



Computer Vision
& Multimedia Lab

Livello di rete

Indirizzi IP

IPv4

IPv6

Internet statistics





Nota per l'utilizzo:

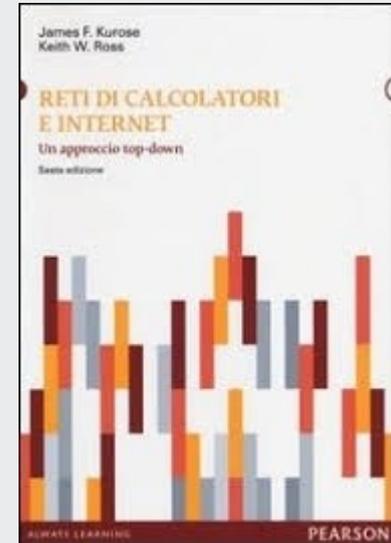
Abbiamo preparato queste slide con l'intenzione di renderle disponibili a tutti (professori, studenti, lettori). Sono in formato PowerPoint in modo che voi possiate aggiungere e cancellare slide (compresa questa) o modificarne il contenuto in base alle vostre esigenze.

Come potete facilmente immaginare, da parte nostra abbiamo fatto *un sacco* di lavoro. In cambio, vi chiediamo solo di rispettare le seguenti condizioni:

- se utilizzate queste slide (ad esempio, in aula) in una forma sostanzialmente inalterata, fate riferimento alla fonte (dopo tutto, ci piacerebbe che la gente usasse il nostro libro!)
- se rendete disponibili queste slide in una forma sostanzialmente inalterata su un sito web, indicate che si tratta di un adattamento (o che sono identiche) delle nostre slide, e inserite la nota relativa al copyright.

Thanks and enjoy! JFK/KWR

All material copyright 1996-2007
J.F Kurose and K.W. Ross, All Rights Reserved



*Reti di calcolatori e Internet:
Un approccio top-down*

6^a edizione
Jim Kurose, Keith Ross

Pearson Paravia Bruno Mondadori Spa
©2013



4.1 Introduzione

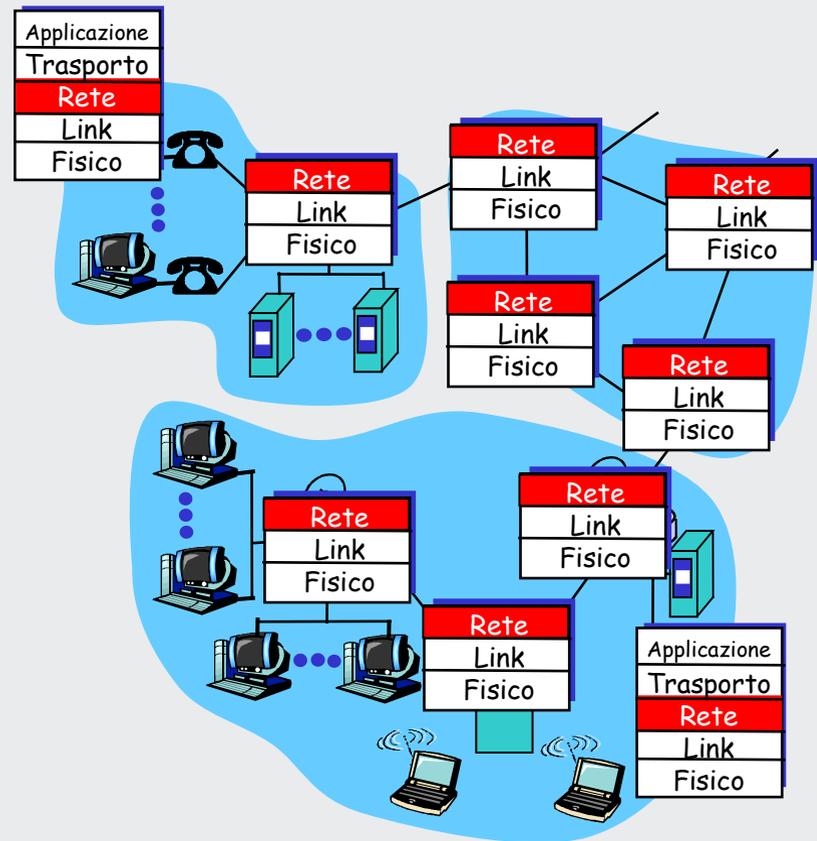
4.2 Reti a circuito virtuale e a datagramma

4.3 Che cosa si trova all'interno di un router?

4.4 Protocollo Internet (IP)

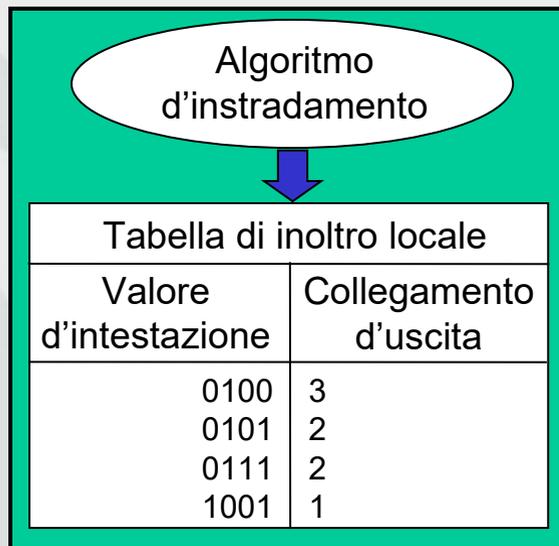
- Formato dei datagrammi
- Indirizzamento IPv4
- ICMP
- IPv6

