

il livello di rete

nelle reti locali e
nelle reti geografiche

g.di battista, m.patrignani, m.pizzonia

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

nota di copyright

- questo insieme di slides è protetto dalle leggi sul copyright
- il titolo ed il copyright relativi alle slides (inclusi, ma non limitatamente, immagini, foto, animazioni, video, audio, musica e testo) sono di proprietà degli autori indicati sulla prima pagina
- le slides possono essere riprodotte ed utilizzate liberamente, non a fini di lucro, da università e scuole pubbliche e da istituti pubblici di ricerca
- ogni altro uso o riproduzione è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori
- l'informazione contenuta in queste slides è fornita per scopi didattici e non può essere usata in progetti di reti, impianti, prodotti, ecc.
- gli autori non si assumono nessuna responsabilità per il contenuto delle slides, che sono comunque soggette a cambiamento
- questa nota di copyright non deve essere mai rimossa e deve essere riportata anche in casi di uso parziale

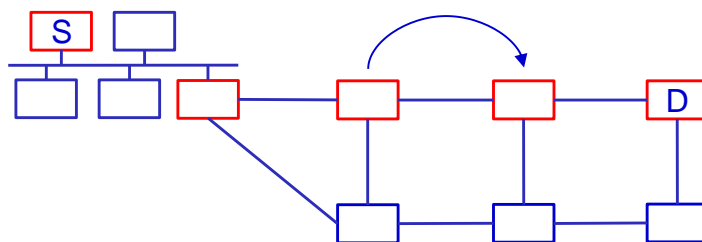
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

metodi e modelli per il livello di rete

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

il livello di rete

- il livello di rete sceglie una strada per i pacchetti
 - conosce la topologia della rete
- la strada verso la destinazione è composta da vari passaggi intermedi (*salti* o *hop*)



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

il livello di rete

- il livello di rete fornisce servizi al livello di trasporto, il quale non è interessato a conoscere:
 - il numero e la topologia delle varie reti (lan o semplici link) che vengono attraversate per raggiungere una destinazione
 - le tecnologie usate per realizzare le reti attraversate

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

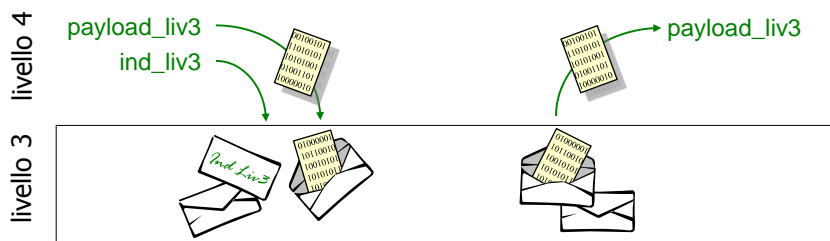
livello di rete: connesso o non connesso?

- i servizi offerti dal livello di rete al livello di trasporto possono essere connessi o non connessi
 - il protocollo di rete più diffuso (IPv4) offre esclusivamente un servizio non connesso
- l'instradamento può essere a datagramma o a circuito virtuale
 - un livello di rete connesso fa tipicamente uso della commutazione a circuito virtuale
 - un livello di rete non connesso fa tipicamente uso della commutazione a datagramma

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

interfaccia con il livello 4

- il livello di trasporto (livello 4) ha bisogno di conoscere le macchine attraverso:
 - indirizzi univoci, distribuiti in modo consistente su tutta la rete
- esempio di primitiva di servizio non connesso offerta al livello di trasporto:
 - `spedisci_pacchetto(ind_liv3, payload_liv3)`



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

assunzioni e terminologia

- i sistemi sulla rete possono essere:
 - *end system (es)* o *intermediate system (is)*
- ad ogni sistema è associato un indirizzo numerico
 - talvolta (oltre all'indirizzo) al sistema è associato un nome
 - informazioni sulla corrispondenza nomi-indirizzi sono gestite da server appositi, spesso chiamati name server

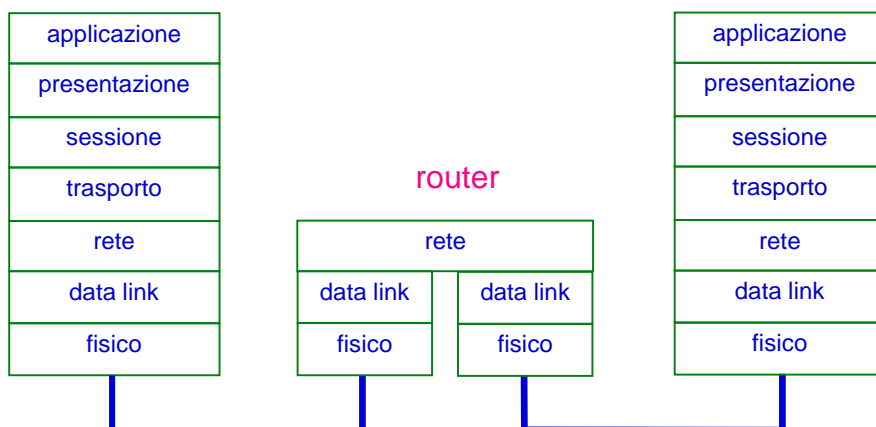
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

assunzioni e terminologia

- gli is, chiamati anche *router* o *gateway*, operano a livello 3 e contengono (almeno) gli strati 1,2 e 3 dell'architettura iso-osi
 - nota: talvolta gli is, per motivi di gestione, contengono anche gli strati superiori dell'architettura
 - nota: l'instradamento è normalmente effettuato a livello 3, però alcuni casi elementari di instradamento si riscontrano anche a livello 2 (bridge-switch)

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

router e modello iso-osi



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento

- l'indirizzo di livello 2 (mac) identifica il destinatario in una lan
- l'indirizzo di livello 3 identifica il destinatario nell'ambito dell'intera rete
- un sistema necessita di tanti indirizzi mac quante sono le sue schede di rete e di un solo indirizzo di livello 3
 - alcuni protocolli di livello tre (come il protocollo IPv4) assegnano un indirizzo di rete ad ogni scheda di rete
- esistono vari modi per mantenere la corrispondenza tra indirizzi di livello 2 e 3

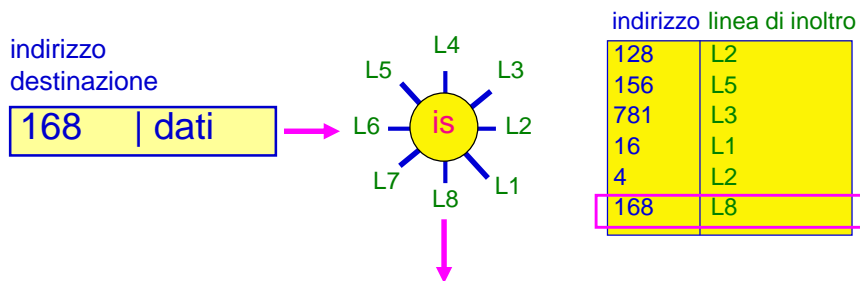
120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

metodi di instradamento

- gli is possono effettuare instradamento con tre metodi principali:
 - routing by network address
 - nel pacchetto c'è l'indirizzo del sistema destinatario
 - la commutazione è a datagramma in base a tale indirizzo
 - label swapping
 - nel pacchetto c'è una label che identifica il cammino virtuale
 - la commutazione è a circuito virtuale in base alla label
 - source routing
 - nel pacchetto è specificata la successione di is da attraversare
 - es: bridge token ring

