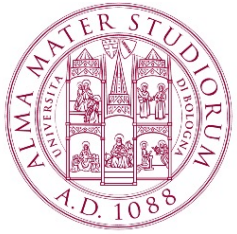


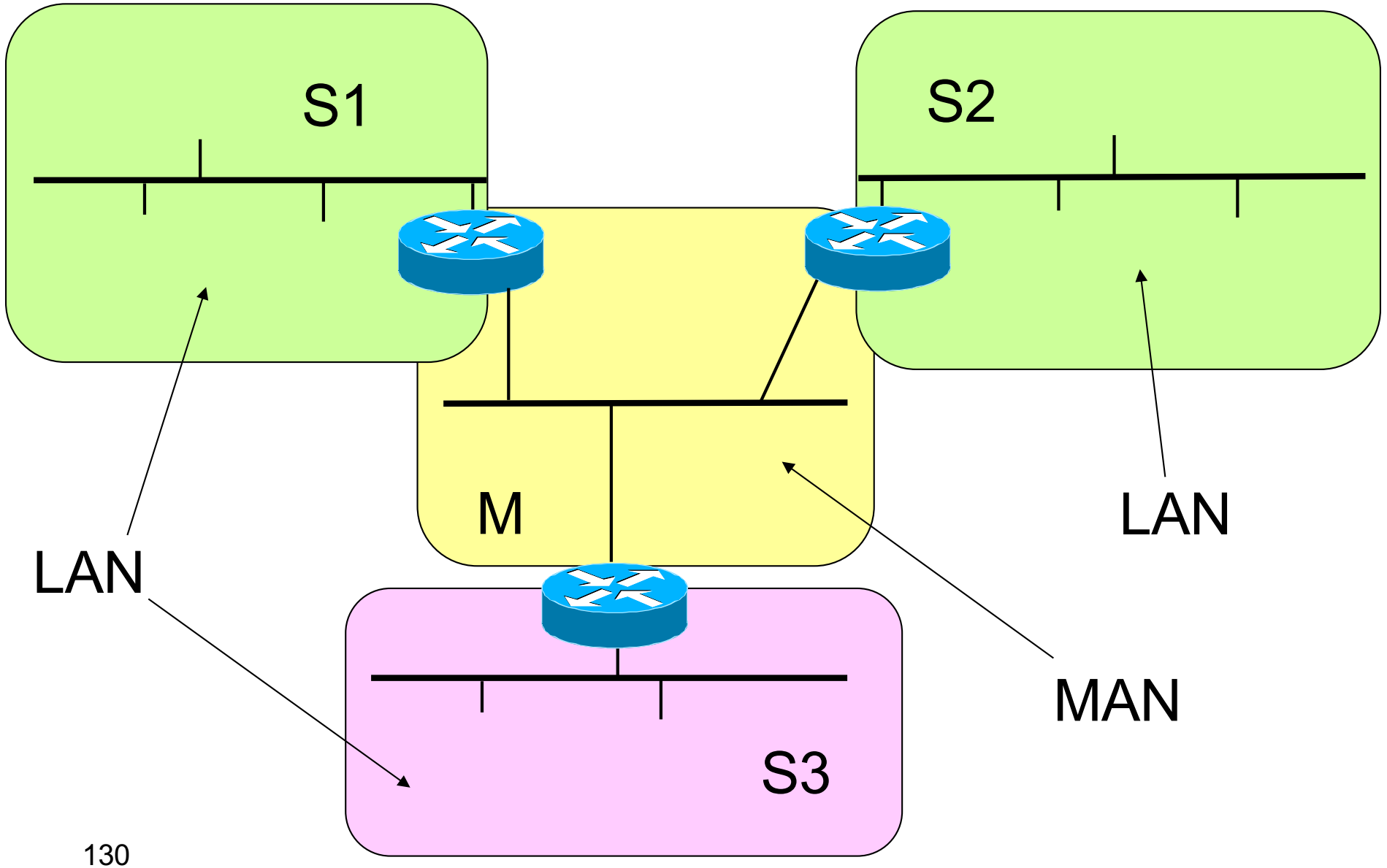
ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Pianificare la numerazione di reti IP

Esempio

- Un’azienda possiede tre siti distribuiti su una grande area urbana: S1, S2, S3.
- Ciascun sito aziendale è dotato di infrastrutture informatiche comprendenti, tra l'altro, una LAN ed un router di uscita verso il mondo esterno. Tutti i siti devono essere interconnessi tra loro con una rete a maglia completa.
- I siti sono così divisi:
  - S1, S2: 50 host
  - S3: 20 host
- Si richiede di progettare una rete di classe C a cui viene assegnato l’indirizzo 196.200.96.0/24 comprensiva della numerazione dei router, definendo le relative netmask

Architettura



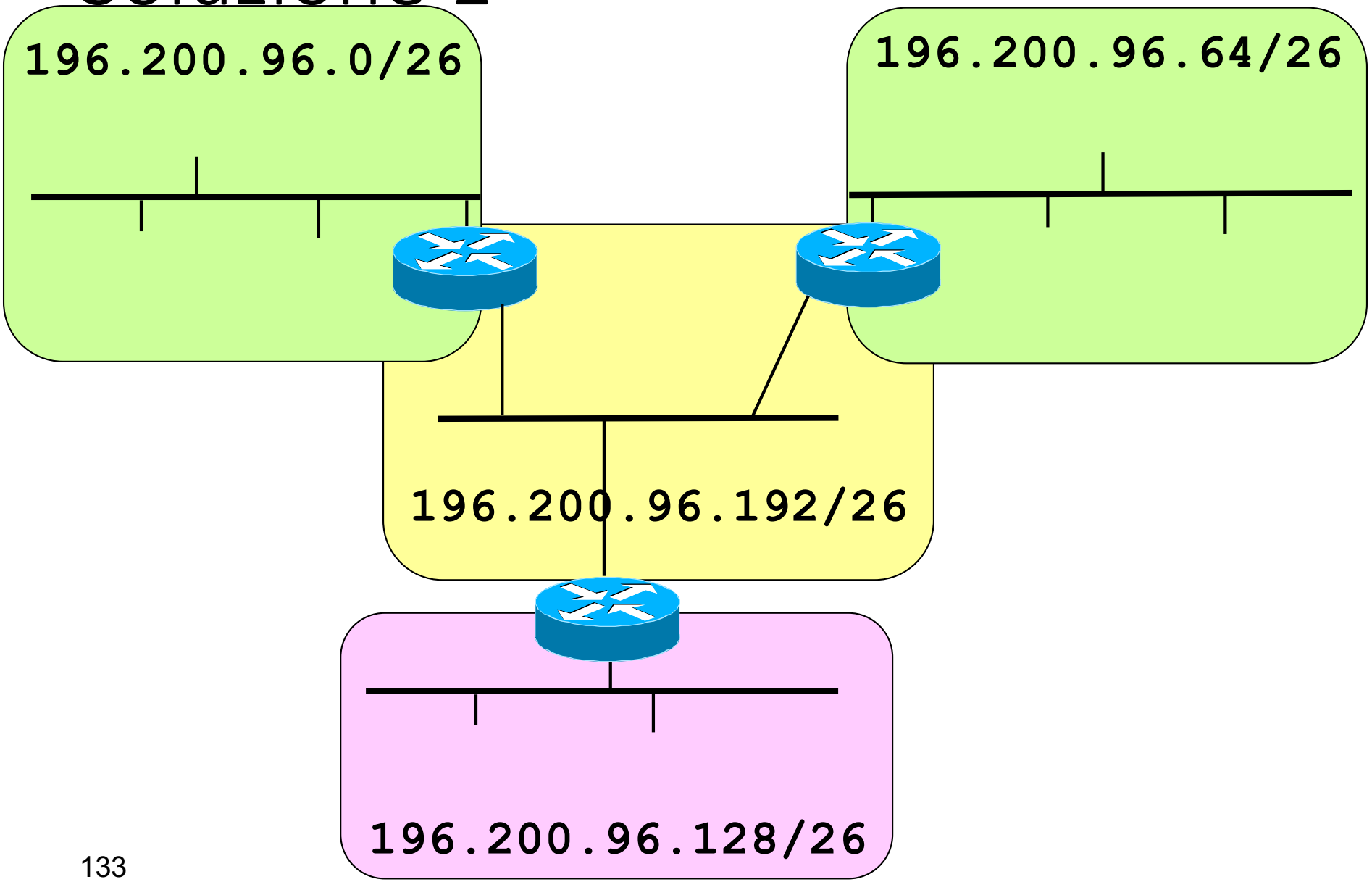
La scelta della netmask

Ultimo byte netmask	# host	# subnets
00000000	254	1
10000000	126	2
11000000	62	4
11100000	30	8
11110000	14	16
11111000	6	32
11111100	2	64

Soluzione 1

- Subnets:
  - **196.200.96.0/26** **(S1)**
  - **196.200.96.64/26** **(S2)**
  - **196.200.96.128/26** **(S3)**
  - **196.200.96.192/26** **(M)**
- Netmask: **255.255.255.192**
- Broadcast:
  - **196.200.96.63** **(S1)**
  - **196.200.96.127** **(S2)**
  - **196.200.96.191** **(S3)**
  - **196.200.96.255** **(M)**

Soluzione 1



Soluzione 1

- Routers LAN: **196.200.96.62 (S1)**
  196.200.96.126 (S2)
  196.200.96.190 (S3)

- Routers MAN: qualunque indirizzo tra:
  196.200.96.193 e **.254 (M)**

- IP Hosts: qualunque indirizzo tra:
  196.200.96.1 e **.61 (S1)**
  196.200.96.65 e **.125 (S2)**
  196.200.96.129 e **.189 (S3)**

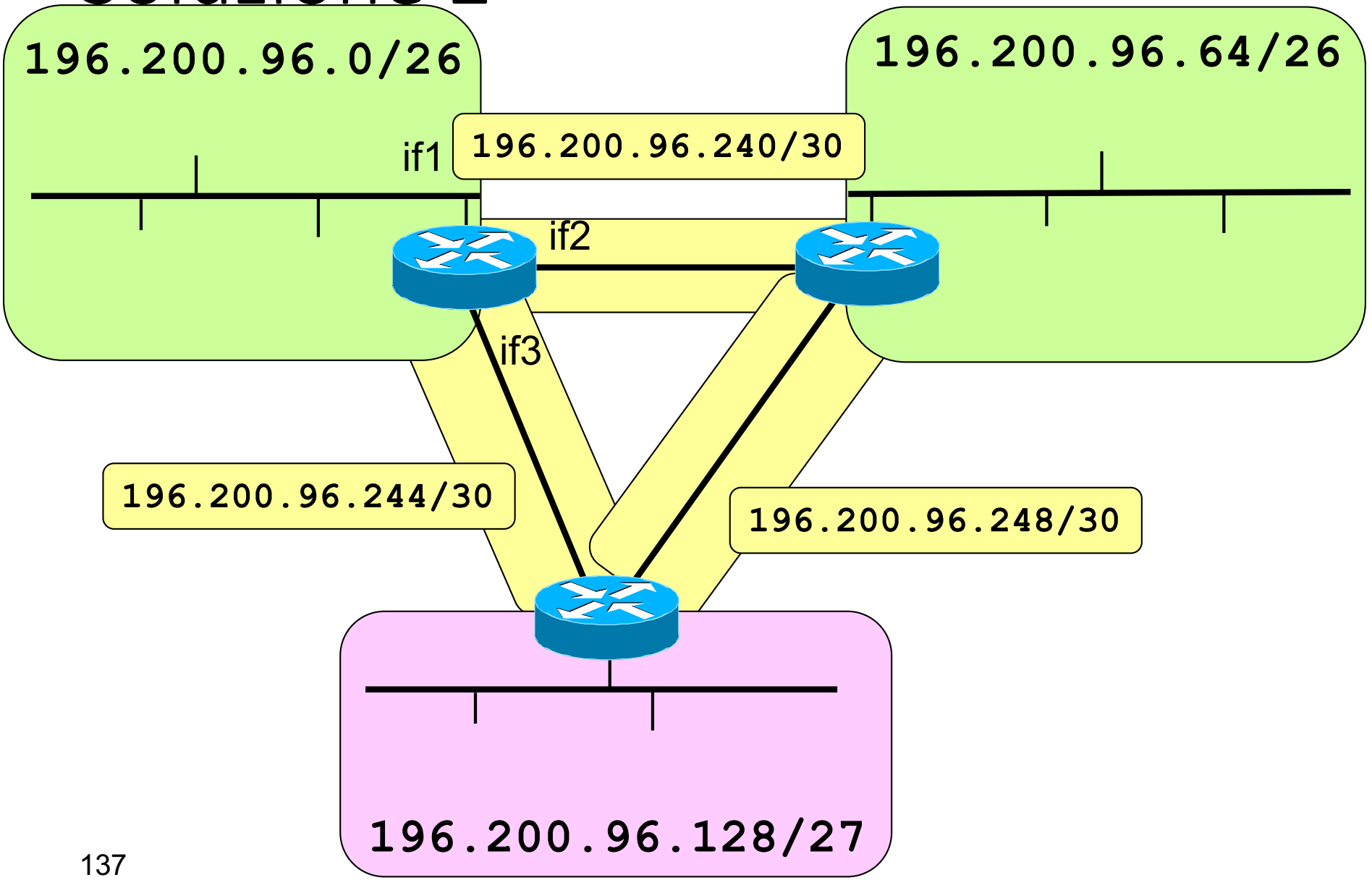
Scelta di netmask diverse

Ultimo byte netmask	# host	# subnets
00000000	254	1
10000000	126	2
11000000	62	4
11100000	30	8
11110000	14	16
11111000	6	32
11111100	2	64