- Il livello di rete prende i segmenti dal livello di trasporto nell'host mittente
- Sul lato mittente, incapsula i segmenti in datagrammi
- Sul lato destinatario, consegna i segmenti al livello di trasporto
- Protocolli del livello di rete in ogni host, router
- Il router esamina i campi intestazione in tutti i datagrammi IP che lo attraversano

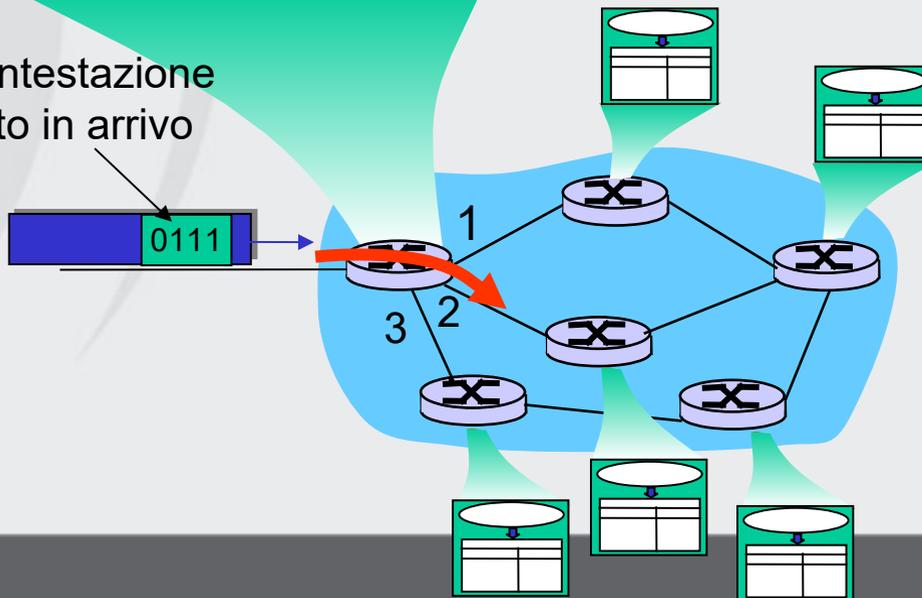




- **Inoltro (forwarding):** trasferisce i pacchetti dall'input di un router all'output del router appropriato
 - **Instradamento (routing):** determina il percorso seguito dai pacchetti dall'origine alla destinazione
 - *Algoritmi d'instradamento*
- Analogia:**
- *instradamento: processo di pianificazione di un viaggio dall'origine alla destinazione*
 - *inoltro: processo di attraversamento di un determinato svincolo*



Valore nell'intestazione del pacchetto in arrivo





4.1 Introduzione

4.2 Reti a circuito virtuale e a datagramma

4.3 Che cosa si trova all'interno di un router?

4.4 Protocollo Internet (IP)

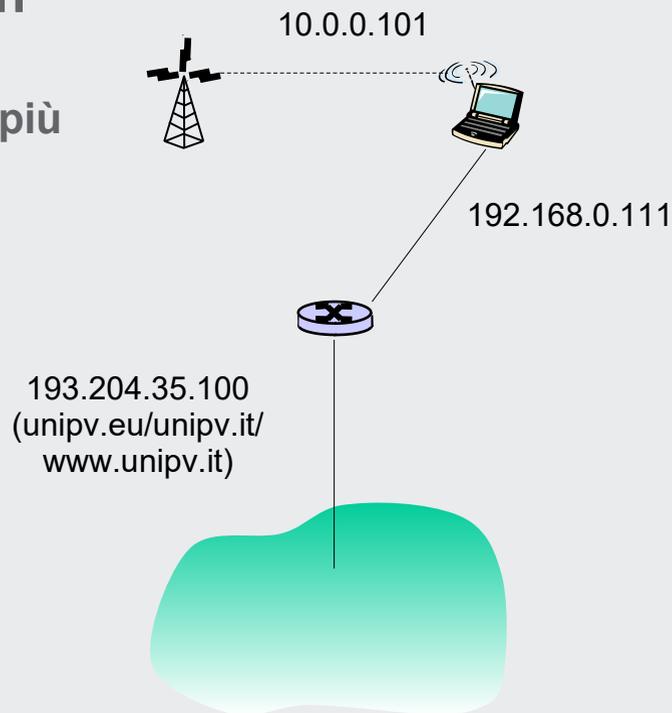
- Formato dei datagrammi
- Indirizzamento IPv4
- ICMP
- IPv6