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

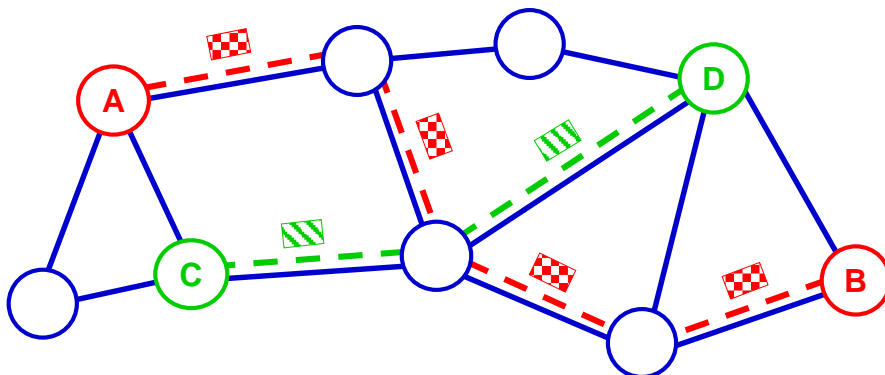
routing by network address



- nel pacchetto c'è l'indirizzo del sistema destinatario
- l'is usa l'indirizzo come chiave di ricerca in una tabella locale e determina la linea di ritrasmissione
- la commutazione è a datagramma

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

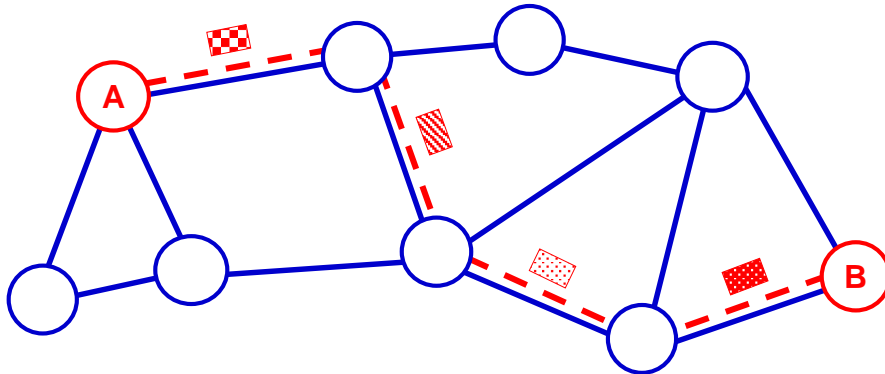
label (senza) swapping



- nel pacchetto c'è un'etichetta (label) che indentifica il circuito virtuale
- l'is usa la label come chiave di ricerca in una tabella locale (molto piccola) e determina la linea di ritrasmissione
- la commutazione è a circuito virtuale

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

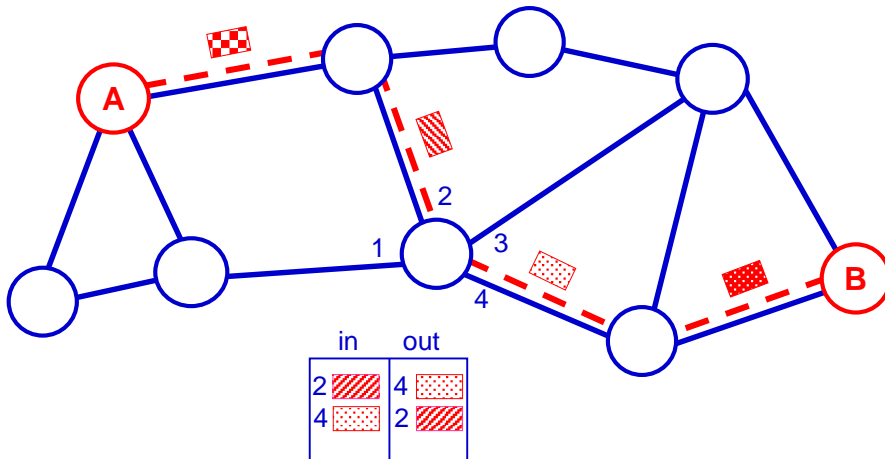
label swapping



- per evitare di dover verificare nell'intera rete che una specifica label non sia già utilizzata per qualche altra connessione, ad ogni tratto del circuito è assegnata una label (in generale) diversa ed assegnata localmente

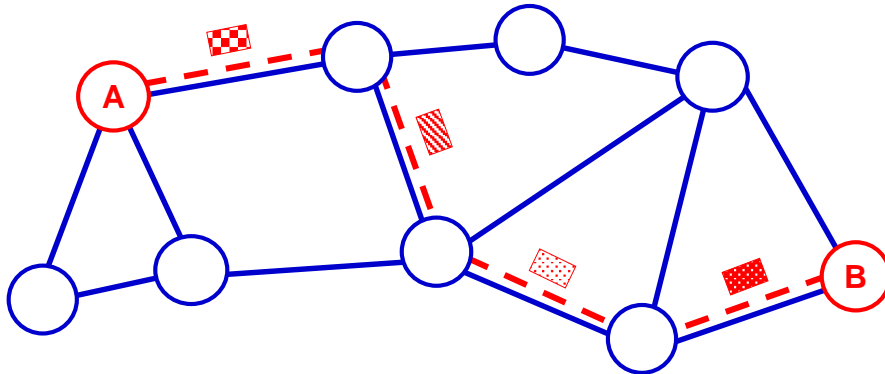
120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

label swapping



120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

label swapping

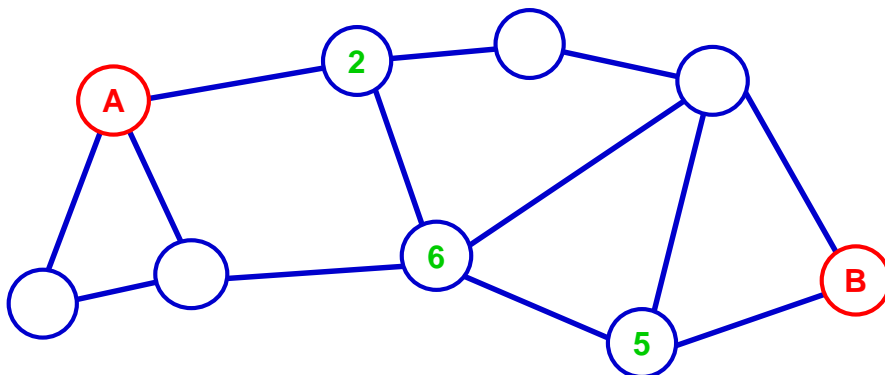


■ in questo modo

- la label può essere scelta dagli is che condividono il link
- il numero delle label disponibili non è un limite superiore al numero dei circuiti virtuali attivabili

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

source routing

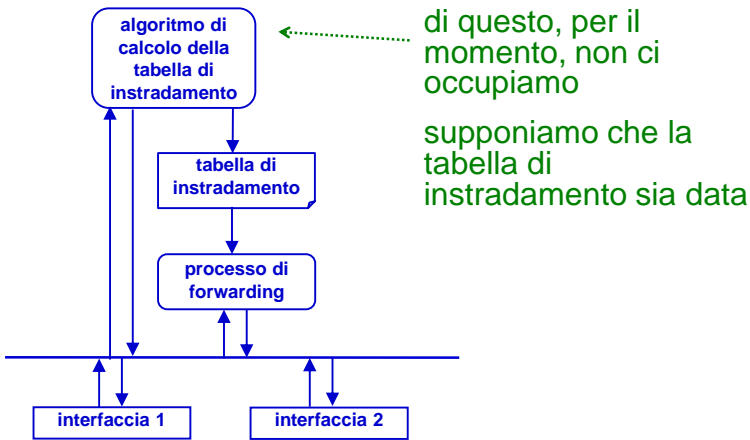


■ nel pacchetto tutta la strada da fare tra A e B



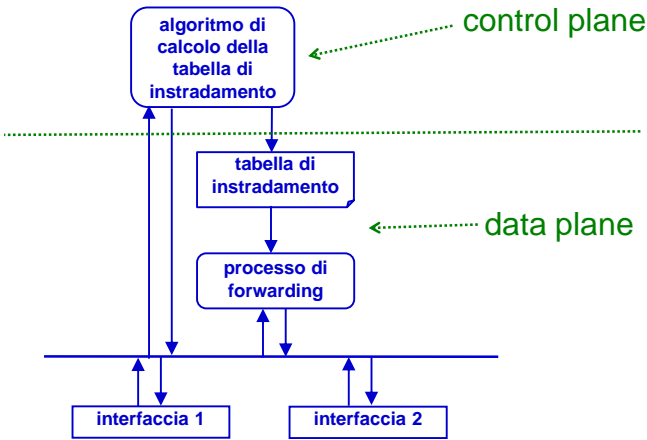
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

