Università di Roma Tor Vergata
Corso di Laurea triennale in Informatica

Sistemi operativi e reti

A.A. 2018-2019

Pietro Frasca

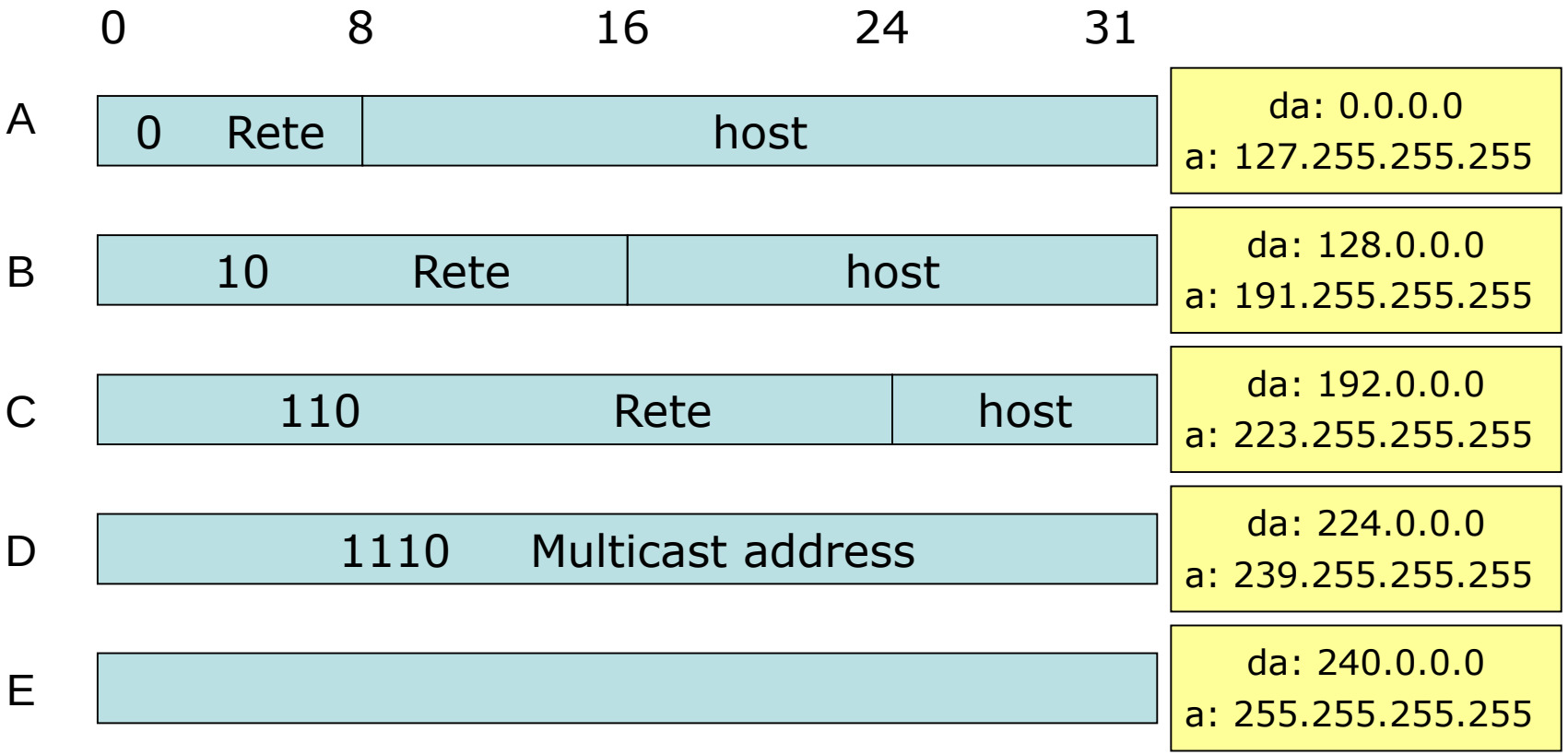
Parte II: Reti di calcolatori

Lezione 17 (41)

Martedì 7-05-2019

Indirizzamento per classe

- Inizialmente, il formato dell'indirizzamento IP definiva **quattro classi dell'indirizzo**, come illustrato nella figura seguente.
- Per un indirizzo della Classe A, i primi otto bit identificano la rete, e gli ultimi 24 bit identificano le interfacce all'interno della rete. Quindi, nella Classe A possiamo avere fino a 2^7 reti (il primo degli otto bit è posto a 0), ciascuna con, al massimo, 2^{24} interfacce.
- Lo spazio nella Classe B dell'indirizzo permette 2^{14} reti, con fino a 2^{16} interfacce entro ciascuna rete.
- Un indirizzo della classe C usa 24 bit per identificare la rete e otto bit per le interfacce.
- Gli indirizzi della Classe D sono riservati per gli indirizzi multicast.
- Gli indirizzi della classe E sono riservati per usi futuri.



Formato di indirizzo di IPV4

- Alcuni indirizzi sono riservati per usi speciali (RFC 3330).