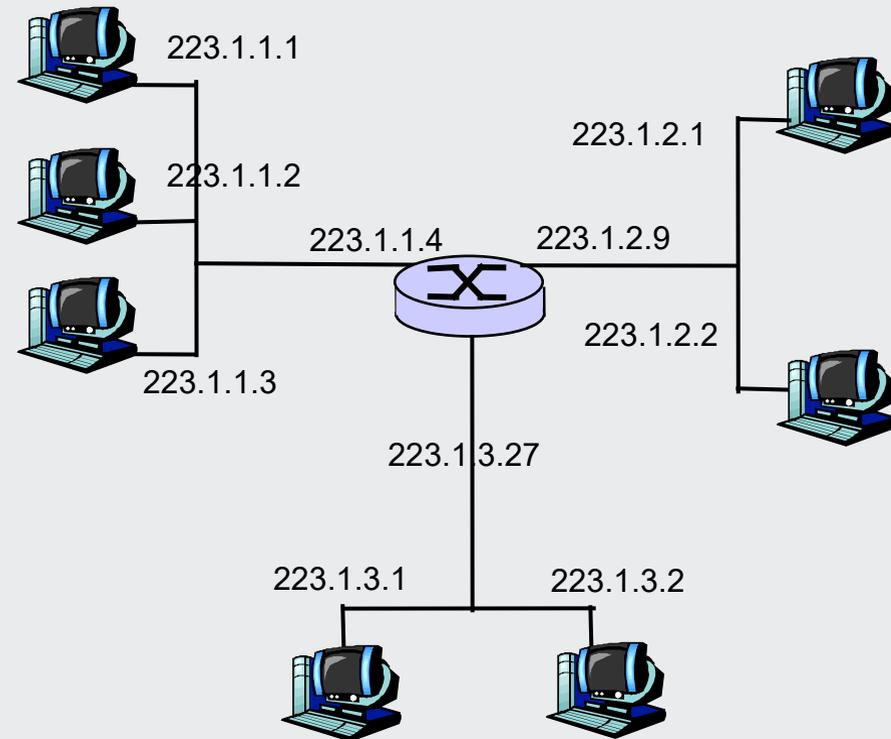
- Ogni dispositivo connesso a internet ha un indirizzo univoco (sia host che router)
 - Il protocollo IPv4 utilizza indirizzi di 32 bit ($\sim 4 \times 10^9$)
 - Normalmente l'indirizzo è rappresentato tramite 4 numeri decimali separati da “.” (dot decimal notation)
$$n_1 \cdot n_2 \cdot n_3 \cdot n_4$$
 - Ognuno di essi corrisponde a 8 bit ($2^8=256$)
$$0 \leq n_i \leq 255$$
 - Non tutti i numeri sono effettivamente utilizzabili



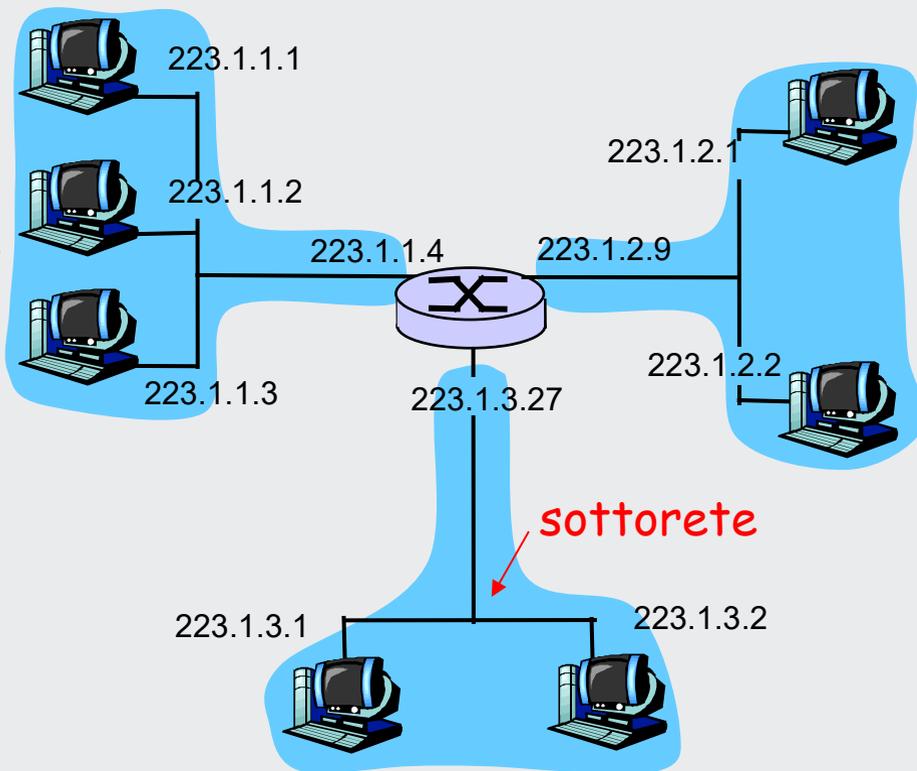
- Ogni interfaccia deve avere un indirizzo univoco
 - NB: ogni dispositivo può averne più di una
 - NB2: i numeri usati sono presi a caso
 - (quasi)



- **Interfaccia:** è il confine tra host e collegamento fisico
 - I router devono necessariamente essere connessi ad almeno due collegamenti