Soluzione 2

Subnet	# host	Indirizzi	Broadcast
196.200.96.0/26	62	1 – 62	63
196.200.96.64/26	62	65 – 126	127
196.200.96.128/27	30	129 – 158	159
196.200.96.160/27	30	161 – 190	191
196.200.96.192/27	30	193 – 222	223
196.200.96.224/28	14	225 – 238	239
196.200.96.240/30	2	241 – 242	243
196.200.96.244/30	2	245 – 246	247
196.200.96.248/30	2	249 – 250	251
196.200.96.252/30	2	253 – 254	255

Soluzione 2


196.200.96.0/26
196.200.96.64/26
196.200.96.240/30
if1
if2
if3
196.200.96.244/30
196.200.96.248/30
196.200.96.128/27

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Il protocollo ICMP

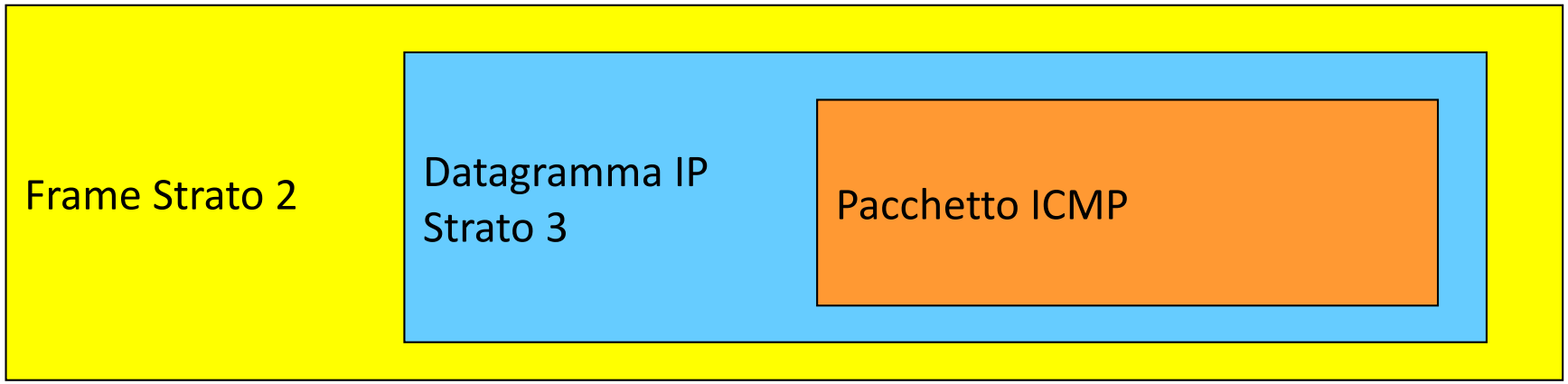
Il protocollo IP…

- offre un servizio di tipo best effort
  - non garantisce la corretta consegna dei datagrammi
  - se necessario si affida a protocolli affidabili di livello superiore (TCP)
- è comunque necessario un protocollo di controllo
  - gestione di situazioni anomale
  - notifica di errori o di irraggiungibilità della destinazione
  - scambio di informazioni sulla rete

  → **ICMP (Internet Control Message Protocol)**
  - ICMP segnala solamente errori e malfunzionamenti, ma non esegue alcuna correzione
  - ICMP **non rende affidabile** IP

ICMP

- **Internet Control Message Protocol** (RFC 792) svolge funzioni di controllo per IP
  - IP usa ICMP per la gestione di situazioni anomale, per cui ICMP offre un servizio ad IP
  - i pacchetti ICMP sono incapsulati in datagrammi IP, per cui ICMP è anche utente IP



Pacchetto ICMP

IP header	20 - 60 byte
Message Type	1 byte
Message Code	1 byte
Checksum	2 byte
Additional Fields (optional)	variabile
Data	variabile

- **Type** definisce il tipo di messaggio ICMP
  - messaggi di errore
  - messaggi di richiesta di informazioni
- **Code** descrive il tipo di errore e ulteriori dettagli
- **Checksum** controlla i bit errati nel messaggio ICMP
- **Add. Fields** dipendono dal tipo di messaggio ICMP
- **Data** intestazione e parte dei dati del datagramma che ha generato l'errore

Tipi di errori

- **Destination Unreachable** (Type = 3)
  - Generato da un gateway quando la sottorete o l'host non sono raggiungibili
  - Generato da un host quando si presenta un errore sull'indirizzo dell'entità di livello superiore a cui trasferire il datagramma
- Codici errore di Destination Unreachable
  - 0 = sottorete non raggiungibile
  - 1 = host non raggiungibile
  - 2 = protocollo non disponibile
  - 3 = porta non disponibile
  - 4 = frammentazione necessaria ma bit don't fragment settato

Tipi di errori

- Time Exceeded (Type = 11)
  - generato da un router quando il Time-to-Live di un datagramma si azzera ed il datagramma viene distrutto (Code = 0)
  - generato da un host quando un timer si azzera in attesa dei frammenti per riassemblare un datagramma ricevuto in parte (Code = 1)
- Source Quench (Type = 4)
  - i datagrammi arrivano troppo velocemente rispetto alla capacità di essere processati: l'host sorgente deve ridurre la velocità di trasmissione (obsoleto)
- Redirect (Type = 5)
  - generato da un router per indicare all'host sorgente un'altra strada più conveniente per raggiungere l'host destinazione

Informazioni

- Echo (Type = 8)
- Echo Reply (Type = 0)
  - l'host sorgente invia la richiesta ad un altro host o ad un gateway
  - la destinazione deve rispondere immediatamente
  - metodo usato per determinare lo stato di una rete e dei suoi host, la loro raggiungibilità e il tempo di transito nella rete
- Additional Fields:
  - Identifier: identifica l'insieme degli echo appartenenti allo stesso test
  - Sequence Number: identifica ciascun echo nell'insieme
  - Optional Data: usato per inserire eventuali dati di verifica

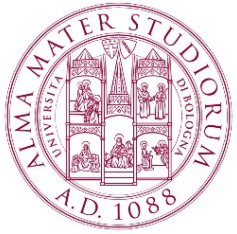
Informazioni

- Timestamp Request (Type = 13)
- Timestamp Reply (Type = 14)
  - l'host sorgente invia all'host destinazione un Originate Timestamp che indica l'istante in cui la richiesta è partita
  - l'host destinazione risponde inviando un
    - Receive Timestamp che indica l'istante in cui la richiesta è stata ricevuta
    - Transmit Timestamp che indica l'istante in cui la risposta è stata inviata
  - serve per valutare il tempo di transito nella rete, al netto del tempo di processamento = $T_{Transmit} - T_{Receive}$

Informazioni

- Address Mask Request (Type = 17)
- Address Mask Reply (Type = 18)
  inviato dall'host sorgente all'indirizzo di broadcast (255.255.255.255) per ottenere la subnet mask da usare dopo aver ottenuto il proprio indirizzo IP tramite RARP o BOOTP

- Router Solicitation (Type = 10)
- Router Advertisement (Type = 9)
  utilizzato per localizzare i router connessi alla rete



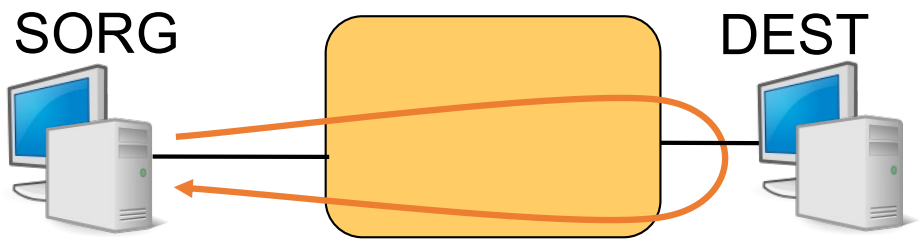
ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Applicazioni di ICMP

Comando PING

`ping DEST`

Permette di controllare se l'host DEST è raggiungibile o meno da SORG



- SORG invia a DEST un pacchetto **ICMP** di tipo **"echo"**
- Se l'host DEST è raggiungibile da SORG, DEST risponde inviando indietro un pacchetto ICMP di tipo **"echo reply"**

Opzioni

- **`-n N`** permette di specificare quanti pacchetti inviare (un pacchetto al secondo)
- **`-l M`** specifica la dimensione in byte di ciascun pacchetto
- **`-t`** esegue **`ping`** finché interrotto con **`Ctrl-C`**
- **`-a`** traduce l'indirizzo IP in nome DNS
- **`-f`** setta il bit *don't fragment* a 1
- **`-i T`** setta *time-to-live* = **`T`**
- **`-w` T_{out}** specifica un timeout in millisecondi

- Per maggiori informazioni consultare l'help: **`ping /?`**

Comando PING – Output

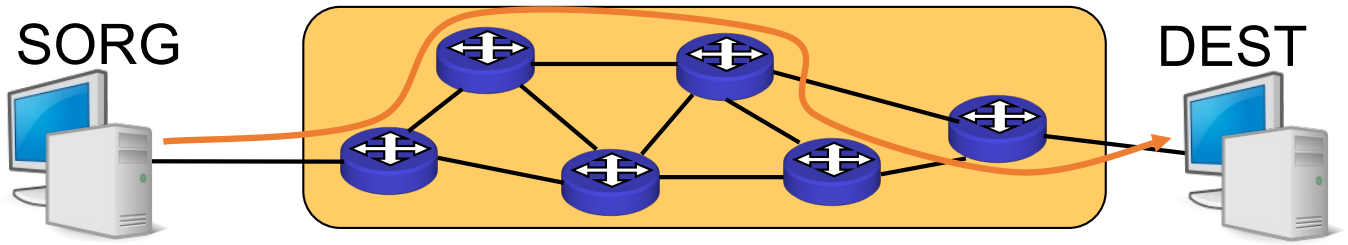
L'output mostra

- la dimensione del pacchetto "echo reply"
- l'indirizzo IP di DEST
- il numero di sequenza della risposta (solo UNIX-LINUX)
- il "time-to-live" (TTL)
- il "round-trip time" (RTT)
- alcuni risultati statistici: N° pacchetti persi, MIN, MAX e media del RTT

Comando TRACEROUTE

`tracert DEST`

Permette di conoscere il percorso seguito dai pacchetti inviati da SORG e diretti verso DEST