architettura di massima di un router



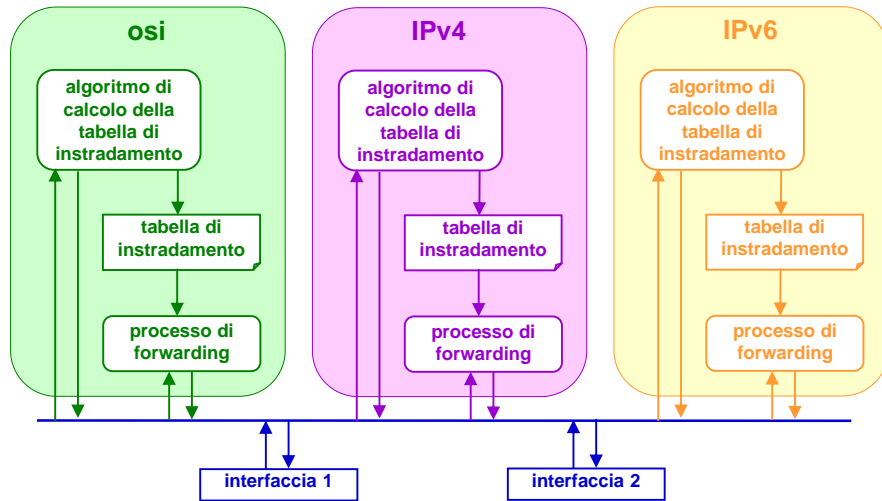
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

le due funzioni di un router



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

architettura di massima di un router multiprotocollo



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonla

IPv4 e la suite TCP/IP

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonla

il protocollo IPv4 e la suite TCP/IP

- il protocollo IPv4 (Internet Protocol versione 4) è il principale protocollo di rete della “suite TCP/IP”, detta anche “internet protocol suite”
- la suite TCP/IP è la pila protocollare utilizzata per la rete internet ed implementata nella stragrande maggioranza dei computer
 - attenzione ai vari significati della parola “internet”
- i protocolli della suite sono descritti da documenti chiamati request for comments (rfc)
 - ad es. l'rfc 791 descrive IPv4

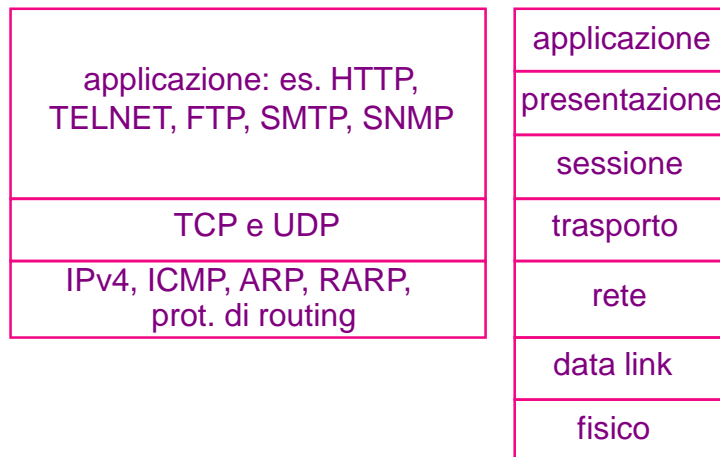
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

breve storia della suite TCP/IP

- nella prima metà degli anni '70, la defense advanced research project agency (darpa) finanzia l'università di stanford e la bbn per lo sviluppo di protocolli per lo scambio di dati tra computer
- alla fine degli anni '70, nasce l'internet protocol suite che comprende transmission control protocol (TCP) e internet protocol (IPv4) e ne deriva una prima rete chiamata arpanet
- da allora la rete internet è in costante crescita
 - 20.000.000 di calcolatori all'inizio del 1994, tasso di crescita del 5% all'anno

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

architettura della suite TCP/IP



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

architettura

- esempi di possibili stratificazioni di protocolli:
 - TELNET/TCP/IPv4/802.3
 - FTP/TCP/IPv4/802.3
 - SNMP/UDP/IPv4/802.11
- sotto lo strato IPv4 ci possono essere i vari standard lan (es. ieee 802) e wan (es. hdlc, ppp)

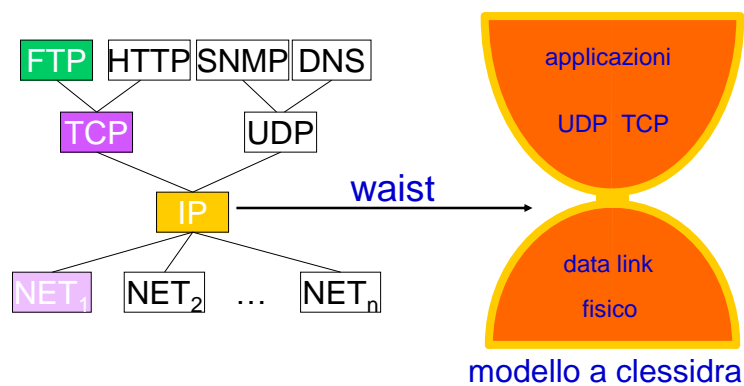
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

principi progettuali della suite TCP/IP

- semplificazione estrema del data plane degli is e spostamento di tutte le funzioni complesse sugli es
- routing by network address, commutazione di pacchetto a datagramma
- servizio non connesso
- servizio best-effort – un pacchetto:
 - può andare perduto
 - può essere corrotto
 - può essere consegnato in ordine errato

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

principi progettuali della suite TCP/IP



la "narrow waist" facilita l'interoperabilità

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

IPv4

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. piztonia

IPv4 (Internet Protocol versione 4)

- è attualmente il protocollo principale di livello 3
 - descritto nell'rfc 791
- il pacchetto si viene chiamato "IPv4 datagram"
- funzioni di instradamento, frammentazione, riassetblaggio, rilevazione di errori
- riceve messaggi dai protocolli UDP e TCP del livello superiore
- preleva i datagram, eventualmente li frammenta, e provvede al loro instradamento

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. piztonia

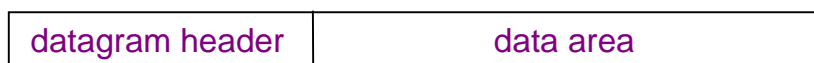
IPv4 (Internet Protocol versione 4)

- la grandezza del datagram dipende dai vincoli del livello due
- se il datagram è troppo grande, IPv4 provvede alla frammentazione
- provvedere al routing è semplice nel caso in cui il datagram viaggi all'interno di una lan, più complesso se la spedizione coinvolge un host remoto
- lo strato IPv4 di un router non può comunque riassemblare i datagrammi

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

formato dell'IPv4 datagram

- analogamente ai pacchetti di livello 2, il datagram IPv4 è diviso in due aree: l'header e l'area dei dati



- l'header contiene gli indirizzi del mittente e del destinatario
 - si tratta ovviamente di indirizzi IPv4

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

formato dell'IPv4 datagram

31

version	ihl	type of service	total length	
ident			flags	fragment offset
time to live	protocol		header checksum	
source IP address				
destination IP address				
options				padding
data				
...				

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

linguaggio comune di tutti gli es e is del mondo

0					31						
version		ihl		type of service			total length				
ident					flags		fragment offset				
time to live			protocol			header checksum					
source IP address											
destination IP address											
options							padding				
data											
...											

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

i campi version e ihl

- version (4 bit)
 - è il numero di versione del protocollo IP che ha generato il pacchetto, attualmente vale 4 😊
 - grazie al campo version la migrazione tra due versioni può essere più chiara, lenta e controllata (?)
- ihl (4 bit)
 - è la lunghezza dell'header, espressa in parole di 32 bit
 - variabile in funzione dei campi options
 - valore minimo 5
 - quanti byte al massimo può avere l'header?