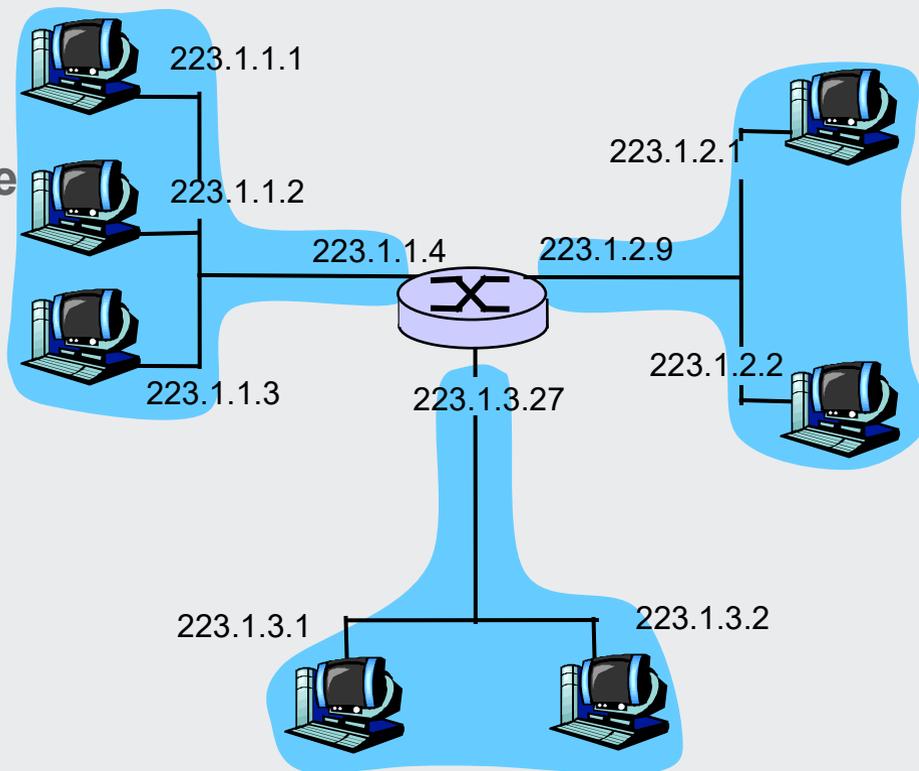


- **Indirizzo IP:**
 - Parte di sottorete (bit alti).
 - Parte dell'host (bit bassi).
- **Cos'è una sottorete?**
 - Interfacce con la stessa parte di sottorete nell'indirizzo IP.
 - Sono interconnesse direttamente fra di loro senza un router.



rete composta da 3 sottoreti

- Come individuare le sottoreti?
- Staccate ogni interfaccia dall'host o router, ogni rete isolata è una sottorete.



rete composta da 3 sottoreti



- **Configurazione manuale:**
 - **Windows:**
control-panel → network → configuration → tcp/ip → properties
 - **UNIX:**
/etc/rc.config
- **DHCP (Dynamic Host Configuration Protocol):**
 - permette a un host di ottenere un indirizzo IP in modo automatico
“plug-and-play”



- Cosa deve fare un amministratore di rete per ottenere un blocco di indirizzi IP?
 - deve contattare il proprio ISP
- Ma come fa un ISP, a sua volta, a ottenere un blocco di indirizzi?
 - **ICANN: Internet Corporation for Assigned Names and Numbers**
 - Ha la responsabilità di allocare i blocchi di indirizzi
 - ICANN gestisce anche i server radice DNS, assegna e risolve dispute sui nomi di dominio