- SORG invia a DEST una serie di pacchetti **ICMP** di tipo **ECHO** con un **TIME-TO-LIVE (TTL)** progressivo da **1** a **30** (per default)
- Ciascun nodo intermedio decrementa **TTL**
- Il nodo che rileva **TTL = 0** invia a SORG un pacchetto **ICMP** di tipo **TIME EXCEEDED**
- SORG costruisce una lista dei nodi attraversati fino a DEST
- L'output mostra il **TTL**, il nome **DNS** e l'indirizzo **IP** dei nodi intermedi ed il **ROUND-TRIP TIME (RTT)**

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Gestione della numerazione

Dispositivi di rete

- DHCP
  - Permette ad un Host di ottenere una configurazione IP
- Packet Filter
  - Permette/blocca l'invio di pacchetti da/verso determinati indirizzi
  - Protegge la rete dal traffico "vagante"
- Application Layer Gateway (ALG) / Proxy
  - Controlla la comunicazione a livello applicativo
- Firewall
  - Combinazione dei dispositivi descritti sopra
  - Protegge le risorse interne da accessi esterni
- Network Address Translator (NAT)
  - Riduce la richiesta dello spazio di indirizzamento Internet
  - Nasconde gli indirizzi IP interni
  - Esegue un packet filtering per il traffico sconosciuto

DHCP – RFC 2131,2132

Dynamic Host Configuration Protocol

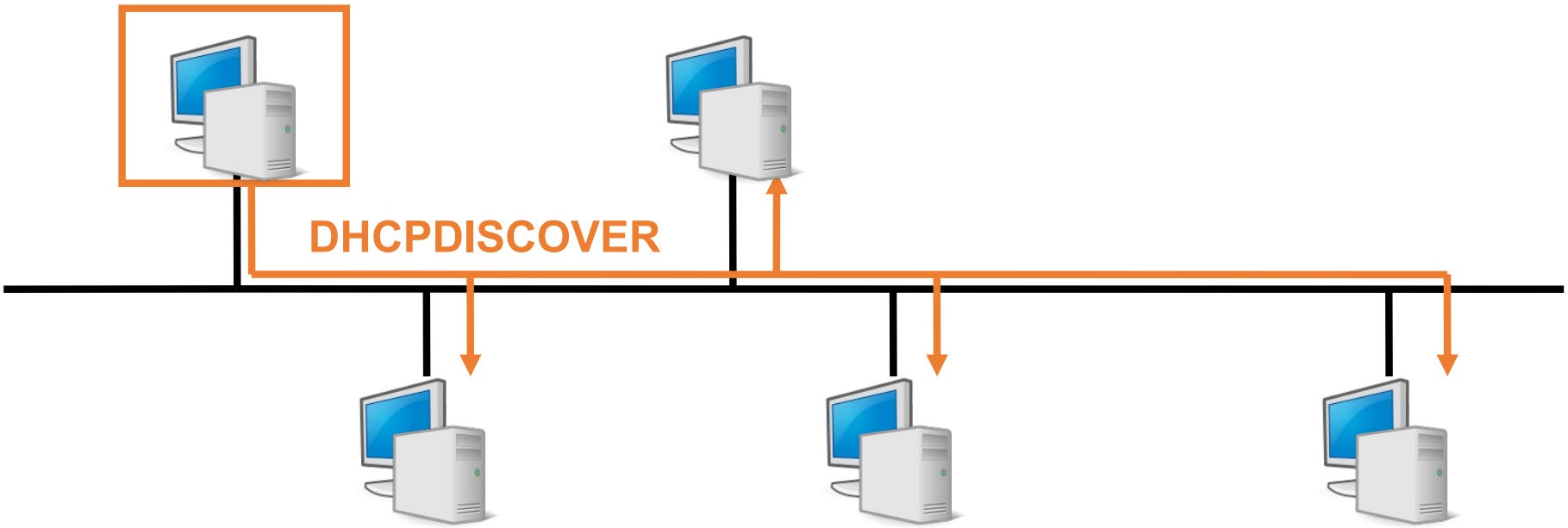
Configurazione **automatica** e **dinamica** di

- Indirizzo IP
- Netmask
- Broadcast
- Host name
- Default gateway
- Server DNS

Server su porta **67** UDP

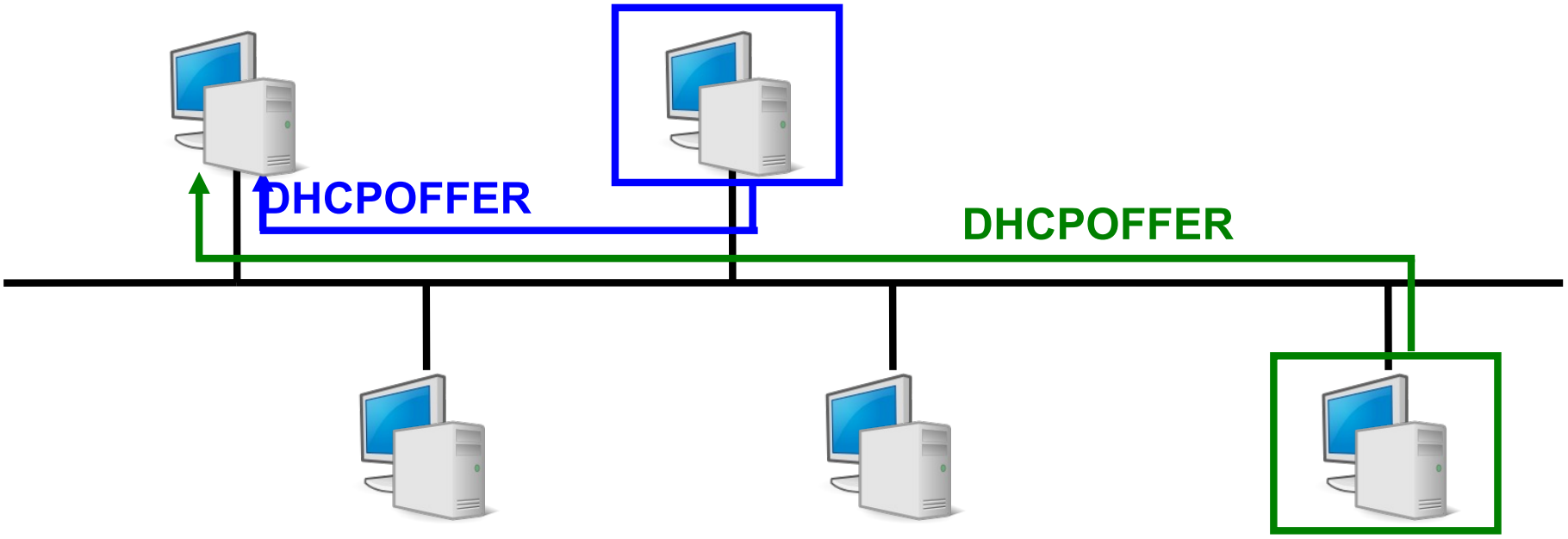
DHCP – 1

- Quando un host attiva l'interfaccia di rete, invia in modalità broadcast un messaggio **DHCPDISCOVER** in cerca di un server DHCP



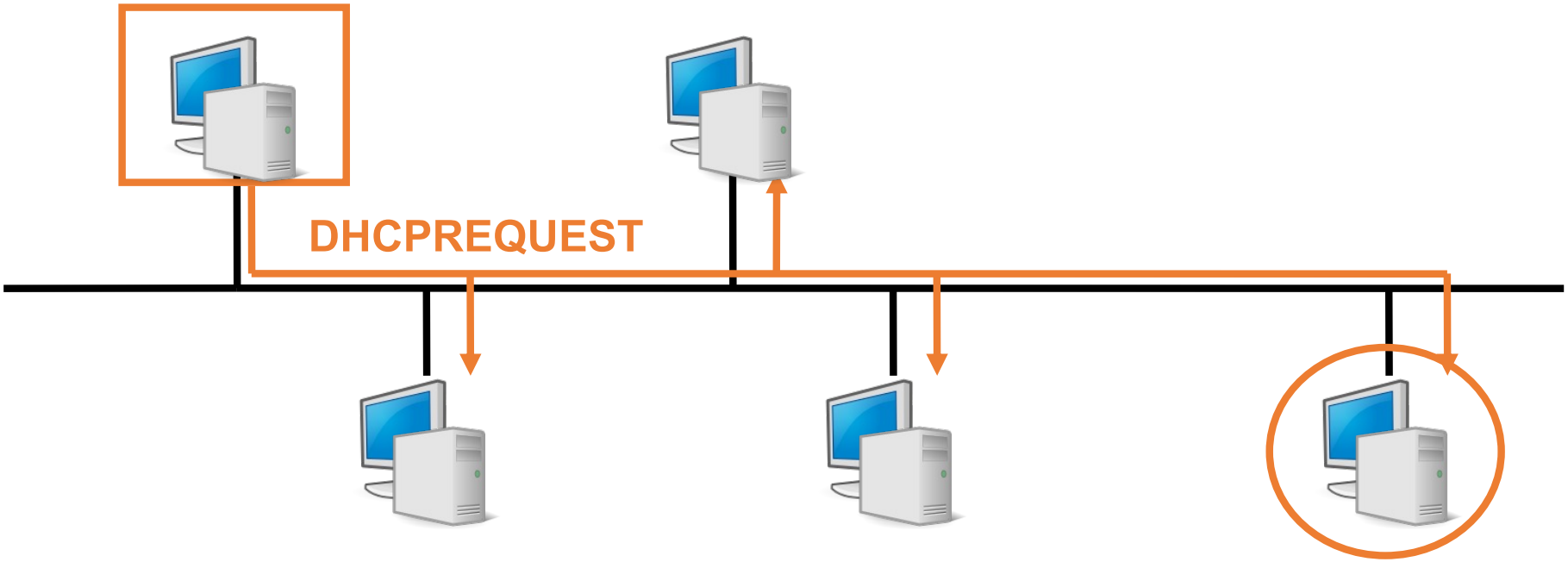
DHCP – 2

- Ciascun server DHCP presente risponde all'host con un messaggio **DHCPOFFER** con cui propone un indirizzo IP



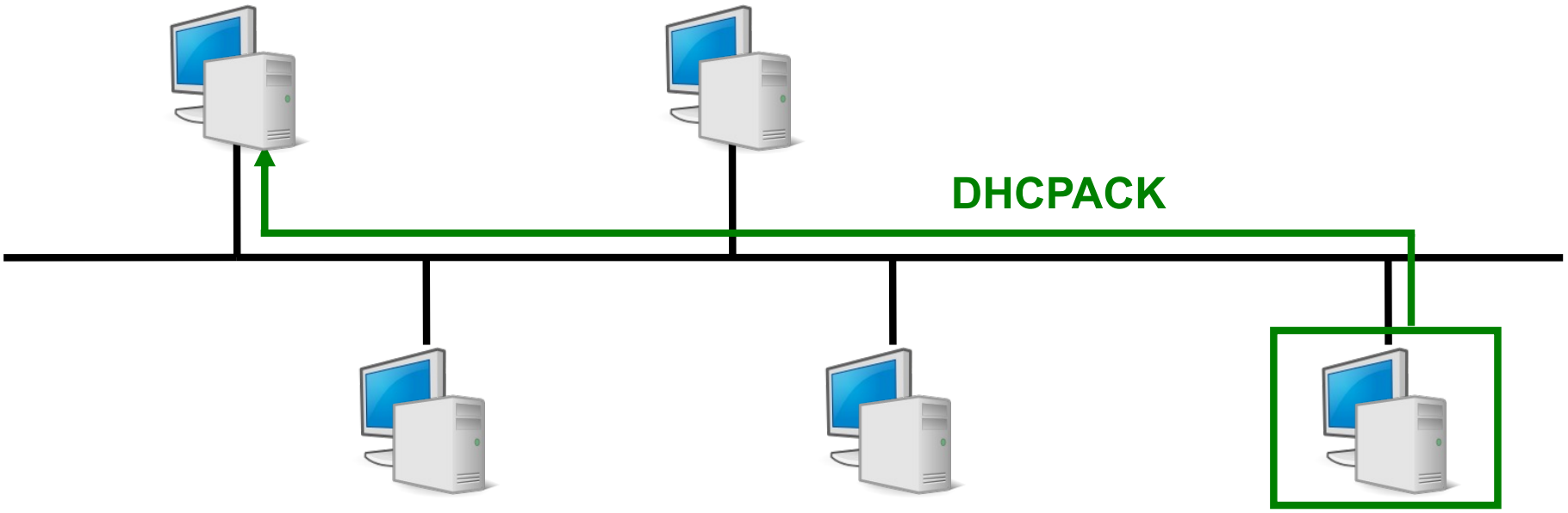
DHCP – 3

- L'host accetta una delle offerte proposte dai server e manda un messaggio **DHCPREQUEST** in cui richiede la configurazione, specificando il server



