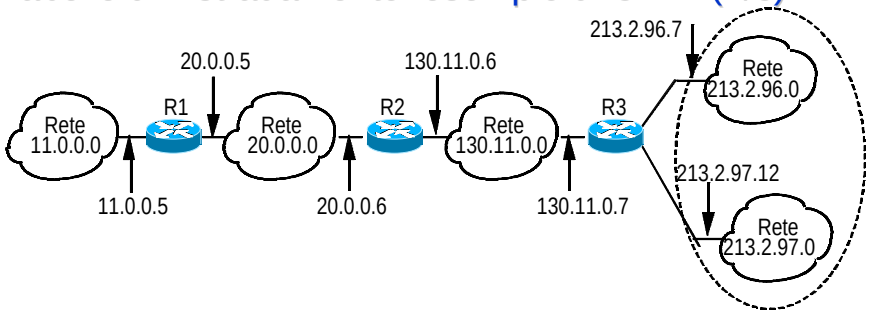


Tabella di instradamento di R2

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: esempio di CIDR (3/3)

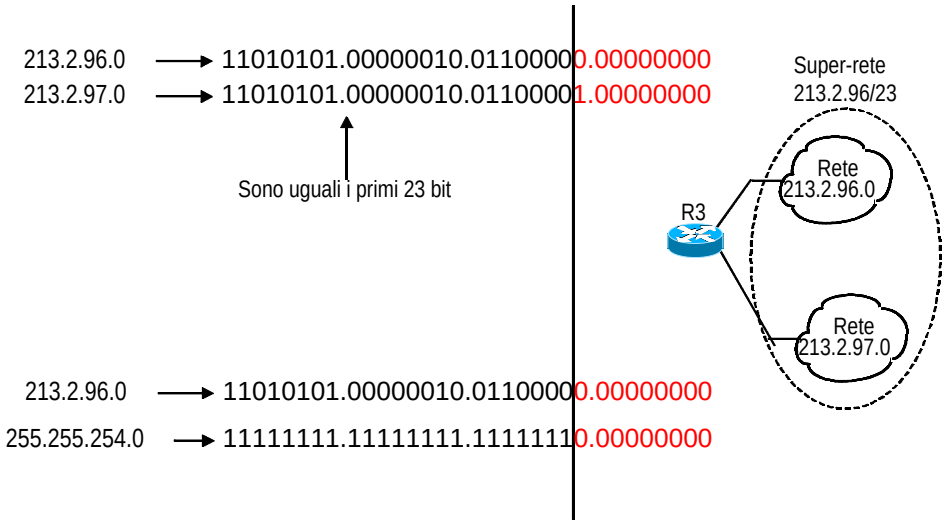


Tabelle di instradamento

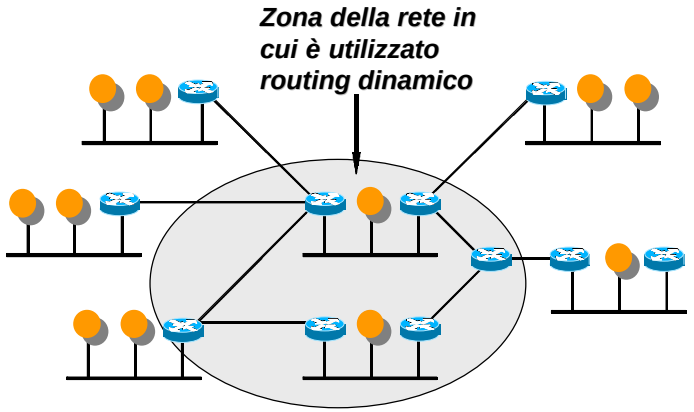
- Al fine di
  - **nascondere il più possibile i dettagli inerenti la rete,**
  - **mantenere piccole le tabelle di instradamento, e**
  - **consentire un instradamento efficiente,**

  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**
- 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)