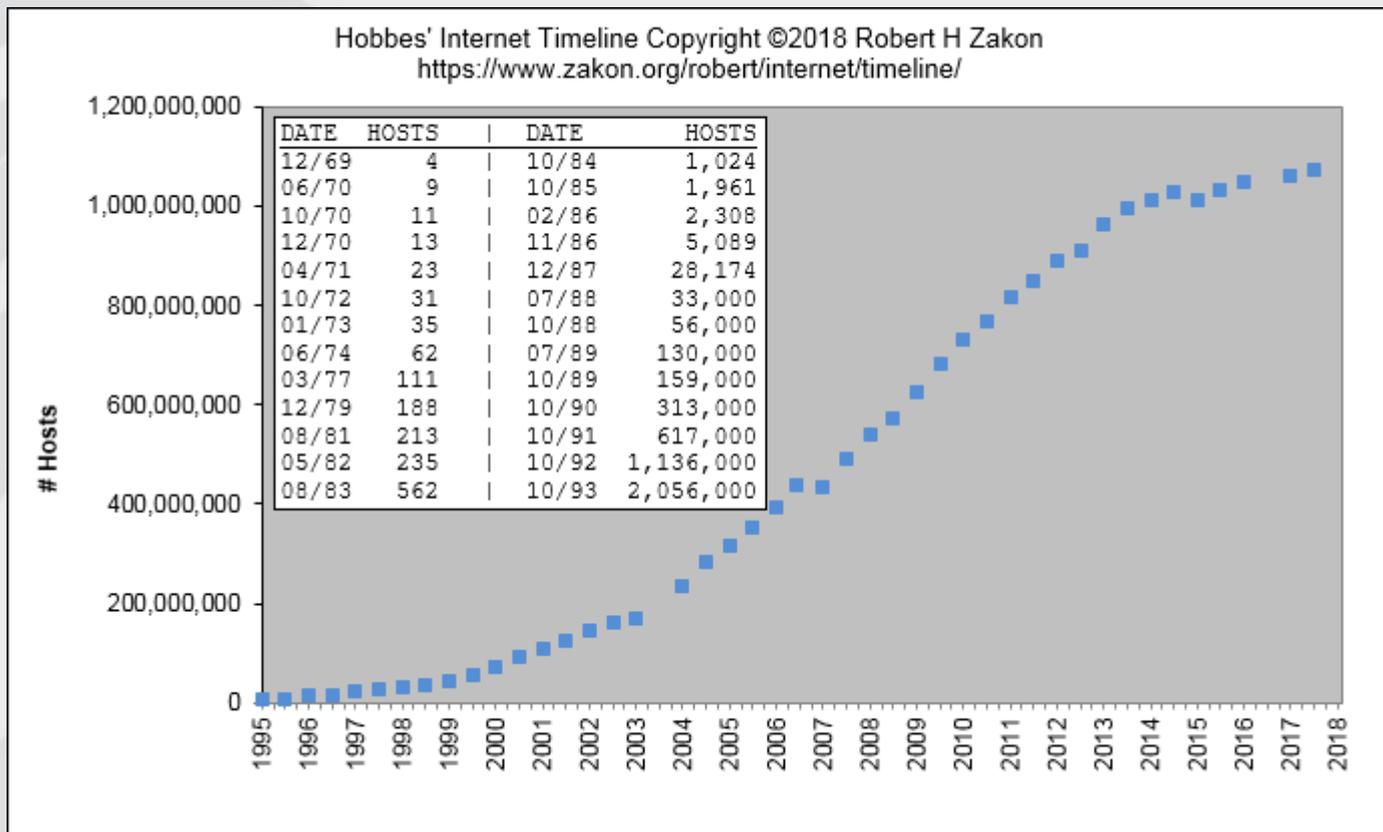
4.1 Introduzione

4.2 Reti a circuito virtuale e a datagramma

4.3 Che cosa si trova all'interno di un router?

4.4 Protocollo Internet (IP)

- Formato dei datagrammi
- Indirizzamento IPv4
- ICMP
- IPv6



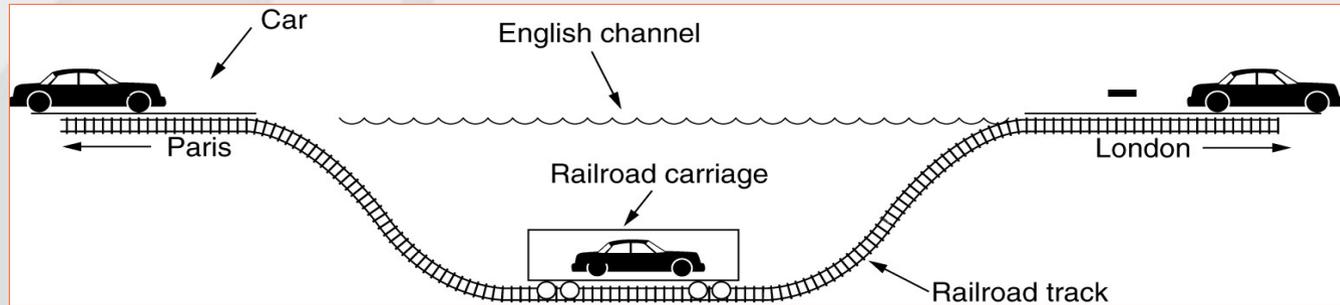


- **Esigenza principale: lo spazio di indirizzamento IP a 32 bit si sta esaurendo**
 - I nuovi indirizzi usano 128 bit ($2^{128} \approx 3 \times 10^{38}$) cioè 16 byte.
 - Superficie terrestre: $5.1 \times 10^8 \text{ Km}^2 \approx 5 \times 10^{20} \text{ mm}^2$
più di 10^{17} indirizzi per mm^2
 - Sono rappresentati da 8 numeri esadecimali di 4 cifre separati da “:”





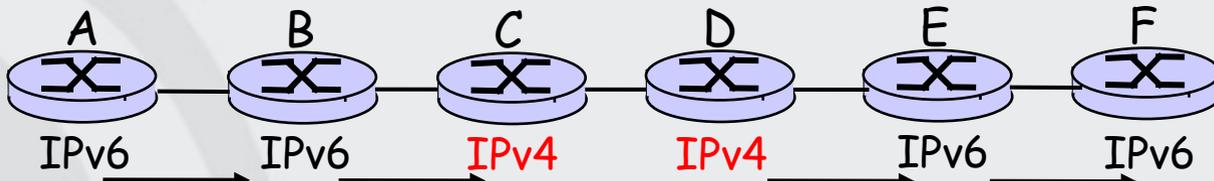
- Non è possibile aggiornare contemporaneamente tutti i router
 - Impossibile dichiarare una “giornata campale” in cui tutte le macchine Internet verranno spente e aggiornate da IPv4 a IPv6
- Come riuscirà la rete a funzionare in presenza di router IPv4 e IPv6?
- **Tunneling**: IPv6 viene trasportato come payload in datagrammi IPv4 quando attraversa router IPv4



Vista logica:



Vista fisica:



Flusso: X
Orig.: A
Dest: F

dati

**Orig.: B
Dest: E**

Flusso: X
Orig.: A
Dest: F

dati

**Orig.: B
Dest: E**

Flusso: X
Orig.: A
Dest: F

dati

Flusso: X
Orig.: A
Dest: F

dati

Da A a B:
IPv6

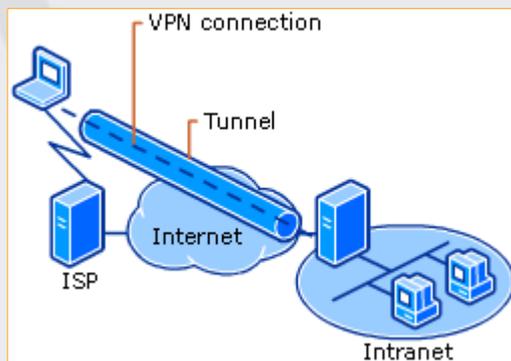
Da B a C:
IPv4 (che
incapsula IPv6)