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

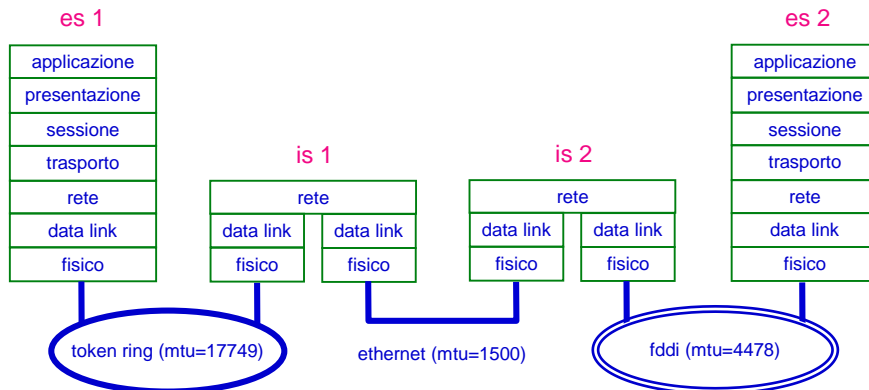
il campo type of service

- il campo type of service specifica la priorità di un datagram rispetto ad un altro
- rfc più recenti suddividono il campo in due parti:
 - DSCP – Differentiated Services Code Point – in funzione del suo valore il pacchetto riceve un diverso trattamento
 - ECN – Explicit Congestion Notification

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

i campi ident, flags e fragment offset

- perché frammentare un pacchetto a livello tre?
- ogni mezzo fisico potrebbe avere una maximum transmission unit (mtu) diversa
- il pacchetto di livello tre potrebbe essere troppo grande per essere imbustato in un pacchetto data link intermedio



120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

frammentazione e riassemblaggio

- consiste nella suddivisione (detta frammentazione) di un pacchetto in pacchetti più piccoli
- il pacchetto originale viene ricostituito (riassemblato) sulla macchina destinazione
 - non è efficiente tentare un riassemblaggio su un is

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

frammentazione e riassetblaggio

- **occorrono degli appositi campi nell'header di livello tre che consentano di:**
 - riconoscere il pacchetto come frammento
 - riconoscere i frammenti generati dallo stesso pacchetto
 - determinare l'ordine dei frammenti in maniera da poter riassetblare il pacchetto originale
 - l'adozione di un semplice contatore non rende possibile la frammentazione di un pacchetto già frammentato
 - l'adozione di un offset (spiazzamento) rispetto al pacchetto originale consente la successiva frammentazione dei frammenti

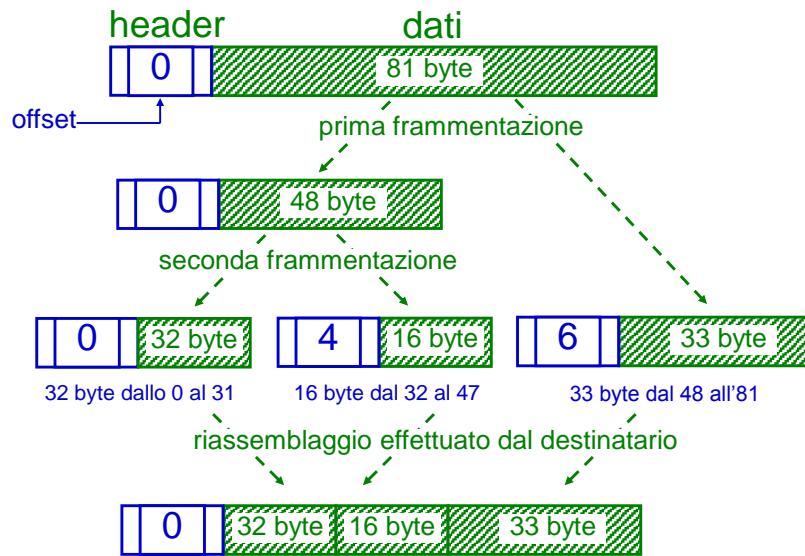
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

i campi ident, flags e fragment offset

- **usati per gestire la frammentazione dei datagrammi**
 - **ident (16 bit)**
 - intero che identifica un datagramma, serve all'IPv4 dell'host ricevente nel momento del riassetblaggio; due datagrammi con lo stesso ident vengono riassetblati nello stesso pacchetto
 - **fragment offset (13 bit)**
 - serve a riunire i frammenti nel giusto ordine
 - essendo di 13 bit, può specificare solo un offset multiplo di 8 (con la convenzione gli ultimi tre bit siano zeri)
 - tutti i frammenti eccetto l'ultimo hanno un numero di byte multiplo di 8; al massimo 8192 frammenti per datagramma
 - **flags (3 bit)**
 - il primo bit è riservato e deve essere sempre zero
 - DF (don't fragment) specifica se il datagram può essere frammentato, e può essere usato per eseguire una path mtu discovery molto primitiva
 - MF (more fragment) permette di riconoscere l'ultimo frammento del pacchetto

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

esempio di uso dell'offset



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

i campi total length e time to live

- **total length (16 bit)**
 - è la lunghezza del pacchetto completo di header e payload (al massimo 65.535 byte)
- **time to live (8 bit)**
 - specifica qual'è il tempo di vita del pacchetto
 - decrementato con il passare del tempo
 - quando vale 0 il pacchetto viene scartato
 - normalmente è decrementato ad ogni "hop"
 - quando il pacchetto è scartato il router manda un avvertimento al mittente

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

i campi protocol e header checksum

- protocol (8 bit)

- identifica il protocollo di livello superiore che è nel payload pacchetto IPv4
- i codici sono descritti nell'rfc 1700
- esempi: 1 = ICMP; 6 = TCP; 17 = UDP; ...

- header checksum (16 bit)

- riguarda solo l'header; deve essere ricalcolato ad ogni hop, perché?

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

il campo option

- è usato per informazioni meno frequenti nei pacchetti e per sperimentazione; ogni opzione inizia con 1 byte di codice che ne specifica il tipo
- opzioni principali (non supportate da tutti i router)
 - sicurezza quanto è segreto il datagramma?
 - source routing specifica del cammino completo
 - loose s.rout. sequenza di router di passaggio obbligato
 - record route ogni router attraversato specifica il proprio indirizzo
 - timestamp ogni router attraversato specifica il proprio indirizzo e un timestamp

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4

- gli indirizzi sono associati alle schede di rete e non agli host
- spazio degli indirizzi
 - gli indirizzi sono di 32 bit (4 byte)
 - univoci a livello mondiale
 - normalmente si rappresentano con 4 numeri decimali separati da punti
 - es. 151.146.5.31
 - di solito agli indirizzi corrispondono dei nomi simbolici

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4

- problema: se gli indirizzi IPv4 fossero assegnati alle macchine in modo del tutto arbitrario la tabella di instradamento di un router dovrebbe contenere un numero enorme di righe

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4

- idea generale di soluzione: assegnare indirizzi che cominciano nello stesso modo (con lo stesso prefisso) a macchine allocate fisicamente nella stessa rete locale
 - come si fa per i numeri telefonici dello stesso distretto
 - un gruppo di macchine è individuato dal suo prefisso
 - un is contiene tabelle di prefissi invece di tabelle di indirizzi

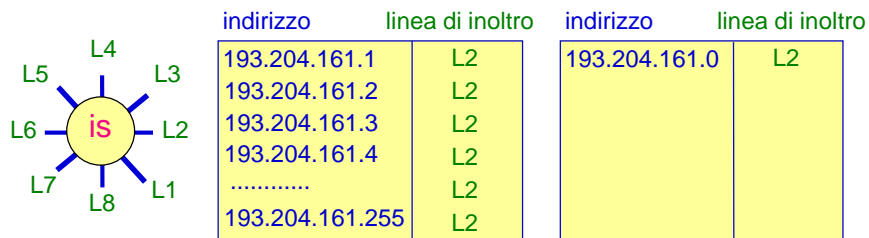
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4 – net