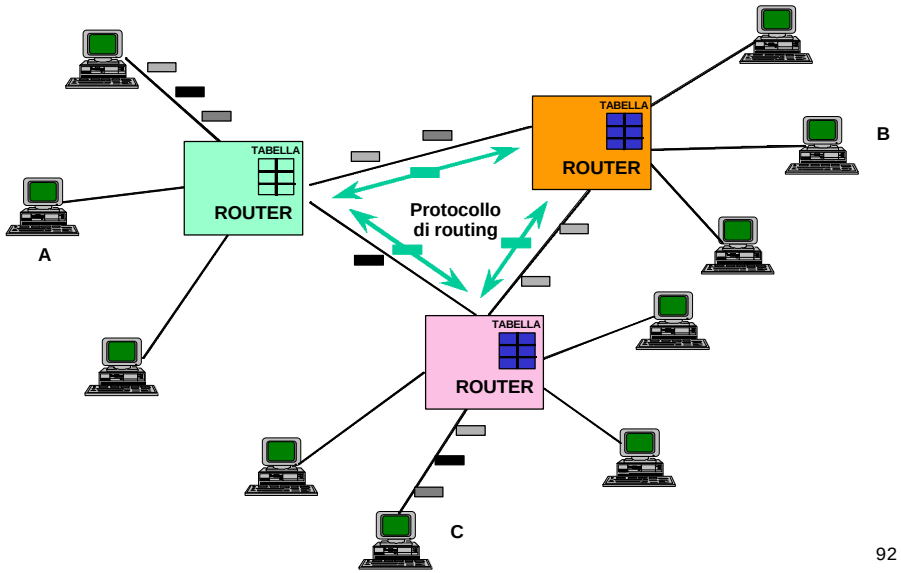
Tabelle di instradamento

- 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



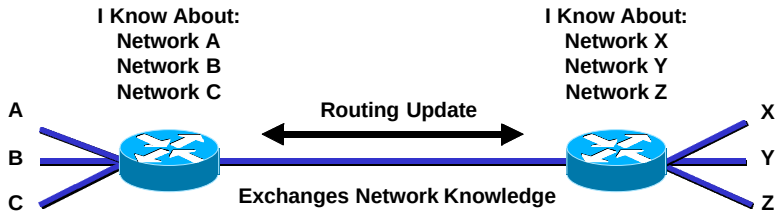
Routing Dinamico



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



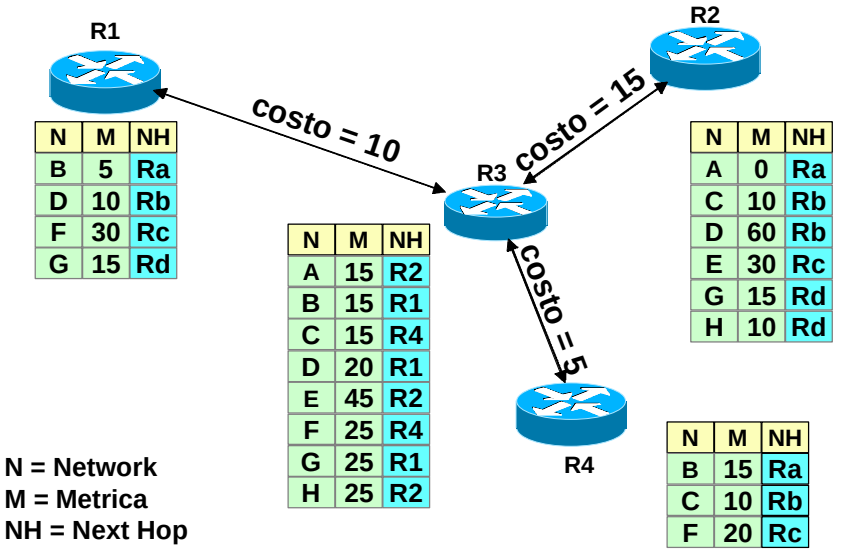
Routing Dinamico

- 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	M	NH
B	5	Ra
D	10	Rb
F	30	Rc
G	15	Rd

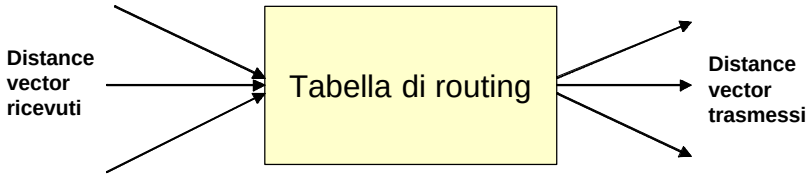
N	M	NH
A	15	R2
B	15	R1
C	15	R4
D	20	R1
E	45	R2
F	25	R4
G	25	R1
H	25	R2