DHCP – 4

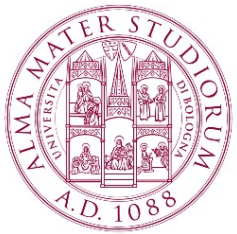
- Il server DHCP risponde all'host con un messaggio **DHCPACK** specificando i parametri di configurazione



Ulteriori dettagli

- Un'analisi dettagliata del protocollo DHCP che include:
  - Esempi operativi
  - Catture di traffico
- Si può trovare alla seguente pagina web

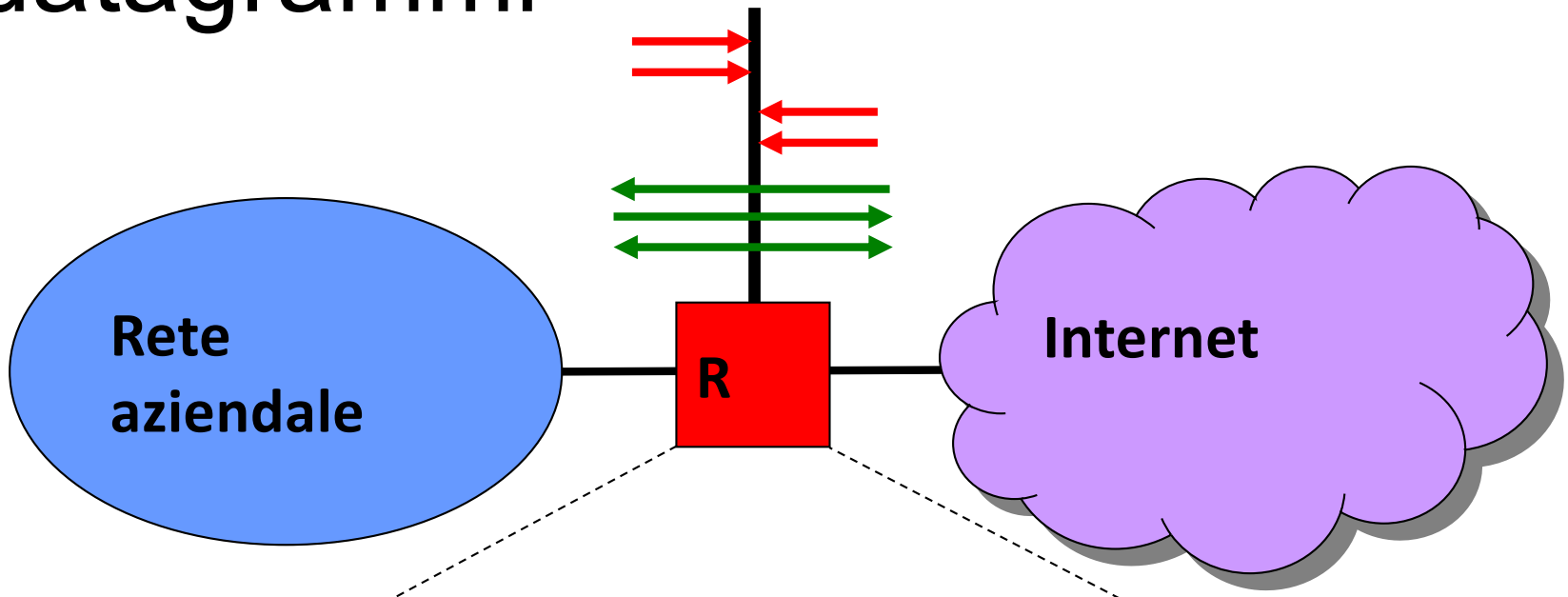
  http://deisnet.deis.unibo.it/DHCP



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Packet Filter e Firewall

Metodologie di filtraggio dei datagrammi

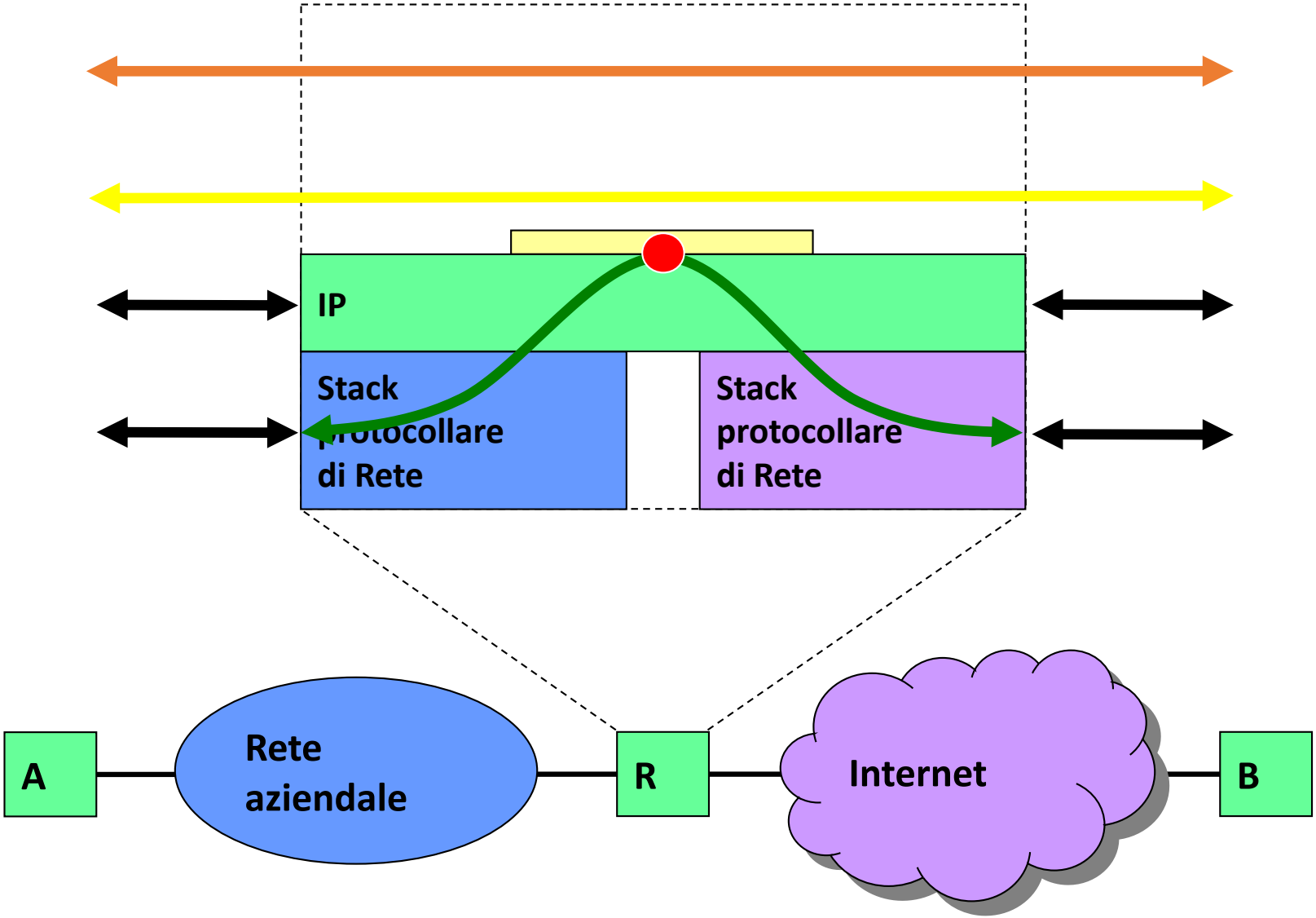


Impostazioni del Packet Filter

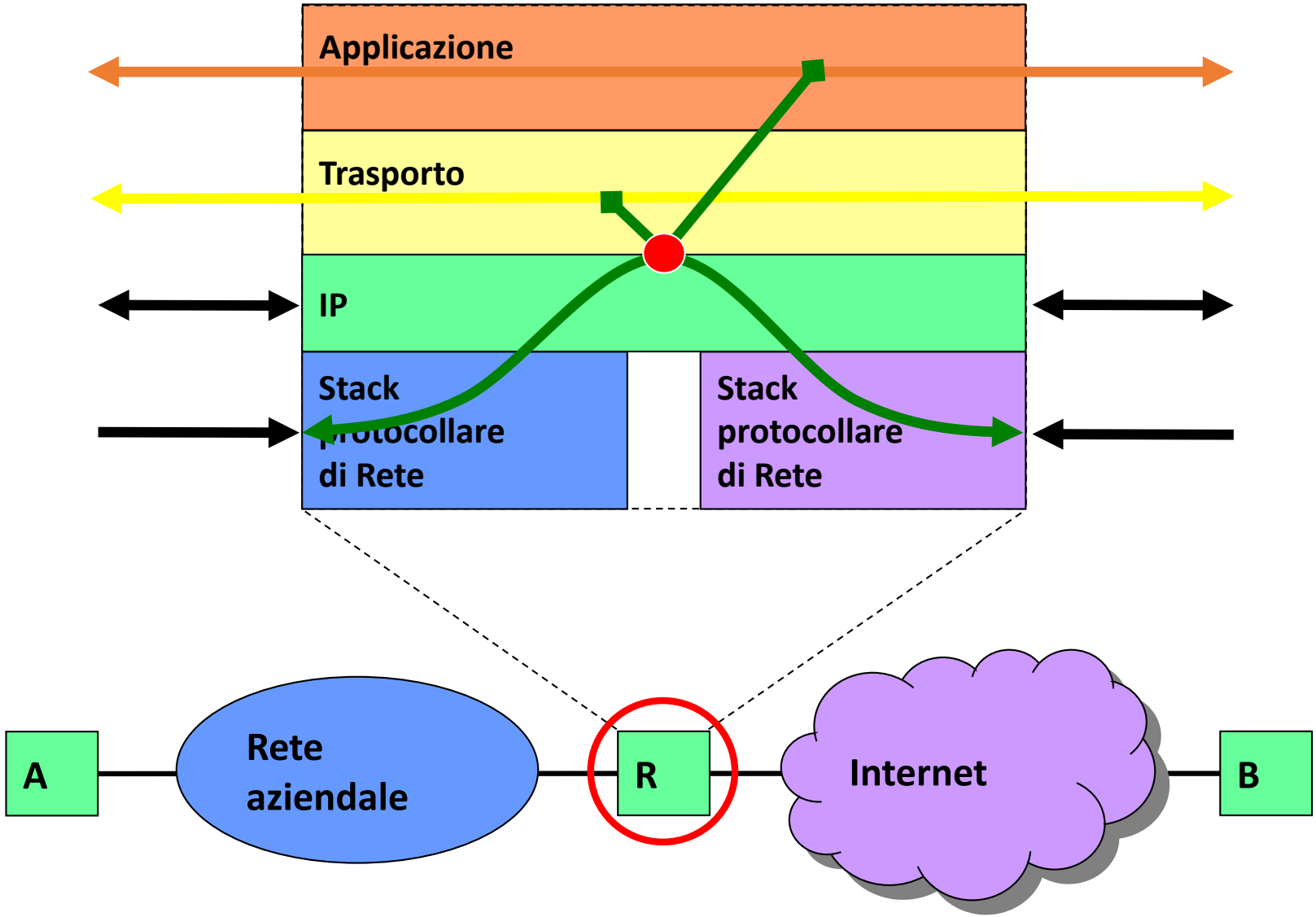
- **Indirizzo IP sorgente e destinazione**
- **Protocollo (TCP, UDP, ICMP)**
- **Porta sorgente e destinazione**
- **Direzione del traffico**