- gli indirizzi sono quindi raggruppati in net
 - per esempio, gli indirizzi:
193.204.161.1
193.204.161.2
193.204.161.3
...
193.204.161.255
con prefisso 193.204.161 sono raggruppati in una sola riga della tabella di instradamento
 - convenzionalmente un prefisso è completato con zeri fino ad ottenere un indirizzo IPv4 legittimo (in questo caso 193.204.161.0)
 - il valore ottenuto viene usato per denotare l'intera lan, e non viene assegnato a nessuna interfaccia di rete
- gli indirizzi delle macchine di una stessa rete fisica (es. lan) appartengono alla stessa net

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4 – net



semplificazione delle tabelle d'instradamento

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

conseguenza del raggruppamento degli indirizzi IPv4 in net

- un indirizzo IPv4 ha due funzioni:
 - identificazione: ogni sistema ha un indirizzo IPv4 distinto
 - location: indirizzi con lo stesso prefisso sono fisicamente nella stessa rete locale

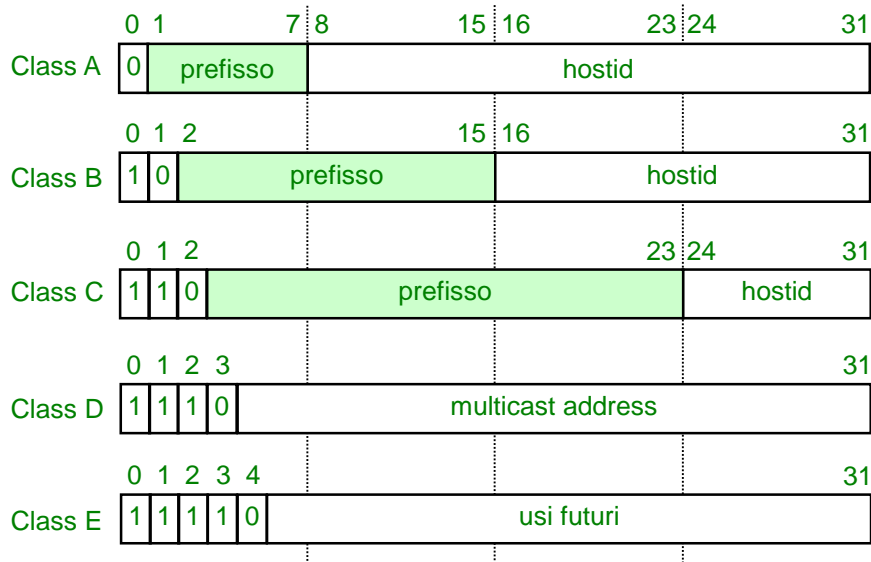
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4 classful

- sono definite cinque classi di indirizzi con prefissi di diversa lunghezza
- le classi sono: Class A, B, C, D, E

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4 classful



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4 classful

Class A	da	0.0.0.0	a	127.255.255.255
Class B	da	128.0.0.0	a	191.255.255.255
Class C	da	192.0.0.0	a	223.255.255.255
Class D	da	224.0.0.0	a	239.255.255.255
Class E	da	240.0.0.0	a	247.255.255.255

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4 classful

- Class A (da 0.0.0.0 a 127.255.255.255)
 - poche reti di dimensioni notevoli, 7 bit per la net e 24 per l'host, max 126 net e circa 16 milioni di host per net, il primo campo ha valore compreso tra 1 e 127
- Class B (da 128.0.0.0 a 191.255.255.255)
 - numero medio di reti di dimensioni medio-grandi, 14 bit per la net e 16 per l'host, max 16382 net e circa 64000 host per net, il primo campo ha valore compreso tra 128 e 191
- Class C (da 192.0.0.0 a 223.255.255.255)
 - molte net di dimensioni piccole, 22 bit per la net e 8 per l'host, max 2milioni di net e 256 di host per net, il primo campo ha valore compreso tra 192 e 223
- Class D (da 224.0.0.0 a 239.255.255.255)
 - riservati per uso multicast
- Class E riservati per usi futuri

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

esempi di indirizzi IPv4 classful

- 18.24.32.234
 - indirizzo di classe A
 - host 24.32.234 della rete con prefisso 18.0.0.0
- 128.148.38.84
 - indirizzo di classe B
 - host 38.84 della rete con prefisso 128.148.0.0
- 193.204.161.179
 - indirizzo di classe C
 - host 179 della rete con prefisso 193.204.161.0
- 224.0.0.1
 - indirizzo multicast che corrisponde a tutti i sistemi sulla net
- 224.0.0.2
 - indirizzo multicast che corrisponde a tutti i router sulla net

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4 classless – netmask

- per regioni di flessibilità l'indirizzamento classful è stato abbandonato per consentire una lunghezza arbitraria della parte prefisso dell'indirizzo IPv4 (indirizzamento *classless*)
 - nell'indirizzamento classful la lunghezza del prefisso è univocamente determinata dal valore dell'indirizzo
 - nell'indirizzamento classless la lunghezza del prefisso deve essere indicata esplicitamente per ogni indirizzo
- ad ogni indirizzo IPv4 viene associata una *netmask*
 - sequenza di 32 bit, composta da uno contigui seguiti da zeri
 - specifica la lunghezza del prefisso (gli uno) e quella di hostid (gli zeri)
 - esempio di netmask
 - binario: 11111111.11111111.11111111.00000000
 - equivalente decimale: 255.255.255.0

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzamento IPv4 classless – netmask

- la netmask 255.255.255.0 associata, per esempio, all'indirizzo 16.204.161.123 indica che il prefisso è costituito dai primi tre byte e l'host è identificato dall'ultimo byte
- tutti gli indirizzi con lo stesso prefisso hanno la stessa netmask, quindi si può parlare di netmask di un prefisso
- la netmask di un prefisso si può denotare più semplicemente specificando, dopo l'indirizzo IPv4, la lunghezza del prefisso, separata da una barra
 - esempio: 193.200.160.0/24
 - equivale a 193.200.160.0 con netmask 255.255.255.0

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

indirizzamento IPv4 classless – netmask

- due indirizzi IPv4 che hanno lo stesso prefisso (cioè sono nella stessa lan) danno luogo allo stesso valore se messi in and bit-a-bit con la netmask relativa
 - esempio
 - 193.200.100.23 con netmask 255.255.255.0
 - 193.200.100.130 con netmask 255.255.255.0
 - producono entrambi 193.200.100.0
- due indirizzi IPv4 che hanno prefisso diverso (cioè cadono in due diverse reti fisiche) se messi in and bit-a-bit con la propria netmask producono valori diversi
 - ciò è vero se gli insiemi di indirizzi sono assegnati alle reti in modo tale che siano tutti disgiunti tra loro
 - la responsabilità di assegnare indirizzi è lasciata ad organizzazioni internazionali quali RIPE, ecc....