N	M	NH
A	0	Ra
C	10	Rb
D	60	Rb
E	30	Rc
G	15	Rd
H	10	Rd

N	M	NH
B	15	Ra
C	10	Rb
F	20	Rc

N = Network
M = Metrica
NH = Next Hop

Distance Vector



Distance Vector: caratteristiche

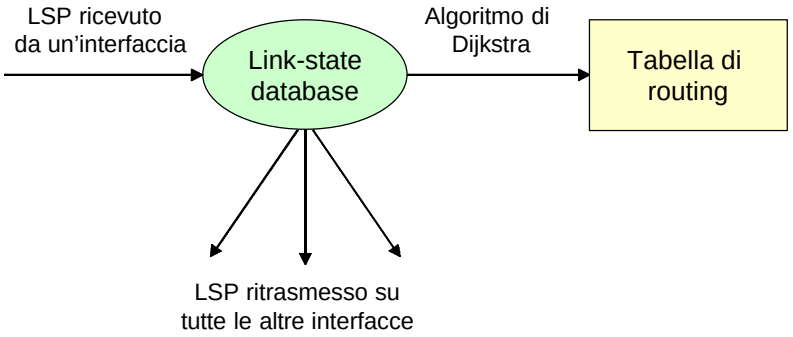
- Vantaggi:
  - **Molto semplice da implementare**
- Svantaggi
  - **Possono innescarsi dei loop a causa di particolari variazioni della topologia**
  - **Converge alla velocità del link più lento e del router più lento**
  - **Difficile capirne e prevederne il comportamento su reti grandi: nessun nodo 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**

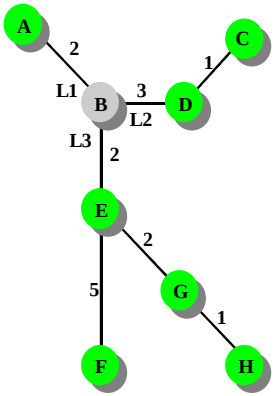
Link State: operazione di un router

- 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*
A	B(2) D(3) E(2)
B	A(2) D(3) E(2)
C	D(1)
D	B(3) C(1)
E	B(2) F(5) G(2)
F	E(5)
G	E(2) H(1)
H	G(1)

Tabella di routing di B

A	L1
C	L2
D	L2
E	L3
F	L3
G	L3
H	L3

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)

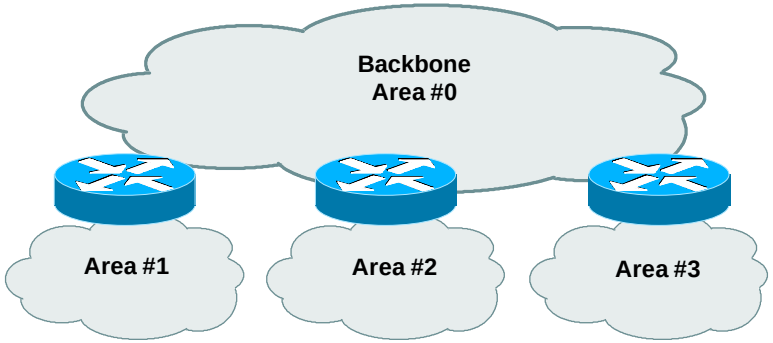
RIP

- 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 (*core 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*

Sistemi autonomi

- Un sistema autonomo (*Autonomous System* - AS) è un insieme di host e router controllato da una singola autorità amministrativa
  - **un particolare AS è detto "Core AS" e costituisce il backbone di Internet**
  - **un router del core AS è detto *Core Router***
  - **gli altri AS sono detti "Stub AS"**
- Ogni AS ha il proprio protocollo di instradamento
- Uno Stub AS deve avere almeno un router connesso ad un core router; questi router sono detti *Exterior Gateway*
- Un router interno ad un AS è detto *Interior Gateway*