Da D a E:
IPv4 (che
incapsula IPv6)

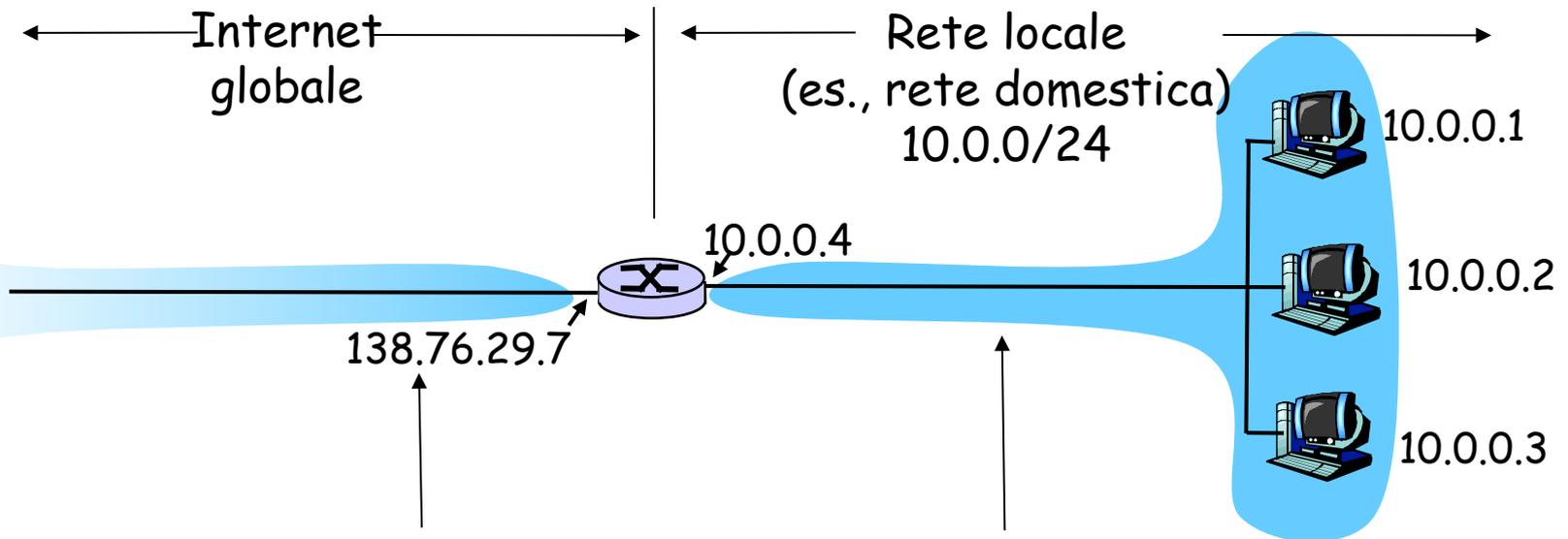
Da E a F:
IPv6



- Le VPN (Virtual Private Network) sono realizzate in maniera simile



Traduzione degli indirizzi di rete (NAT)



I router abilitati alla NAT non appaiono al mondo esterno come router ma come un *unico* dispositivo con un *unico* indirizzo IP. Indirizzo IP origine: 138.76.29.7, e tutto il traffico verso Internet deve riportare lo stesso indirizzo.

Spazio di indirizzi riservato alle reti private, molte delle quali usano un identico spazio, 10.0.0/24 per scambiare pacchetti tra i loro dispositivi

Traduzione degli indirizzi di rete (NAT)