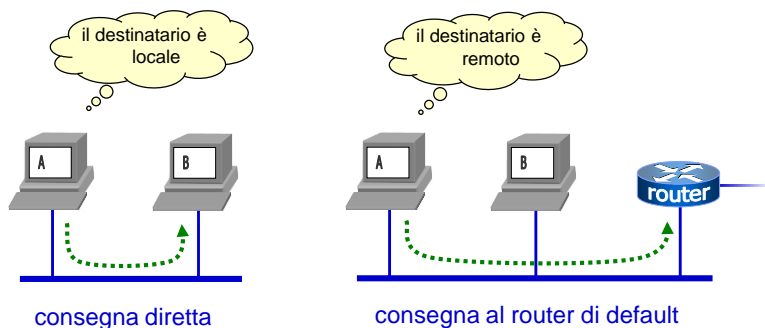
120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

invio di un pacchetto

- la configurazione delle interfacce degli es prevede, oltre all'assegnazione di un indirizzo IPv4, anche la specifica della netmask della net di appartenenza
- mettendo in and-bit-a-bit il proprio indirizzo e quello del destinatario con la propria netmask, l'es determina se un destinatario è locale o remoto
 - se il destinatario è locale il pacchetto viene inviato al destinatario stesso (trasmissione diretta)
 - se il destinatario è remoto il pacchetto viene inviato al default gateway, cioè ad un is

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

invio di un pacchetto



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

invio di un pacchetto

■ esempio:

- un es (calcolatore) con indirizzo 193.204.161.8 deve mandare un pacchetto all'es 193.204.162.4
- 193.204.161.8 sa che la sua netmask è
 $255.255.255.128 = 11111111.11111111.11111111.10000000$
- mette in and bit-a-bit il suo indirizzo e la netmask e ottiene 193.204.161.0
- mette in and bit-a-bit l'indirizzo del destinatario e la netmask e ottiene 193.204.162.0
- conclude che il destinatario non è sulla sua stessa rete fisica

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

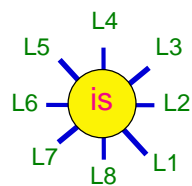
indirizzamento IPv4 classless – IP lookup

■ ricerca nella tabella di instradamento (IP lookup)

- ogni riga della tabella di instradamento di un router contiene un indirizzo di lan (prefisso) e la relativa netmask
- mettendo in and bit-a-bit l'indirizzo IPv4 del destinatario con la netmask e confrontandolo con l'indirizzo di lan il router determina se l'indirizzo è nella lan relativa (matching)
- la tabella di instradamento viene controllata una riga dopo l'altra
 - le righe sono ordinate in base alla lunghezza del prefisso (prefissi più lunghi vengono controllati prima)
 - non appena si riscontra un matching il pacchetto viene inoltrato nella linea relativa
 - se non avviene nessun matching il pacchetto viene scartato
 - la riga 0.0.0.0/0 (se presente) viene chiamata rotta di default; è l'ultima riga controllata e produce un matching con qualsiasi indirizzo

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

esempi di IP lookup



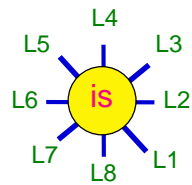
indirizzo	netmask	linea di inoltro
192.4.153.0	255.255.255.192	L3
128.96.39.0	255.255.255.128	L8
128.96.39.128	255.255.255.128	L1
128.96.40.0	255.255.255.128	L2
0.0.0.0	0.0.0.0	L4

pacchetti da inoltrare

128.96.39.10	dati
128.96.40.12	dati
128.96.40.151	dati
192.4.153.17	dati

su quali linee saranno inoltrati?
come si comporta il router?

esempi di IP lookup



indirizzo	netmask	linea di inoltro
192.4.153.0	255.255.255.192	L3
128.96.39.0	255.255.255.128	L8
128.96.39.128	255.255.255.128	L1
128.96.40.0	255.255.255.128	L2
0.0.0.0	0.0.0.0	L4

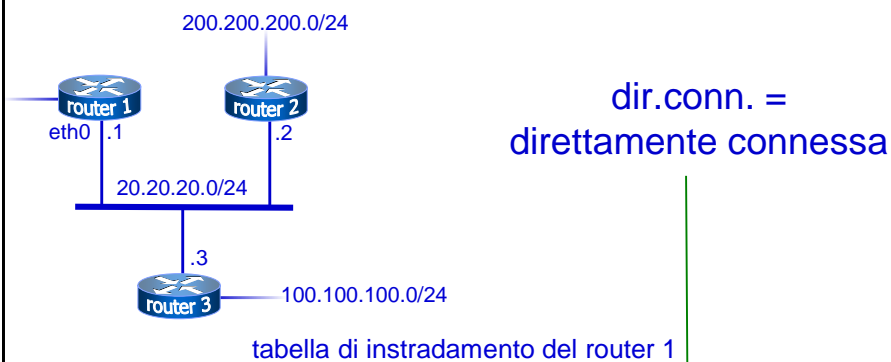
- 128.96.39.10 & 255.255.255.128 = 128.96.39.0 → L8
- 128.96.40.12 & 255.255.255.128 = 128.96.40.0 → L2
- 128.96.40.151 & 255.255.255.128 = 128.96.40.128 → L4
- 192.4.153.17 & 255.255.255.192 = 192.4.153.0 → L3

tabelle di instradamento

- dapprima immaginavamo che nella tabella di instradamento di un router ci fossero tutti i possibili indirizzi e le linee d'oltro
- poi abbiamo visto che le tabelle contengono prefissi, netmask e linee d'oltro
- manca ancora un elemento: il next hop
 - specifica l'indirizzo IPv4 della prossima interfaccia a cui inviare il pacchetto
 - a cosa serve? quando è necessario?

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. piztonia

tabelle di instradamento



network	netmask	interfaccia	next-hop
20.20.20.0	255.255.255.0	eth0	dir. conn.
100.100.100.0	255.255.255.0	eth0	20.20.20.3
200.200.200.0	255.255.255.0	eth0	20.20.20.2
...

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. piztonia

tabelle di instradamento

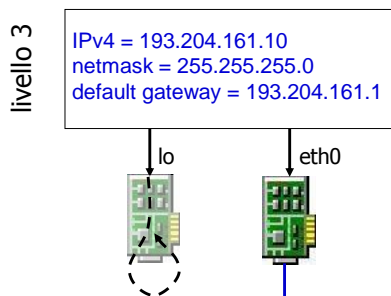
- le operazioni eseguite da un es per l'inoltro di un pacchetto (and bit-a-bit e scelta tra consegna diretta e consegna al router di default) possono essere pensate in termini di accesso ad una tabella d'instradamento
- effettivamente l'es ha a bordo una tabella con:
 - il prefisso a cui appartiene, con la relativa netmask
 - un prefisso convenzionale (127.0.0.0) a cui appartiene l'es stesso
 - una rotta di default

tabella di instradamento dell'es

network	netmask	interfaccia	next-hop
193.204.161.0	255.255.255.0	eth0	d.c.
127.0.0.0	255.0.0.0	lo	d.c.
0.0.0.0	0.0.0.0	eth0	193.204.161.1

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

tabelle di instradamento



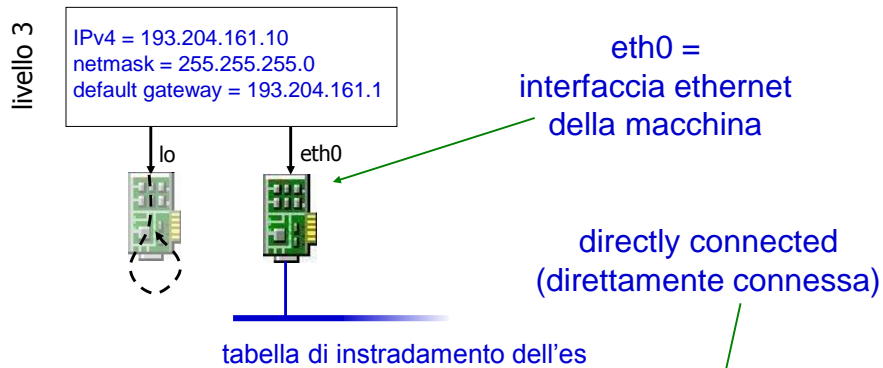
- se il pacchetto da inoltrare fa match con la prima riga, consegna diretta
- se fa match con la seconda riga è diretto alla macchina stessa
- se fa match con la terza riga è inviato al router di default

tabella di instradamento dell'es

network	netmask	interfaccia	next-hop
193.204.161.0	255.255.255.0	eth0	d.c.
127.0.0.0	255.0.0.0	lo	d.c.
0.0.0.0	0.0.0.0	eth0	193.204.161.1