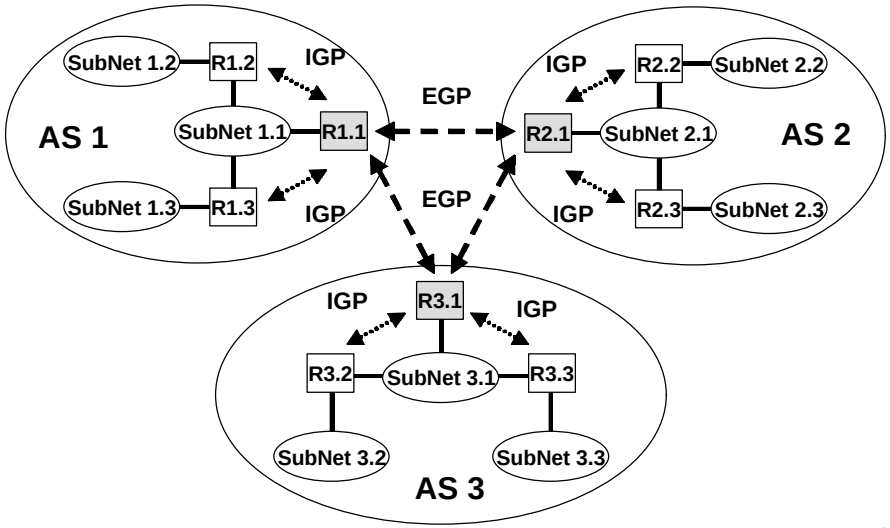
Interior and Exterior Gateway Protocols

- 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)**

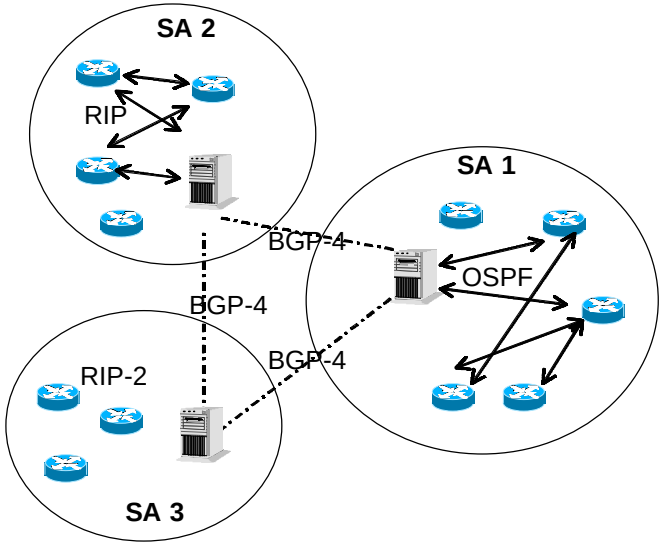
Interior and Exterior Gateway Protocols

- 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 and EGP: architecture



IGP and EGP: protocols



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

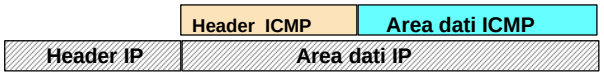
- ICMP ha lo scopo esclusivo di notificare errori all'host di origine
  - **ICMP non specifica le azioni che devono essere prese per rimediare ai malfunzionamenti**
  - **spetta all'host di origine decidere le azioni da intraprendere per correggere il problema**
- I messaggi di ICMP viaggiano come comuni 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

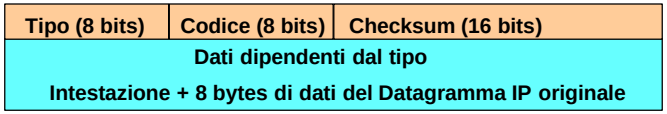
- Esempi:
  - **Source Quench: inviato dal destinatario, interrompe l'emissione di datagrammi del mittente;**
  - **Redirect: il destinatario segnala al mittente di re-instradare il datagramma verso un altro host;**
  - **Echo: controlla se un possibile destinatario è attivo,**
  - **Destination Unreacheable: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

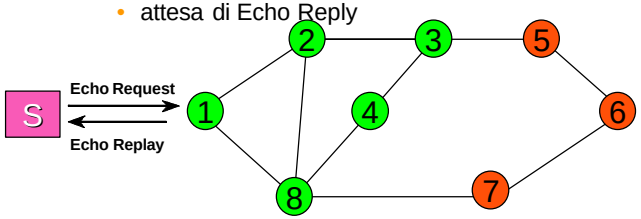
- Echo e Echo replay
  - **sono utilizzati per stabilire l'attività di un elemento di un host**
- Destination unreachable
  - **indica che l'instradamento di un datagramma non è stato completato**
- Time Stamp Request e Time Stamp Replay
  - **sono utilizzati per effettuare misure di prestazioni (es. 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