Può essere configurato dinamicamente

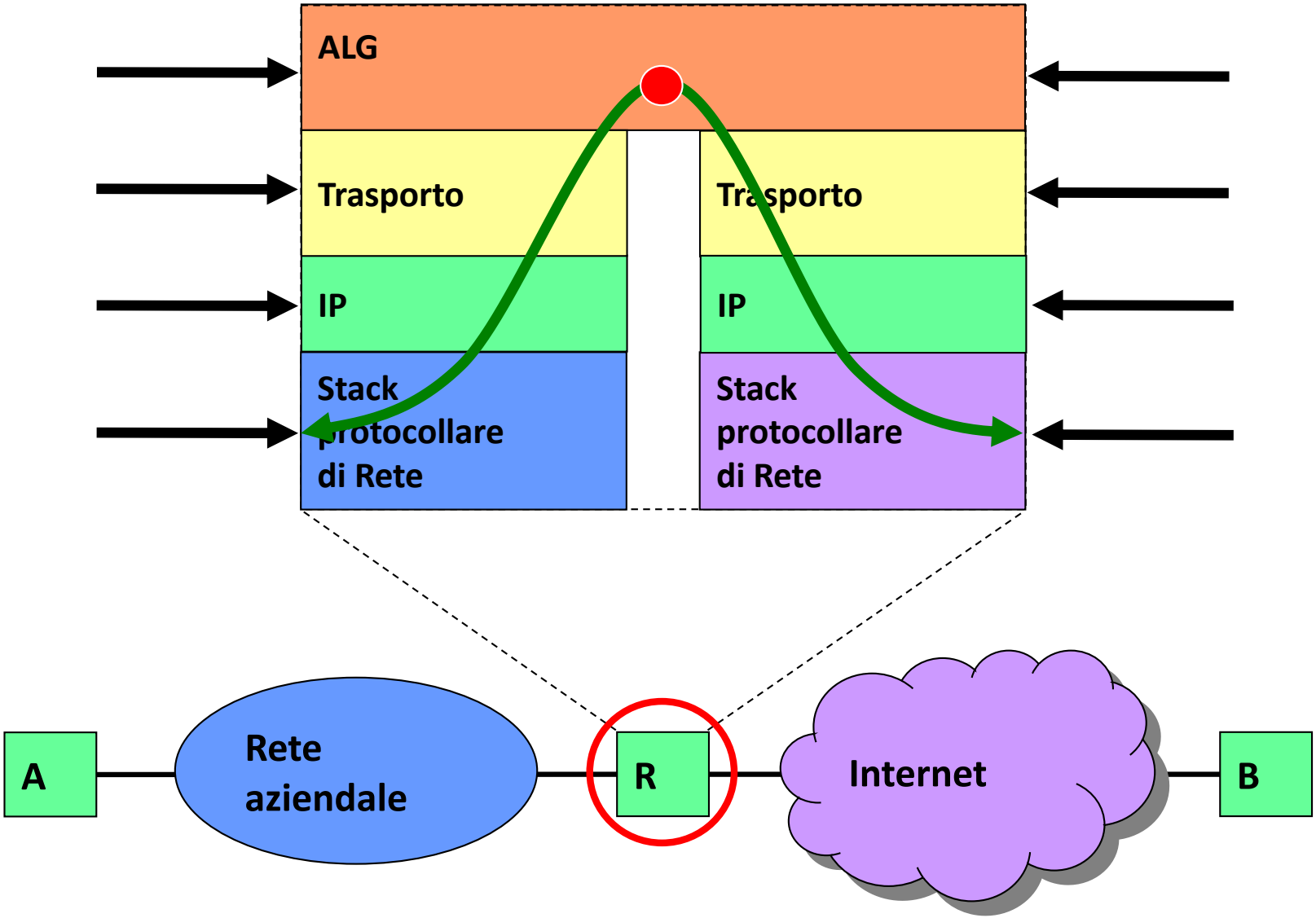
Instradamento selettivo: packet filter



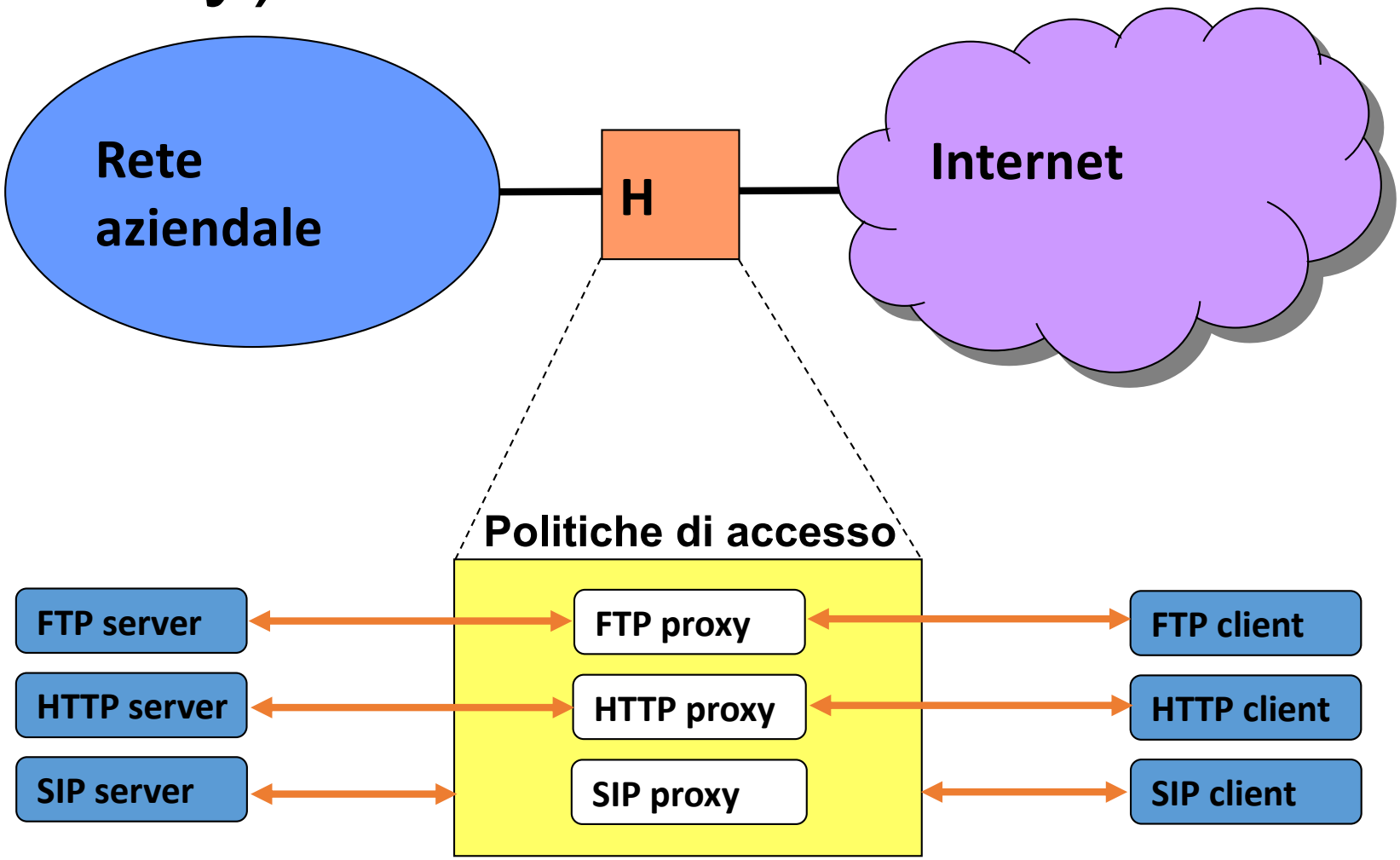
Stateful Packet Inspection



Application Layer Gateway (Proxy)



Application Layer Gateway (Proxy)



Firewall

- Packet Filter: filtra i pacchetti seguendo la politiche stabilite
  - Filtri: generalmente configurati staticamente
  - La maggioranza delle configurazioni non permettono pacchetti per porte “non-standard” (Internet Assigned Numbers Authority – IANA)

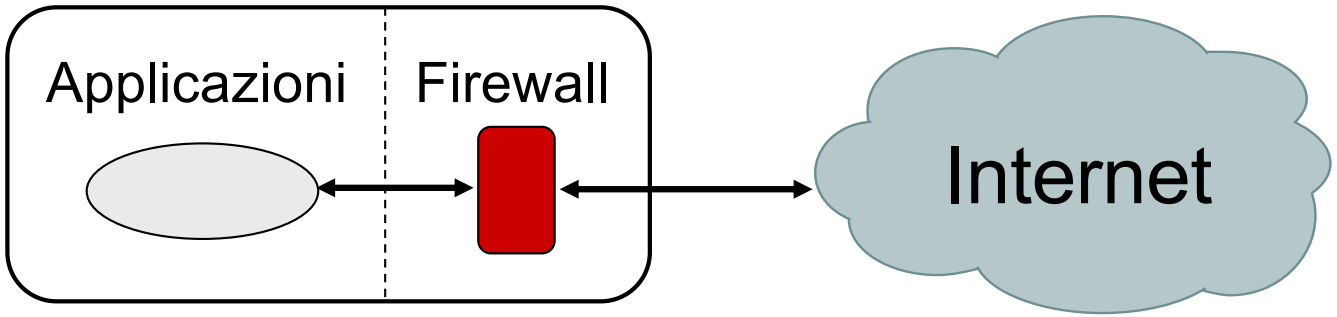
- Stateful Packet Inspection
  - Mantiene il contesto dei pacchetti sia nel trasporto che nello strato applicativo
  - Adatta dinamicamente le specifiche dei filtri

- Application Layer Gateway (trasparente o proxy esplicito)
  - Monitora le connessioni: analizza il contenuto dei protocolli applicativi
    - A scapito della sicurezza di comunicazione end-to-end
  - Adatta dinamicamente le specifiche dei filtri

- Per ogni strato (layer) dello stack possono essere applicate politiche (policies) differenti