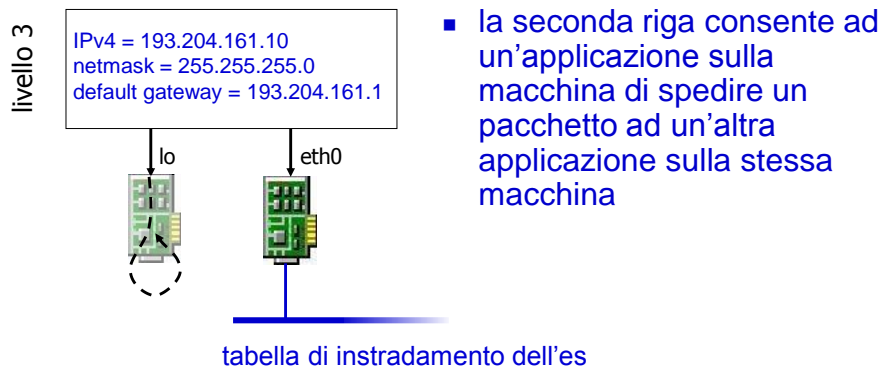
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

tabelle di instradamento



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

tabelle di instradamento



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzi IPv4 convenzionali

- alcuni indirizzi IPv4 hanno un significato convenzionale

0.0.0.0	questo calcolatore (in disuso)
127.0.0.1	questo calcolatore
255.255.255.255	broadcast nella net del mittente
<net>1...1	broadcast nella net <net>
10.0.0.0/8	indirizzi privati (non validi in internet)
172.16.0.0/12	indirizzi privati (non validi in internet)
192.168.0.0/16	indirizzi privati (non validi in internet)

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

distribuzione degli indirizzi IPv4

- IANA (Internet Assigned Numbers Authority)
 - autorità sovranazionale che delega la distribuzione di specifiche porzioni dello spazio di indirizzamento a delle autorità regionali
- ARIN (American Registry for Internet Numbers)
 - consorzio delegato per il Nord America
 - sostituisce la InterNIC (Internet Network Information Center) dal 1997
 - <http://www.arin.net>
- RIPE (Resèaux IP Européen) Coordination Center
 - delegato per l'Europa
 - <http://www.ripe.net>
- APNIC (Asia Pacific Network Information Center)
 - delegato per il pacifico e l'Asia
 - <http://www.apnic.net>

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

IPv4 – domande di riepilogo

- due interfacce di un router possono far parte della stessa rete IPv4?
 - no, il router separa le reti IPv4
 - ogni interfaccia del router ha un indirizzo IPv4 che cade necessariamente in una diversa rete IPv4
- quanti indirizzi IPv4 ha un router?
 - almeno due, in quanto ne ha uno per ogni interfaccia ed ha almeno due interfacce di rete
- uno switch ha un indirizzo IPv4?
 - per le funzioni di bridging non ne ha bisogno
 - necessita di un indirizzo IPv4 solo se contiene anche gli strati 3, 4 e 5 (solitamente per scopi amministrativi)
 - in questo caso lo switch ha un solo indirizzo di rete (una sola interfaccia virtuale) indipendentemente dal numero di porte che ospita

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzi IPv4 – una questione sottile

- l'es PCX, che ha indirizzo 100.100.100.100/16 (netmask 255.255.0.0), deve spedire due pacchetti
 - a PC1, il cui indirizzo è 100.100.100.124
 - a PC2 il cui indirizzo è 100.200.100.125
- per farlo PCX calcola il proprio prefisso e quello di PC1 e PC2 usando in tutti e tre i casi la sua netmask e non quella di PC1 e PC2 (che non conosce): può sbagliare?

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzi IPv4 – una questione sottile

- quando PCX spedisce il pacchetto a PC 1 (100.100.100.124), PC X calcola il proprio prefisso in 100.100.0.0 e il prefisso di PC1 in 100.100.0.0; il vero prefisso di PC 1 può essere 100.0.0.0?
- no, se il prefisso di PC 1 fosse 100.0.0.0, allora il prefisso di PCX sarebbe contenuto in quello di PC1; vorrebbe dire che gli indirizzi sono stati assegnati in modo non disgiunto

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzi IPv4 – una questione sottile

- quando PCX spedisce il pacchetto a PC 1 (100.100.100.124), PC X calcola il proprio prefisso in 100.100.0.0 e il prefisso di PC1 in 100.100.0.0; il vero prefisso di PC 1 può essere 100.100.100.0?
- no, se il prefisso di PC 1 fosse 100.100.100.0, allora il prefisso di PC1 sarebbe contenuto in quello di PCX; vorrebbe dire che gli indirizzi sono stati assegnati in modo non disgiunto

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzi IPv4 – una questione sottile

- quando PCX spedisce il pacchetto a PC 2 (100.200.100.125), PC X calcola il proprio prefisso in 100.100.0.0 e il prefisso di PC2 in 100.200.0.0; il vero prefisso di PC 2 può essere 100.0.0.0?
- no, se il prefisso di PC 2 fosse 100.0.0.0, allora il prefisso di PCX sarebbe contenuto in quello di PC2; vorrebbe dire che gli indirizzi sono stati assegnati in modo non disgiunto

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

indirizzi IPv4 – una questione sottile

- quando PCX spedisce il pacchetto a PC 2 (100.200.100.125), PCX calcola il proprio prefisso in 100.100.0.0 e il prefisso di PC2 in 100.200.0.0; il vero prefisso di PC 2 può essere 100.200.100.0?
- sì, è possibile; quindi in questo caso PCX avrebbe sbagliato il calcolo del prefisso; però poco male, si tratta comunque di una rete diversa da 100.100.0.0 e quindi il routing avrebbe funzionato ancora correttamente

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

end system con più schede

- gli es tendono ad avere varie schede
 - ethernet
 - wi-fi
- cosa succede ad IPv4 in presenza di più schede?
 - le schede sono tipicamente usate in alternativa invece che in parallelo
 - chi ha pensato IPv4 immaginava che un es avesse una sola scheda

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

ARP e RARP

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

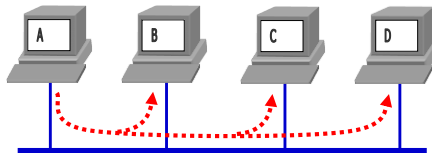
ARP (address resolution protocol)

- definito nell'rfc 826
- alle macchine che condividono una rete fisica sono associati due tipi di indirizzi
 - indirizzi IPv4, a cui fanno riferimento i protocolli di livello superiore
 - indirizzi mac, forniti dall'hardware delle macchine stesse
- il protocollo ARP risolve il problema della traduzione di un indirizzo IPv4 in indirizzo mac (neighbor greeting)

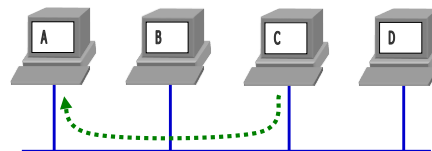
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

ARP – funzionamento

- l'host invia un messaggio broadcast a tutti gli host di una rete nel quale chiede alle macchine l'indirizzo mac corrispondente all'IPv4 dato (ARP request)



- l'host che ha quell'indirizzo IPv4 risponde con ARP reply, fornendo il proprio mac



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

ARP – uso della cache

- mandare messaggi broadcast è costoso
 - provocano un'interruzione a bordo di tutti gli host della lan
 - passano attraverso gli hub e gli switch
 - sono bloccati solo dai router
- gli host che usano ARP hanno a disposizione una cache in cui memorizzano le corrispondenze IPv4-mac di cui sono venuti a conoscenza
- solo se l'indirizzo IPv4 non viene trovato nella "ARP cache" si procede ad inviare in broadcast un ARP request

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

ARP – esempio di uso della cache

```
<gdb@hilbert ~> arp -a
fenarete.inf.uniroma3.it (193.204.162.47) at
0:a0:cc:66:73:cc [ethernet]
tutte.inf.uniroma3.it (193.204.162.23) at
8:0:7:bc:56:57 [ethernet]
mail.inf.uniroma3.it (193.204.162.99) at
2:60:8c:2f:61:f0 [ethernet]
salini-gw.uniroma3.it (193.204.162.1) at
0:0:c:3b:cb:6 [ethernet]
pascal.inf.uniroma3.it (193.204.162.8) at
8:0:5a:c7:45:79 [ethernet]
euclide.inf.uniroma3.it (193.204.162.11) at
2:60:8c:2d:d3:b7 [ethernet]
```