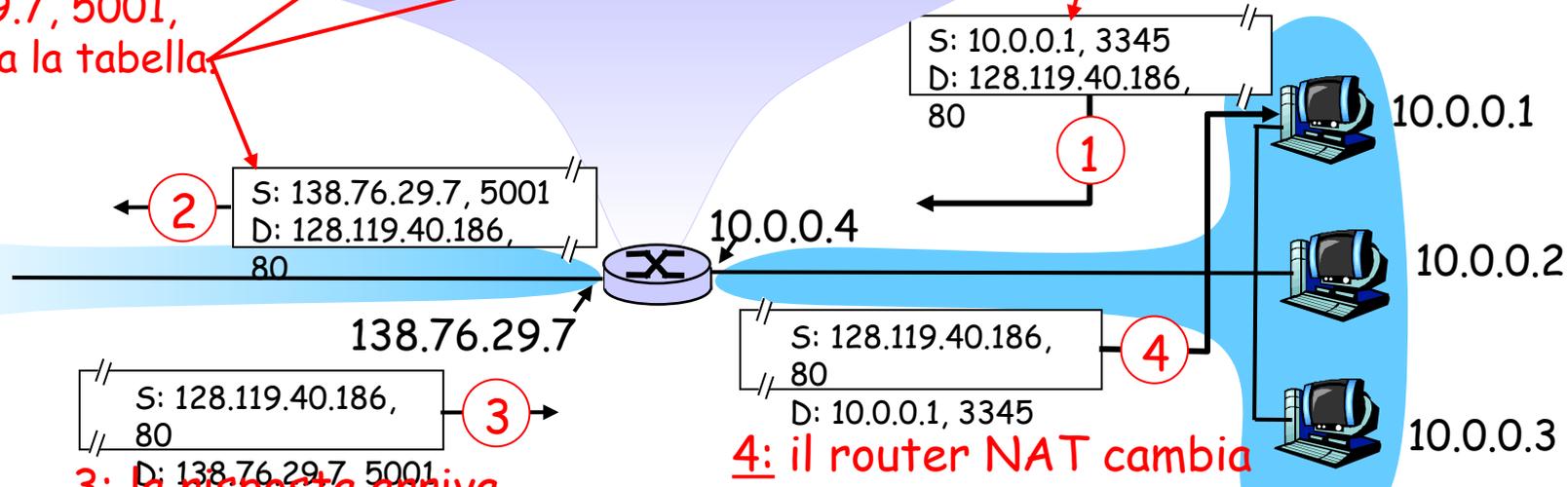
- La rete locale usa solo un indirizzo IP per quanto riguarda il mondo esterno:
 - Non è necessario allocare un intervallo di indirizzi da un ISP: un unico indirizzo IP è sufficiente per tutte le macchine di una rete locale.
 - È possibile cambiare gli indirizzi delle macchine di una rete privata senza doverlo comunicare all'Internet globale.
 - È possibile cambiare ISP senza modificare gli indirizzi delle macchine della rete privata
 - I dispositivi all'interno della rete locale non sono esplicitamente visibili dal mondo esterno (una ulteriore sicurezza)

Traduzione degli indirizzi di rete (NAT)

2: il router NAT cambia l'indirizzo d'origine del datagramma da 10.0.0.1, 3345 a 138.76.29.7, 5001, e aggiorna la tabella

Tabella di traduzione NAT	
Lato WAN	Lato LAN
138.76.29.7, 5001	10.0.0.1, 3345
.....

1: l'host 10.0.0.1 invia il datagramma a 128.119.40.186, 80



3: la risposta arriva all'indirizzo di destinazione: 138.76.29.7, 5001

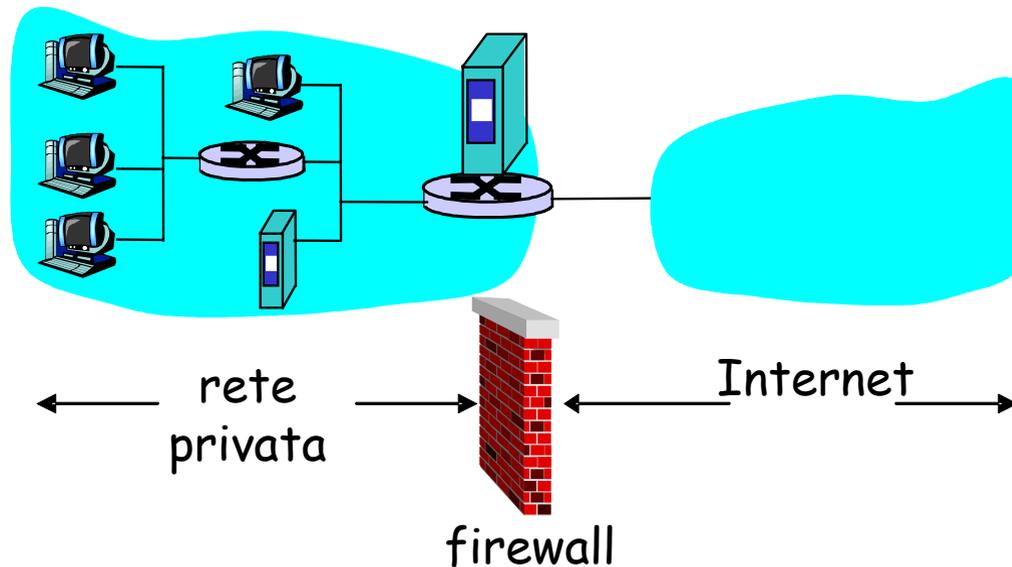
4: il router NAT cambia l'indirizzo di destinazione del datagramma da 138.76.29.7, 5001 a 10.0.0.1, 3345

Traduzione degli indirizzi di rete (NAT)

- Il campo numero di porta è lungo 16 bit:
 - Il protocollo NAT può supportare più di 60.000 connessioni simultanee con un solo indirizzo IP sul lato WAN.
- NAT è contestato perché:
 - i router dovrebbero elaborare i pacchetti solo fino al livello 3.
 - Viola il cosiddetto *argomento punto-punto*
 - Interferenza con le applicazioni P2P, a meno che non sia specificamente configurato per quella specifica applicazione P2P.
 - Per risolvere la scarsità di indirizzi IP si dovrebbe usare IPv6.

Firewall

Struttura hardware e software che separa una rete privata dal resto di Internet e consente all'amministratore di controllare e gestire il flusso di traffico tra il mondo esterno e le risorse interne.



Firewall: perché

Prevenire attacchi di negazione del servizio:

- SYN flooding: l'intruso stabilisce molte connessioni TCP fasulle per non lasciare risorse alle connessioni "vere".

Prevenire modifiche/accessi illegali ai dati interni.