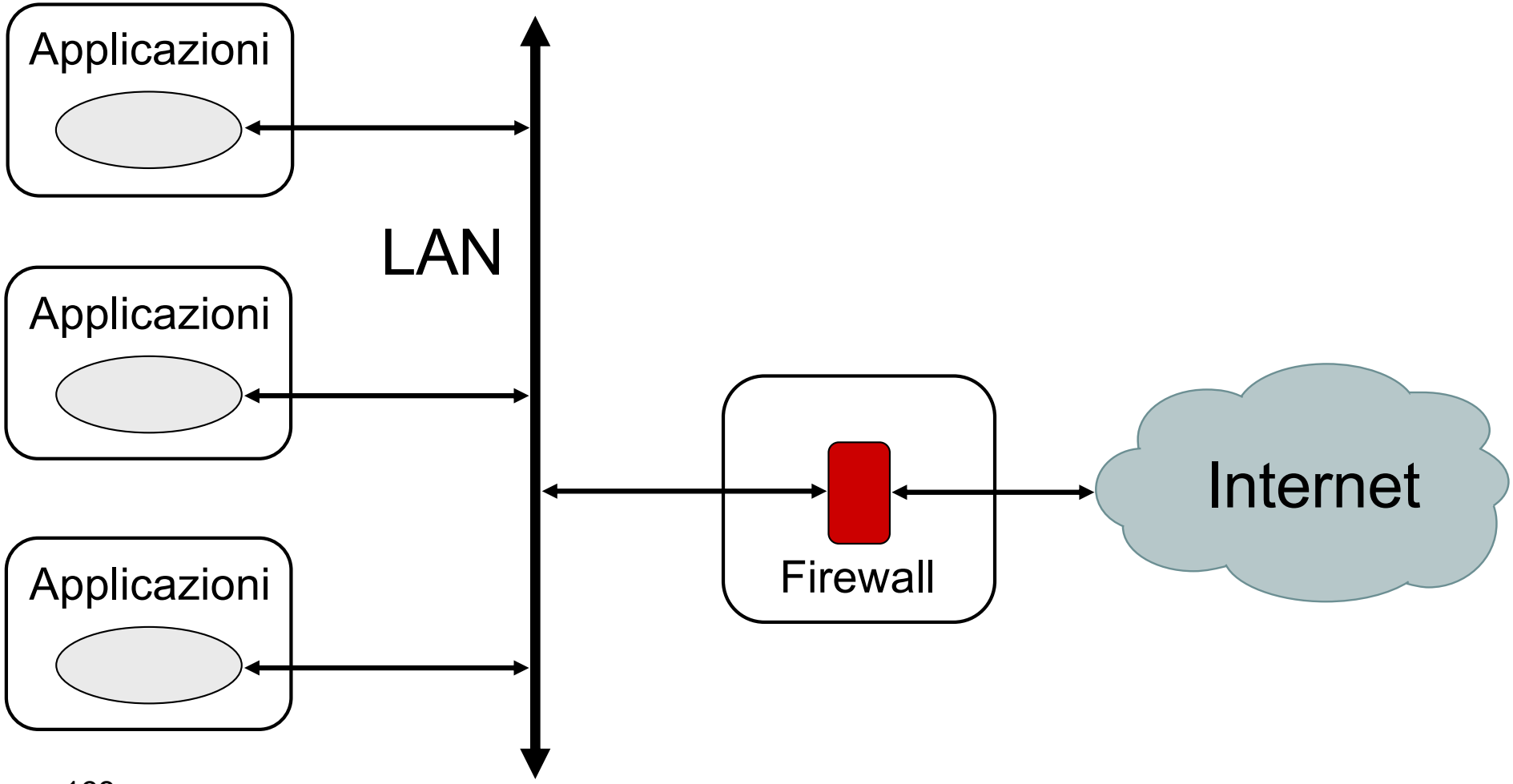
Protezione di host: firewall

- Un firewall è un filtro software/hardware che serve a proteggersi da accessi indesiderati provenienti dall'esterno della rete
- Può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni
  - tipicamente usato in accessi domestici a larga banda (ADSL, FTTH)



Protezione di rete: firewall

- Oppure può essere una macchina dedicata che filtra tutto il traffico da e per una rete locale



Protezione di rete: firewall

- Tutto il traffico fra la rete locale ed Internet deve essere filtrato dal firewall
- Solo il traffico autorizzato deve attraversare il firewall
- Si deve comunque permettere che i servizi di rete ritenuti necessari siano mantenuti
- Il firewall deve essere per quanto possibile immune da problemi di sicurezza sull'host
- In fase di configurazione di un firewall, per prima cosa si deve decidere la politica di default per i servizi di rete
  - **default deny**: tutti servizi non esplicitamente permessi sono negati
  - **default permit**: tutti i servizi non esplicitamente negati sono permessi

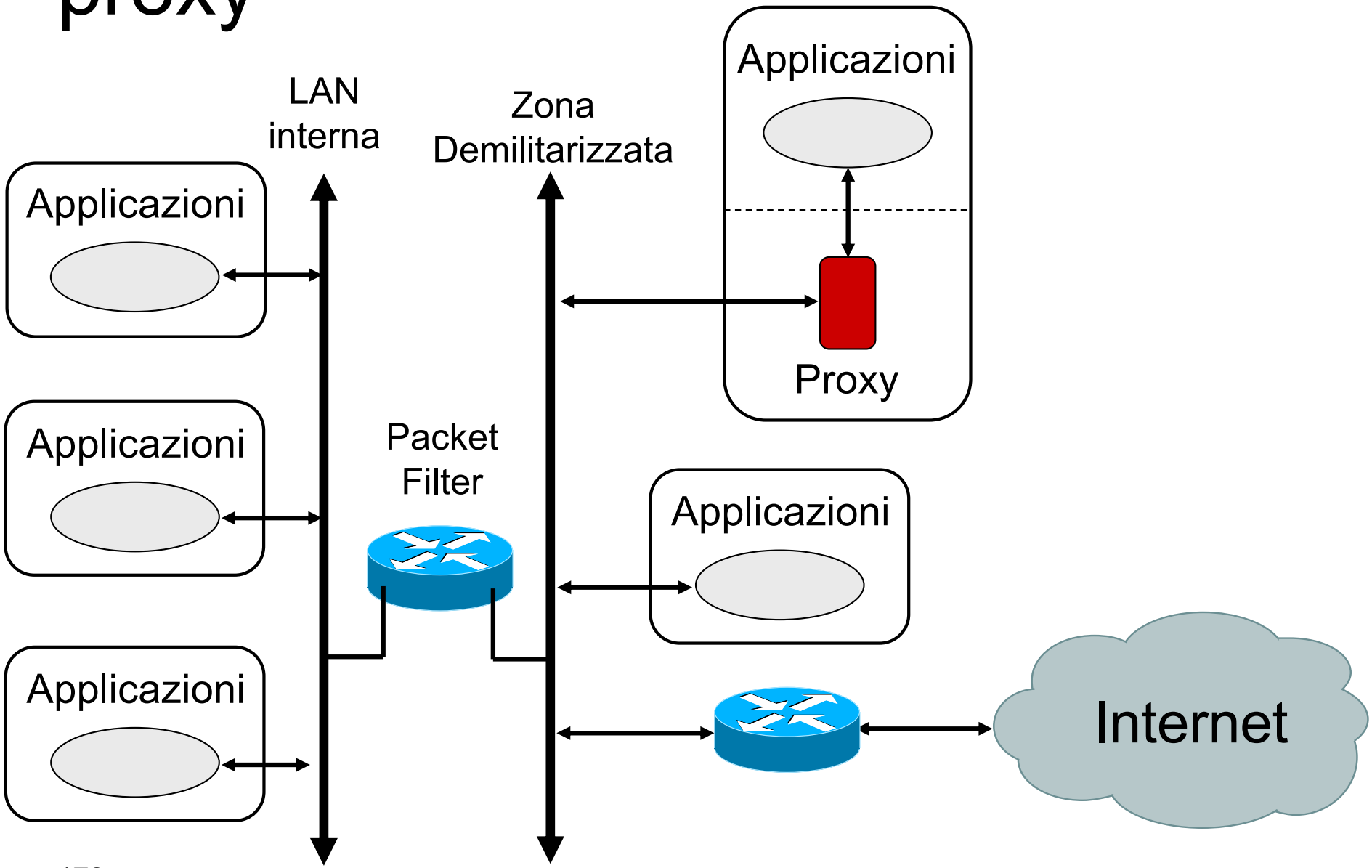
Livelli di implementazione

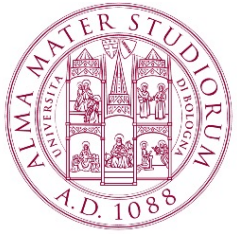
- Un firewall può essere implementato come
  - packet filter
  - proxy server
    - application gateway
    - circuit-level gateway
- **Packet filter**
  - si interpone un router fra la rete locale ed Internet
  - sul router si configura un filtro sui datagrammi IP da trasferire attraverso le varie interfacce
  - il filtro scarta i datagrammi sulla base di
    - indirizzo IP sorgente o destinazione
    - tipo di servizio a cui il datagramma è destinato (porta TCP/UDP)
    - interfaccia di provenienza o destinazione

Livelli di implementazione

- **Proxy server**
  - nella rete protetta l'accesso ad Internet è consentito solo ad alcuni host
  - si interpone un server apposito detto proxy server per realizzare la comunicazione per tutti gli host
  - il proxy server evita un flusso diretto di datagrammi fra Internet e le macchine della rete locale
  - **application level**
    - viene impiegato un proxy server dedicato per ogni servizio che si vuole garantire
  - **circuit level gateway**
    - è un proxy server generico in grado di inoltrare le richieste relative a molti servizi

Configurazione di packet filter e proxy





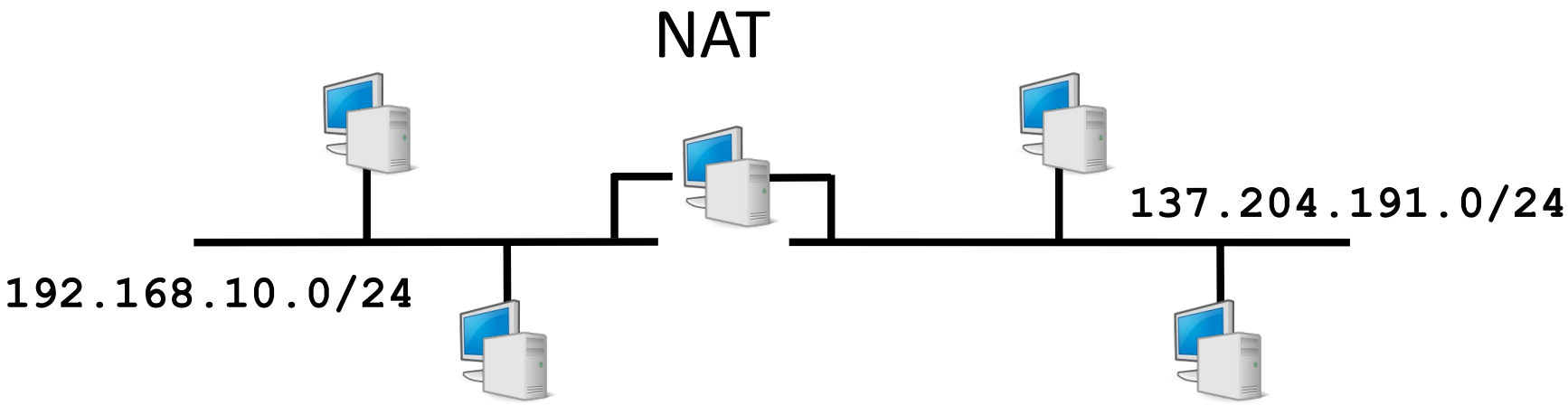
ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Network Address Translation

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

Network Address Translation (NAT)

- Tecnica per il filtraggio di pacchetti IP con sostituzione degli indirizzi (mascheramento)
  - Indirizzi e porte
- Definito nella RFC 3022 per permettere a reti IP private l'accesso a reti IP pubbliche tramite un apposito gateway
- Utile per il risparmio di indirizzi IP pubblici e il riutilizzo di indirizzi IP privati