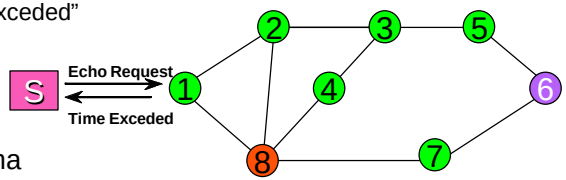
```
[user]$ ping pinco.pallino.net

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
  - **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

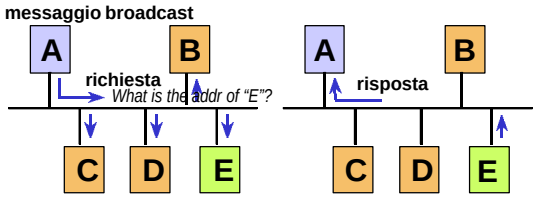
```
traceroute to www.stanford.edu (171.64.14.203), 30 hops max, 40 byte
packets
 1  151.100.238.1 (151.100.238.1)  2678.773 ms
 2  rc-uniromaI.rm.garr.net (193.206.131.49)  1859.746 ms
 3  rt-rc-2.rm.garr.net (193.206.134.165)  788.237 ms
 4  mi-rm-1.garr.net (193.206.134.17)  766.614 ms
 5  ny-mi.garr.net (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)

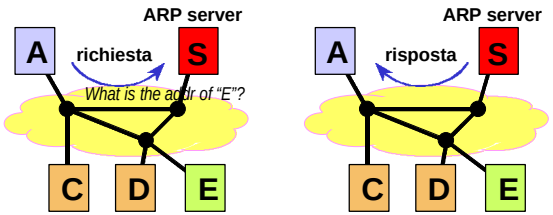
Risoluzione degli indirizzi

- 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)