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

ARP – esempio di uso della cache

```
<gdb@hilbert ~> ping fermat.inf.uniroma3.it
PING fermat.inf.uniroma3.it: (193.204.162.7): 56 data bytes
64 bytes from 193.204.162.7: icmp_seq=0 ttl=255 time=1 ms
64 bytes from 193.204.162.7: icmp_seq=1 ttl=255 time=1 ms
64 bytes from 193.204.162.7: icmp_seq=2 ttl=255 time=1 ms
^C
----fermat.inf.uniroma3.it PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0/0/1 ms
```

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

ARP – esempio di uso della cache

```
<gdb@hilbert ~> arp -a
fenarete.inf.uniroma3.it (193.204.162.47) at
0:a0:cc:66:73:cc [ethernet]
tutte.inf.uniroma3.it (193.204.162.23) at
8:0:7:bc:56:57 [ethernet]
mail.inf.uniroma3.it (193.204.162.99) at
2:60:8c:2f:61:f0 [ethernet]
salini-gw.uniroma3.it (193.204.162.1) at
0:0:c:3b:cb:6 [ethernet]
fermat.inf.uniroma3.it (193.204.162.7) at
8:0:2b:bd:75:cf [ethernet]
pascal.inf.uniroma3.it (193.204.162.8) at
8:0:5a:c7:45:79 [ethernet]
euclide.inf.uniroma3.it (193.204.162.11) at
2:60:8c:2d:d3:b7 [ethernet]
```

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

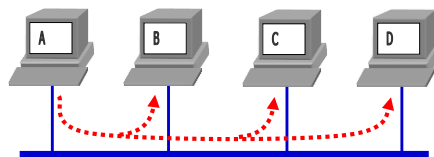
RARP (reverse ARP)

- definito nell'rfc 903
- risolve il problema della traduzione di un indirizzo mac nel corrispondente indirizzo IPv4
- uno scenario in cui RARP può essere usato è quello dello startup di una macchina priva di hard-disk
 - non disponendo di memoria secondaria la macchina deve avere tutti i dati in ram
 - allo startup richiede ad un server esterno il proprio indirizzo IPv4 (fornendo il proprio indirizzo mac)
 - successivamente, avendo un indirizzo di rete, può richiedere il caricamento del sistema operativo

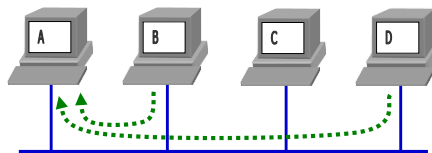
120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

RARP – funzionamento

- l'host invia un messaggio broadcast nel quale chiede l'indirizzo IPv4 corrispondente al proprio indirizzo mac (RARP request)



- rispondono con un RARP reply tutte le macchine (server) che conoscono la corrispondenza



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

ARP e RARP – formato del pacchetto

- i messaggi ARP e RARP vengono spediti da una macchina all'altra incapsulati nel campo dati della trama di livello 2
 - sono imbustati direttamente nel pacchetto mac (ethernet 2.0) e non fanno uso dello strato llc (ieee 802.2)

hardware		protocol
hlen	plen	operation
sender HA (byte 0-3)		
sender HA (byte 4-5)		sender IA (byte 0-1)
sender IA (byte 2-3)		target HA (byte 0-1)
target HA (byte 2-5)		
target IA (byte 0-3)		

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

ARP e RARP – formato del pacchetto

- i campi hardware e protocol specificano il tipo di indirizzo di livello 2 e il tipo di indirizzo di livello 3
- i campi hlen e plen specificano la lunghezza dei due indirizzi (hardware e protocol)
- questi campi permettono di usare ARP e RARP con varie reti fisiche
 - nello standard ieee 802 hlen è 48 bit
 - nella suite TCP/IP plen è 32 bit

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

ARP e RARP – formato del pacchetto

- nel campo operation si specifica se il messaggio è una ARP request o una ARP reply
- i campi sender ia e ha sono rispettivamente l'indirizzo di livello 3 e di livello 2 del mittente
- il campo target ia contiene l'indirizzo di livello 3 della macchina di cui si vuole conoscere l'indirizzo di livello 2 nel caso di un ARP request
- osservazione: dato che nel pacchetto di livello 2 è già contenuto l'indirizzo mac del mittente, il messaggio ARP e quello RARP hanno informazioni ridondanti

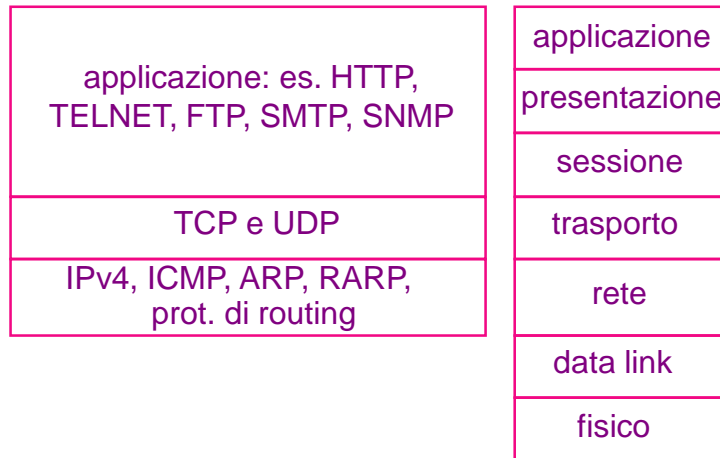
120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

ARP – domande di riepilogo

- come si potrebbe eliminare il protocollo ARP?
 1. si potrebbe adottare a livello 3 (IPv4) lo stesso schema di indirizzamento del livello 2 (mac)
 - la determinazione della località del destinatario e l'IP lookup diventerebbero però operazioni proibitive
 2. si potrebbe adottare a livello 2 (mac) lo stesso schema di indirizzamento del livello 3 (IPv4)
 - solo le macchine IPv4 avrebbero un indirizzo di livello 2
 - non potrebbero esistere altri protocolli di livello 3
 3. si potrebbe ricorrere ad altre strategie di neighbor greeting come l'annuncio periodico
 - il traffico broadcast sarebbe ancora necessario e la dimensione della cache delle coppie IPv4-mac aumenterebbe notevolmente

120-rete-06 copyright ©2015 g.di battista, m.patignani, m. pizzonia

riepilogo sui protocolli di livello tre



120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

IPv6

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

IPv6

- gli indirizzi IPv4 sono in rapido esaurimento
- IPv6 ha uno spazio d'indirizzamento molto più ampio di IPv4
- IPv6 potrebbe rimpiazzare IPv4 nei prossimi anni

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

IPv6 e IPv4

- IPv4 e IPv6 sono tra loro alternativi
 - sono entrambi protocolli di livello 3
- vari meccanismi di transizione sono stati studiati e sono in corso di studio per facilitare il passaggio tra i due protocolli

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

header IPv6

- 40 byte; spariscono gli extension headers

Ver	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit

128 bits Source Address
128 bits Destination Address

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

campi dell'header IPv6

- version – 4 bit
 - 6 – IPv6
- traffic class – 8 bit
 - simile al type of service IPv4

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

campi dell'header IPv6

- flow label – 20 bit
 - per distinguere un flusso
 - pacchetti appartenenti allo stesso flusso hanno:
 - stesso indirizzo IPv6 sorgente, stesso indirizzo IPv6 destinazione, stesso valore del campo flow-label
- payload length – 16 bit
 - specifica la lunghezza dei dati nel pacchetto

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

campi dell'header IPv6

- next header – 8 bit
 - simile a protocol IPv4; consente anche di specificare extension header
- hop limit – 8 bit
 - ttl IPv4
- source address – 16 byte
- destination address – 16 byte

120-rete-06 copyright ©2015 g.di battista, m.patrignani, m. pizzonia

campi dell'header IPv6

- non ci sono più
 - i campi per la frammentazione: in IPv6 i router non possono frammentare i pacchetti
 - checksum: si suppone che i controlli di livello 2 e 4 siano sufficienti
 - hlen: l'header ha sempre 40 byte