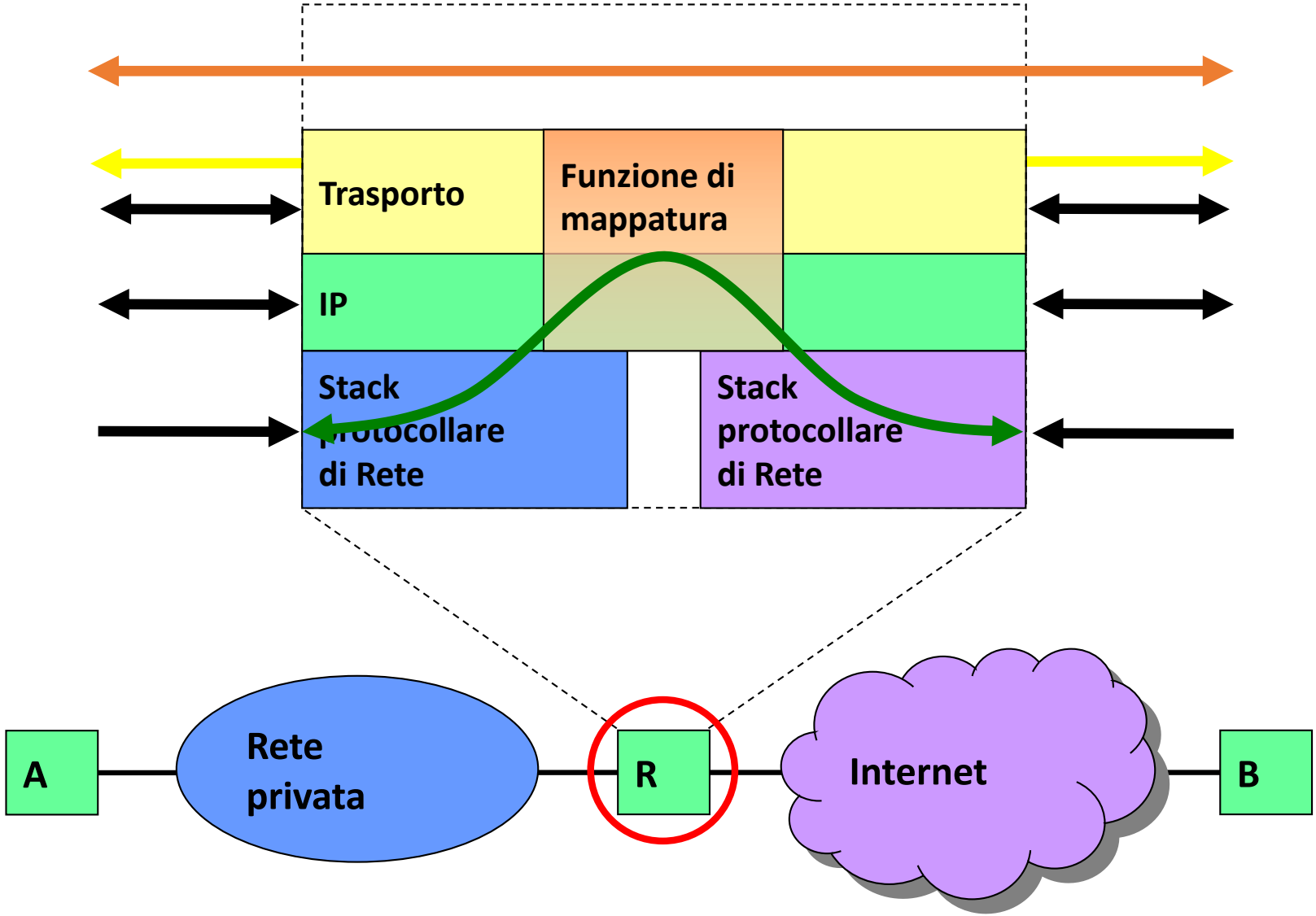
NAT: motivazioni

- Efficiente uso della spazio degli indirizzi
- Condividere uno o pochi indirizzi
- Uso di indirizzi privati nella LAN locale (10.x.x.x, 192.168.x.x, …)

- Security
  - Rendere gli host interni non accessibili dall'esterno
  - Nascondere gli indirizzi e la struttura della rete

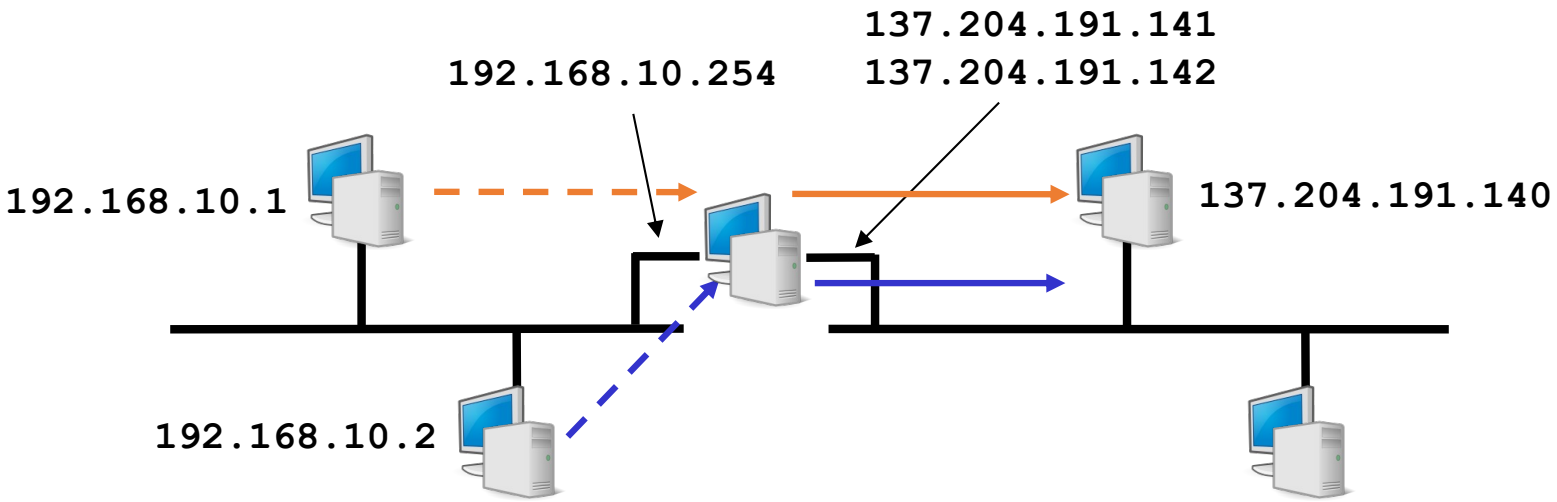
- Include un packet filter, stateful packet inspection configurati dinamicamente

Network (+Port) Address Translator (NAT)



Basic NAT – Conversione di indirizzo

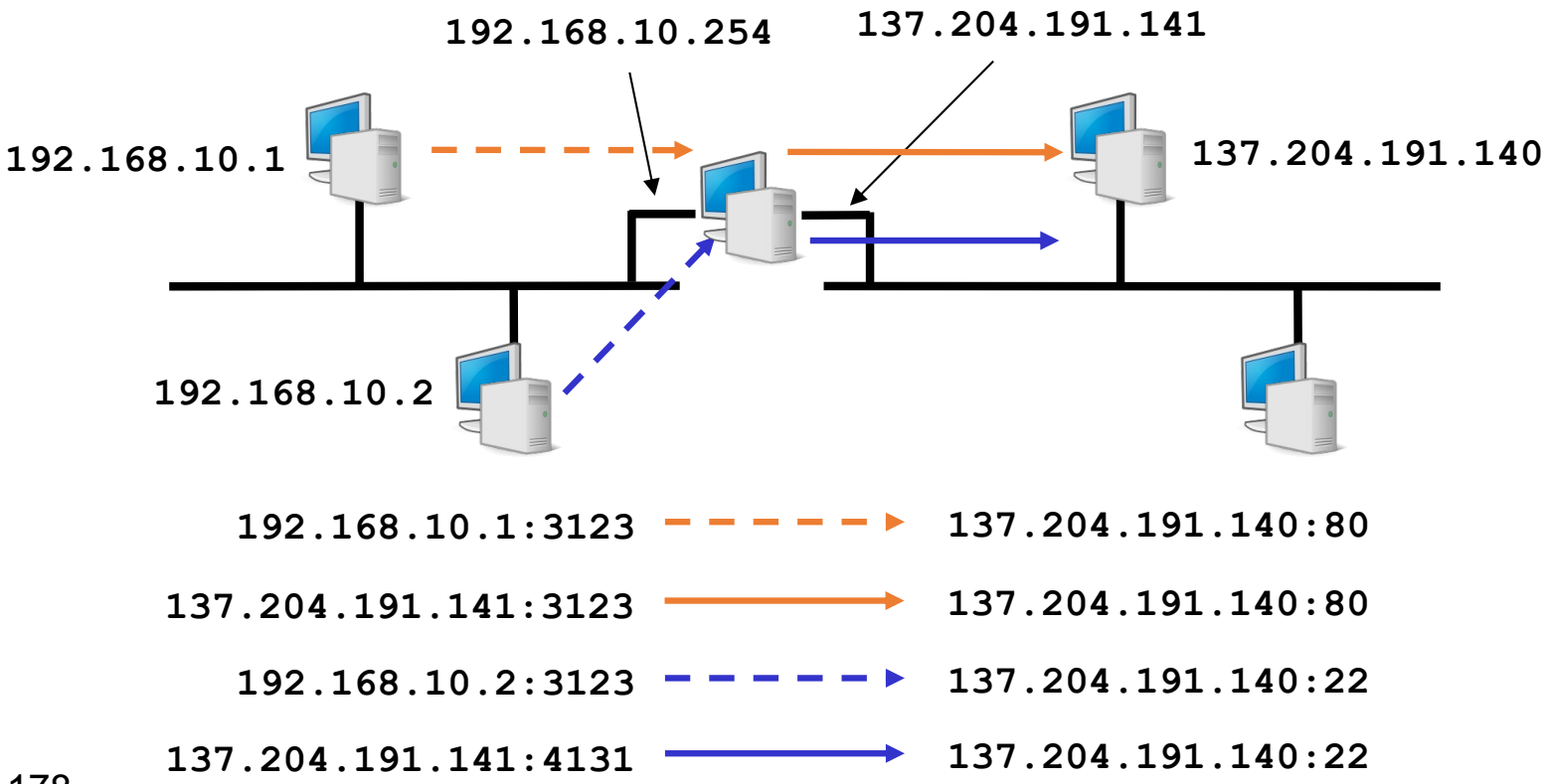
- Il NAT può fornire una semplice conversione di indirizzo IP (statica o dinamica)
- Conversioni contemporanee limitate dal numero di indirizzi IP pubblici a disposizione del gateway NAT



192.168.10.1:3123	⇢	137.204.191.140:80
137.204.191.141:3123	→	137.204.191.140:80
192.168.10.2:5039	⇢	137.204.191.140:22
137.204.191.142:5039	→	137.204.191.140:22

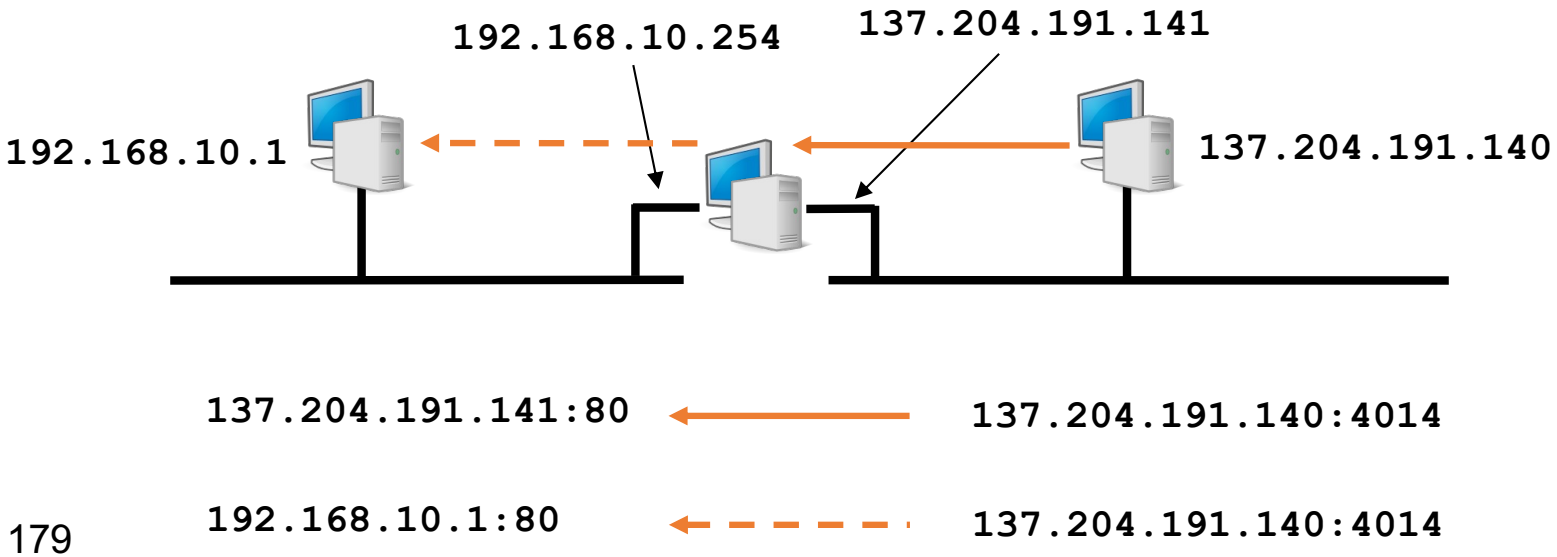
Conversione di indirizzo e porta

- Il NAT può fornire anche conversione di indirizzo IP e porta TCP o UDP
- Conversioni contemporanee possibili anche con un unico indirizzo IP pubblico del gateway NAT