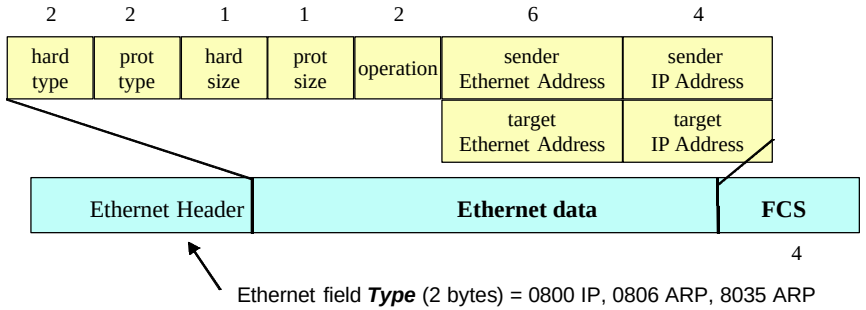


ARP

- 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

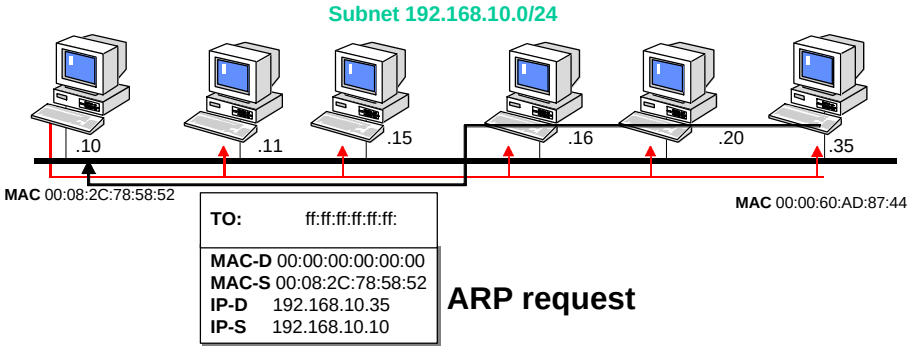
ARP

- 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



La postazione aggiunge la coppia MAC/IP alla propria cache

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

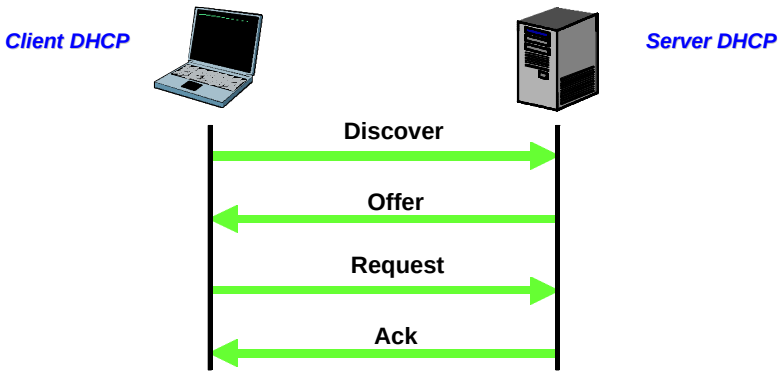
- BOOTP (BOOTstrap Protocol) (RFC 951, 1048, 1084)
  - **permette di acquisire all'avvio (bootstrap) informazioni di configurazione quali: (proprio IP address, indirizzo di un router, indirizzo di un server,...)**
  - **è adatto per host senza disco rigido**
  - **vengono scambiati messaggi (UDP) tra 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

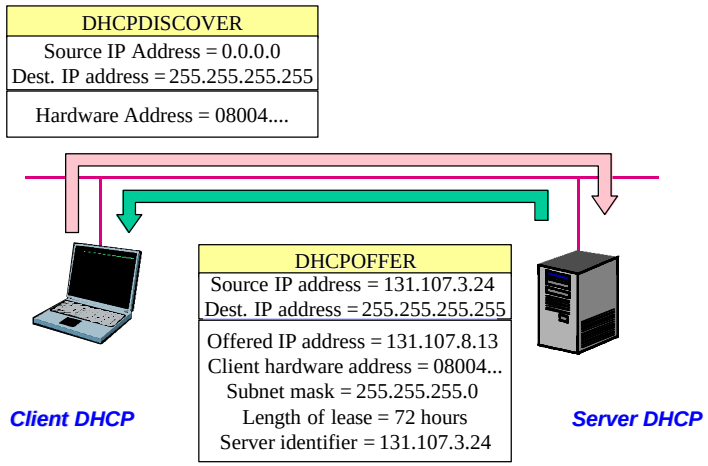
- DHCP (RFC 2131) è un'estensione di BOOTP che permette di:
  - **assegnare dinamicamente gli indirizzi IP**
  - **ricevere altre informazioni di configurazione (esempio: subnet mask)**
- DHCP è utile quando:
  - **i computer si connettono e disconnettono frequentemente**
  - **il numero di computer 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**

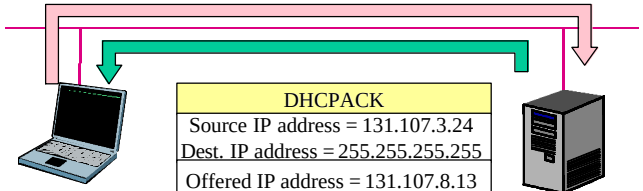


DHCP: Discover e Offer



DHCP: Request e Ack

DHCPREQUEST
Source IP address = 0.0.0.0 Dest. IP address = 255.255.255.255
Hardware address = 08004… Requested IP address = 131.107.8.13 Server identifier = 131.107.3.24



DHCPACK
Source IP address = 131.107.3.24 Dest. IP address = 255.255.255.255
Offered IP address = 131.107.8.13 Client hardware address = 08004... Subnet mask = 255.255.255.0 Length of lease = 72 hours Server identifier = 131.107.3.24 DHCP option: router = 131.107.8.1