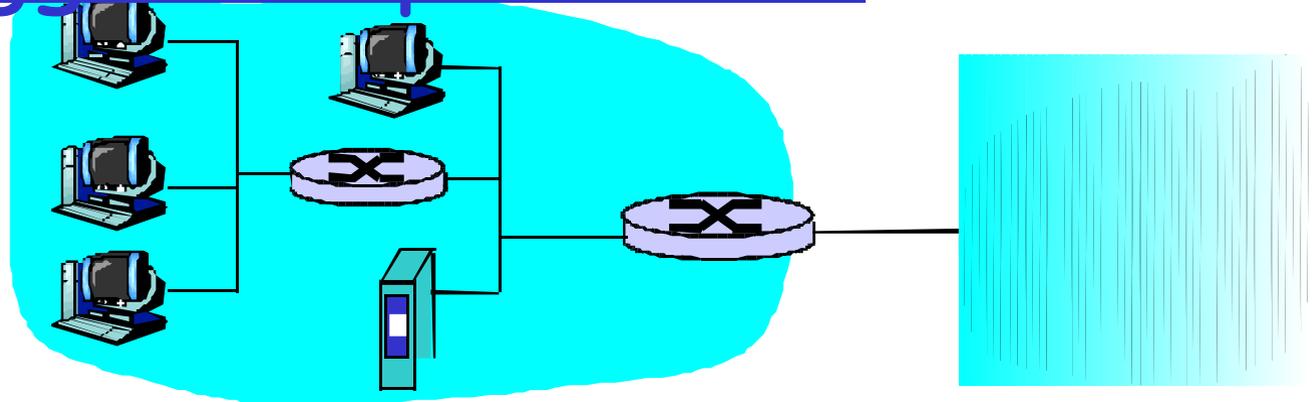
- es., l'intruso può sostituire l'homepage del MIUR con qualcos'altro.

Consentire solo accessi autorizzati all'interno della rete (una serie di utenti/host autenticati)

Tre tipi di firewall:

- A livello di applicazione (gateway)
- A filtraggio dei pacchetti
- Filtri con memoria dello stato

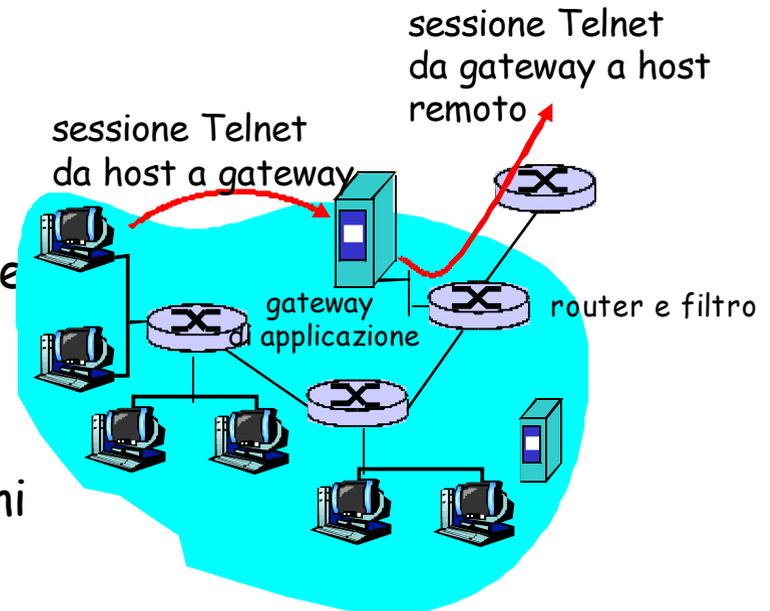
Filtraggio dei pacchetti



- Una rete privata è collegata a Internet mediante un router
- Il router è responsabile del filtraggio dei pacchetti e determina quali pacchetti devono essere bloccati o quali possono passare in base a:
 - Indirizzo IP sorgente o destinazione
 - Porte sorgente e destinazione TCP o UDP
 - Tipo di messaggio ICMP
 - Bit TCP SYN o ACK

Gateway

- Il filtraggio dei pacchetti consente di effettuare un controllo sulle intestazioni IP e TCP/UDP.
- Esempio: permette ai clienti interni (autorizzati) le connessioni Telnet ma impedisce il contrario.



1. Tutte le connessioni Telnet verso l'esterno devono passare attraverso il gateway.
2. Il gateway non solo concede l'autorizzazione all'utente ma smista anche le informazioni fra l'utente e l'host.
3. La configurazione del filtro del router blocca tutti i collegamenti eccetto quelli che riportano l'indirizzo IP del gateway.

Limiti di firewall e gateway

- ❑ IP spoofing: non si può sapere se i dati arrivano **realmente** dalla sorgente dichiarata.
- ❑ Se più applicazioni necessitano di un trattamento speciale, ciascuna avrà il suo gateway di applicazione.
- ❑ Il software del client deve sapere come contattare il gateway.
 - Es. deve impostare l'indirizzo IP del proxy nel browser Web.
- ❑ Spesso sono configurati secondo una politica "intransigente" senza vie di mezzo, per esempio inibendo tutto il traffico UDP.
- ❑ Compromesso: **grado di comunicazione con il mondo esterno/livello di sicurezza**
- ❑ Numerosi siti con protezioni elevate sono ancora soggetti ad attacchi.