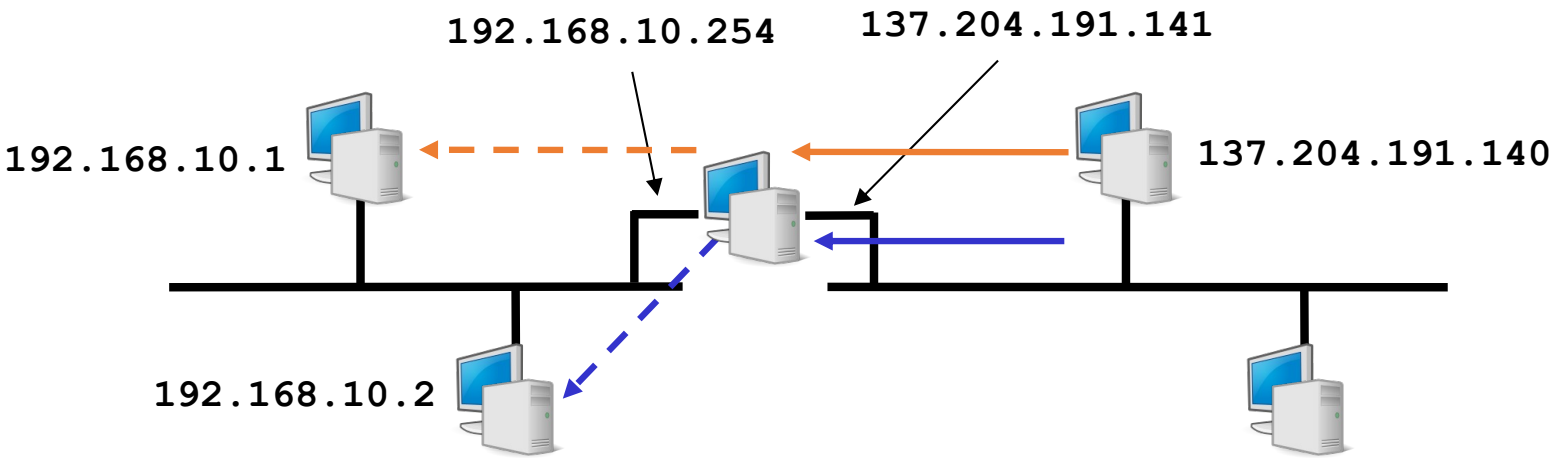
Direzione delle connessioni

- Tipicamente da rete privata verso rete pubblica
  - Il NAT si preoccupa di effettuare la conversione inversa quando arrivano le risposte
  - Registra le corrispondenze in corso in una tabella
- E' possibile contattare dalla rete pubblica un host sulla rete privata?
  - Dipende dal tipo di NAT e dalla relativa configurazione



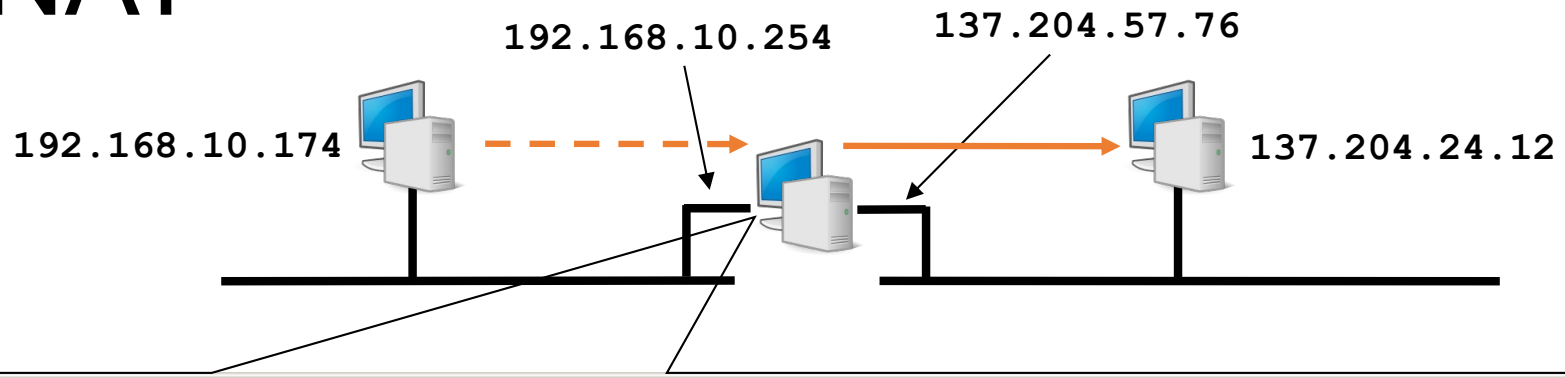
Port forwarding

- Il NAT permette l'ingresso di pacchetti destinati a porte specifiche effettuando la traduzione opportuna



137.204.191.141:80	←	137.204.191.140:4014
192.168.10.1:80	←	137.204.191.140:4014
137.204.191.141:8080	←	137.204.191.140:4015
192.168.10.2:8080	←	137.204.191.140:4015

Analisi di connessioni attraverso NAT

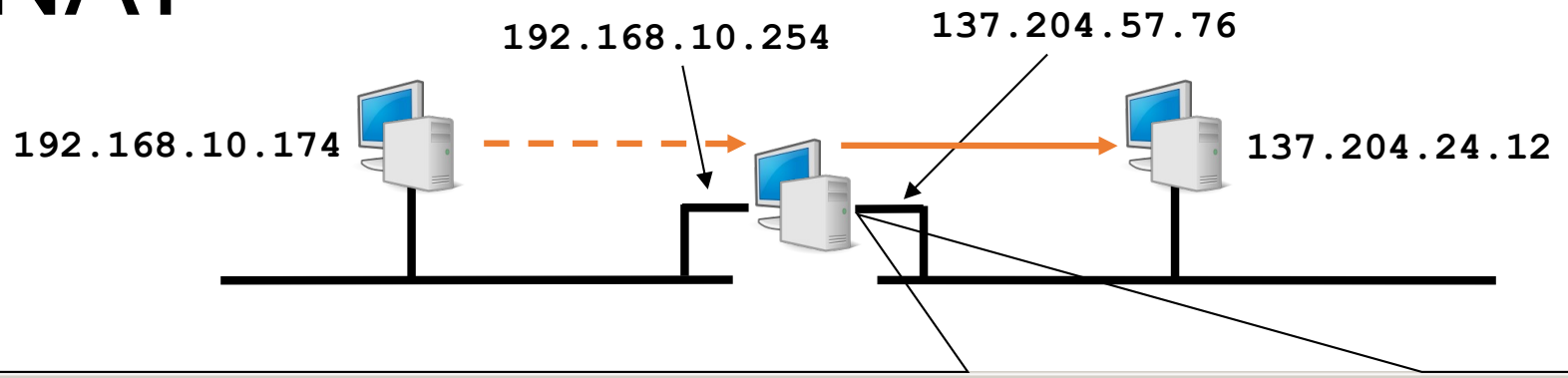


NAT-int.cap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.10.174	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034608	137.204.24.12	192.168.10.174	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1
3	0.896816	137.204.24.12	192.168.10.174	HTTP	HTTP/1.1 200 OK
4	0.896908	137.204.24.12	192.168.10.174	HTTP	Continuation
5	0.898068	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665387993 Win=6
6	0.899848	137.204.24.12	192.168.10.174	HTTP	Continuation
7	0.899971	137.204.24.12	192.168.10.174	HTTP	Continuation
8	0.900095	137.204.24.12	192.168.10.174	HTTP	Continuation
9	0.900913	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665389453 Win=6
10	0.901066	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665392373 Win=6
11	0.902676	137.204.24.12	192.168.10.174	HTTP	Continuation
12	0.902798	137.204.24.12	192.168.10.174	HTTP	Continuation
13	0.902921	137.204.24.12	192.168.10.174	HTTP	Continuation
14	0.903045	137.204.24.12	192.168.10.174	HTTP	Continuation
15	0.903168	137.204.24.12	192.168.10.174	HTTP	Continuation
16	0.903846	192.168.10.174	137.204.24.12	HTTP	GET /NR/Custom/web/Common/css/stile_main.c
17	0.903848	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665393833 Win=6
18	0.903850	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665396753 Win=6
19	0.904022	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665398213 Win=6
20	0.905643	192.168.10.174	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665399673 Win=6

Analisi di connessioni attraverso NAT



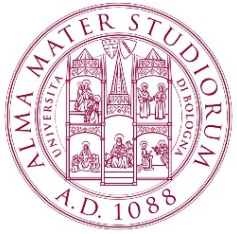
NAT-ext.cap - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	137.204.57.76	137.204.24.12	HTTP	GET /Ingegneria+Cesena/default.htm HTTP/1.
2	0.034559	137.204.24.12	137.204.57.76	TCP	80 > 3770 [ACK] Seq=3665385073 Ack=46511275 Win=1128
3	0.896736	137.204.24.12	137.204.57.76	HTTP	HTTP/1.1 200 OK
4	0.896859	137.204.24.12	137.204.57.76	HTTP	Continuation
5	0.898045	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665387993 Win=6424
6	0.899803	137.204.24.12	137.204.57.76	HTTP	Continuation
7	0.899925	137.204.24.12	137.204.57.76	HTTP	Continuation
8	0.900050	137.204.24.12	137.204.57.76	HTTP	Continuation
9	0.900889	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665389453 Win=6424
10	0.901042	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665392373 Win=6424
11	0.902630	137.204.24.12	137.204.57.76	HTTP	Continuation
12	0.902752	137.204.24.12	137.204.57.76	HTTP	Continuation
13	0.902875	137.204.24.12	137.204.57.76	HTTP	Continuation
14	0.903000	137.204.24.12	137.204.57.76	HTTP	Continuation
15	0.903122	137.204.24.12	137.204.57.76	HTTP	Continuation
16	0.903836	137.204.57.76	137.204.24.12	HTTP	GET /NR/Custom/web/Common/css/stile_main.c
17	0.903847	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665393833 Win=6424
18	0.903855	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665396753 Win=6424
19	0.903999	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665398213 Win=6424
20	0.905619	137.204.57.76	137.204.24.12	TCP	3770 > 80 [ACK] Seq=46511275 Ack=3665399673 Win=6424

NAT e applicazioni di rete

- Il NAT è trasparente per l'applicazione
  - Modifica l'intestazione IP e TCP/UDP ma non il payload
- Questo è un problema in alcuni casi specifici
  - Applicazioni non sono trasparenti al NAT
    - Contengono indirizzi IP e numeri di porta nel payload
    - FTP utilizza due connessioni parallele
      - connessione per l'interazione con il server tramite linea di comando (porta TCP 21)
      - connessione per il trasferimento dei dati da e verso il server
      - i parametri della seconda sono specificati nei dati trasmessi dalla prima
  - Il tipo di traffico permesso dipende dal tipo di NAT
    - Full Cone NAT
    - (Port) Restricted Cone NAT
    - Symmetric NAT



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

IPv6

Prof. Franco Callegati
DEIS Università di Bologna
http://deisnet.deis.unibo.it

Problematiche dell'indirizzamento IP

- Mobilità
  - Indirizzi riferiti alla rete di appartenenza
  - Se un host viene spostato in un'altra rete, il suo indirizzo IP deve cambiare
    - Configurazione automatica con DHCP
    - Mobile IP
- Sicurezza
  - Scarsa protezione del datagramma IP (intestazione in chiaro)
    - IPSec applicabile anche a IPv4
- Dimensioni delle reti prefissate
  - Subnetting e CIDR
- Data l'enorme diffusione di Internet, il numero di indirizzi possibili è troppo basso
  - Reti IP private NAT

IPv6

- Stanti i problemi dell'IPv4 attualmente in uso si è lavorato su una nuova versione con i seguenti obiettivi
  - Supportare molti miliardi di host
  - Semplificare il routing
  - Offrire meccanismi di sicurezza
  - Offrire qualità di servizio (multimedialità)
  - Gestire bene multicast e broadcast
  - Consentire la mobilità
  - Fare tutto questo consentendo future evoluzioni e garantendo compatibilità col passato