Client DHCP *Server DHCP*

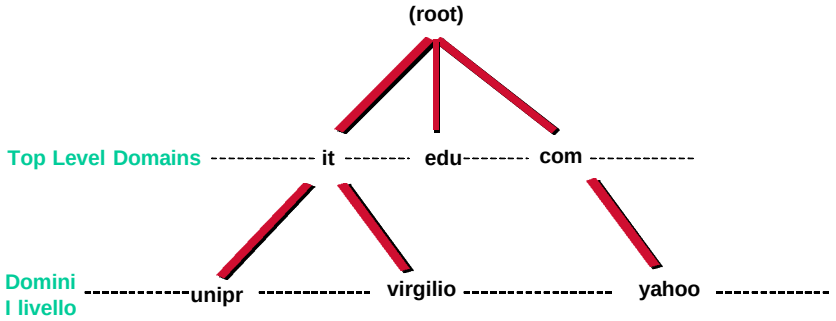
Point to Point Protocol

- 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**

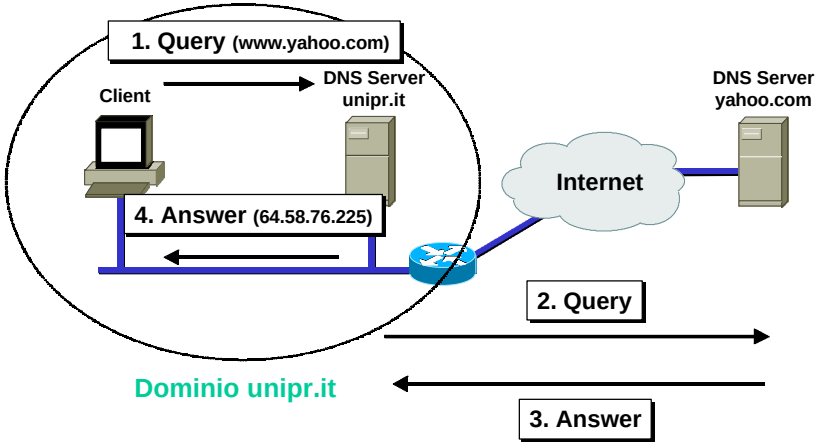


DNS (Domain Name System)

- **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 ...)**
country-code	**Codice di due caratteri per indicare una nazione**

Risoluzione dei nomi



Root Name Server

- Quando un server DNS riceve una query per un nome appartenente ad un dominio di cui non ha autorità effettua le 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**

Cenni a IPv6

Perchè IPv6

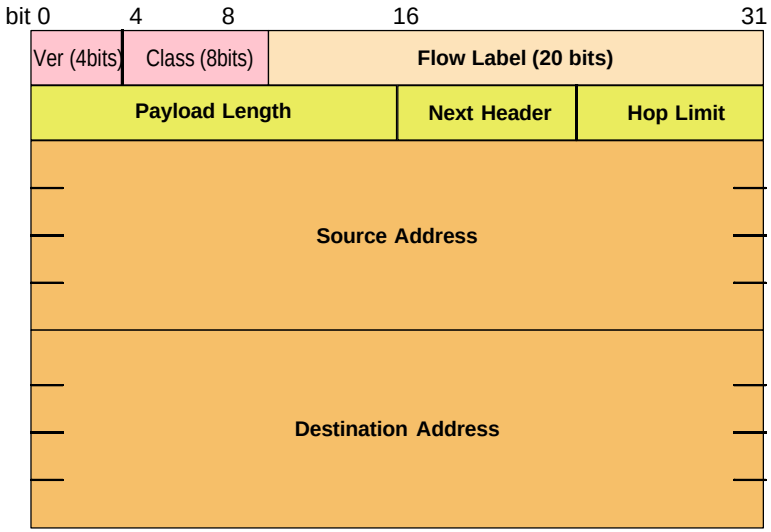
- Esaurimento dello spazio di indirizzamento IPv4
- Esplosione delle tabelle di instradamento sui router
- Servizi nuvi e/o più efficent
  - **Soluzione di networking "plug&play"**
  - **Qualità del Servizio**
  - **Sicurezza**
  - **Mobilità**
  - **Multicast**

Indirizzi IP: quanti?

- Classici terminali IP
  - **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/m2**

  (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 suddividerli in 8 blocchi di 16 bit ciascuno
- I blocchi sono separati mediante il carattere ":" e vengono rappresentati in notazione esadecimale
- Un esempio di indirizzo IPv6 è:
  - **3FFE:1001:7654:3220:FEDC:BA98:789A:32AC**
- Esistono delle semplificazioni:
  - **si possono omettere gli zeri iniziali di ogni blocco**
    - 3ffe:1001:1:100:a00:20ff:fe83:5531
  - **si possono sostituire gruppi di zeri con "::"**
    - 3ffe:1001:1::1