Indirizzi	CIDR	Funzione	RFC	Classe	Totale # indirizzi
0.0.0.0 - 0.255.255.255	0.0.0.0/8	Indirizzi zero	RFC 1700	A	16.777.216
10.0.0.0 - 10.255.255.255	10.0.0.0/8	IP privati	RFC 1918	A	16.777.216
127.0.0.0 - 127.255.255.255	127.0.0.0/8	Localhost Loopback Address	RFC 1700	A	16.777.216
169.254.0.0 - 169.254.255.255	169.254.0.0/16	Zeroconf	RFC 3330	B	65.536
172.16.0.0 - 172.31.255.255	172.16.0.0/12	IP privati	RFC 1918	B	1.048.576
192.0.2.0 - 192.0.2.255	192.0.2.0/24	Documentation and Examples	RFC 3330	C	256
192.88.99.0 - 192.88.99.255	192.88.99.0/24	IPv6 to IPv4 relay Anycast	RFC 3068	C	256
192.168.0.0 - 192.168.255.255	192.168.0.0/16	IP privati	RFC 1918	C	256 reti di 256 host
198.18.0.0 - 198.19.255.255	198.18.0.0/15	Network Device Benchmark	RFC 2544	C	131.072
224.0.0.0 - 239.255.255.255	224.0.0.0/4	Multicast	RFC 3171	D	268.435.456
240.0.0.0 - 255.255.255.255	240.0.0.0/4	Riservato	RFC 1700	E	268.435.456

- L’indirizzamento per classe non è attualmente più utilizzato, anche se è rimasta la terminologia delle classi nel caso in cui il prefisso di rete sia di 1, 2 o 3 byte.
- Dimensionare la parte “rete” di un indirizzo IP a una lunghezza di 1, 2 o 3 byte porta a un’assegnazione di numeri troppo grossolana. Una rete di classe C (/24) può solo contenere al massimo $2^8 - 2 = 254$ indirizzi (il primo è riservato per identificare la rete e l’ultimo per l’indirizzo broadcast) che è un numero troppo piccolo per molte società. D’altra parte, una rete di classe B (/16), con 65634 numeri è troppo grande.
- Nell’indirizzamento per classe, a un’organizzazione con, ad esempio, 2000 host veniva assegnata una classe B (/16). Questo portava a un rapido esaurimento degli indirizzi della classe B e a uno spreco enorme di numeri non usati.

Indirizzamento senza classe

- Nel 1993, l'IETF standardizzò l' instradamento interdominio senza classe (**Classless Inter-Domain Routing**, **CIDR**) [RFC 1519].
- Con l'indirizzamento **CIDR**, il prefisso di rete può avere qualsiasi lunghezza, invece di essere obbligata ad essere di 8, 16 o 24 bit.
- Un indirizzamento CIDR si esprime nella forma decimale puntata ***a.b.c.d/n***, in cui ***n*** indica il numero di bit più significativi che costituisce la parte dell'indirizzo relativa alla rete (prefisso di rete).

- Nel nostro precedente esempio, una società che ha 2000 host può richiedere un blocco di soli 2048 ($\mathbf{2^{11}}$) indirizzi nella forma ***a.b.c.d/21***.
- In questo caso, i primi 21 bit specificano **l'indirizzo della rete** e sono comuni agli indirizzi IP di tutti gli host della società. I restanti 11 bit identificano gli specifici host nella rete dell'organizzazione.
- In pratica, la società può ulteriormente suddividere questi 11 bit rimasti usando una procedura detta **subnetting** [RFC 950] per suddividere la rete *a.b.c.d/21* in sottoreti (subnet) interne.
- Vediamo ora come un'organizzazione può ottenere un blocco di indirizzi di rete, e quindi come si assegna un indirizzo a una scheda di rete.

Assegnazione di indirizzi IP

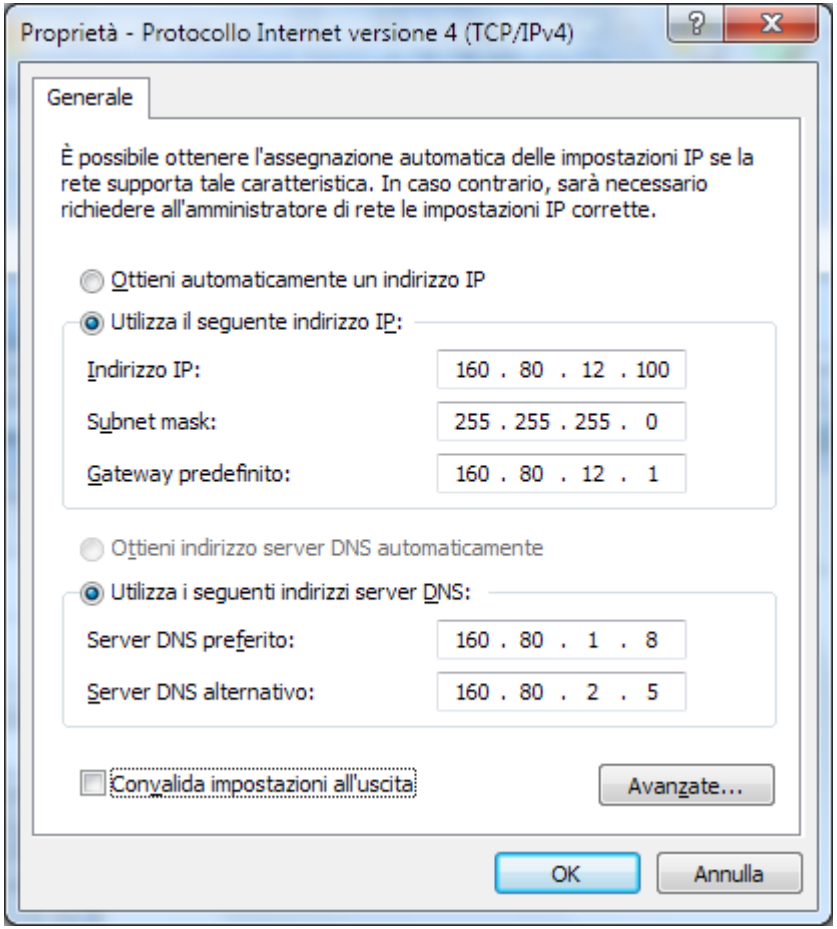
- L' **ICANN** (***Internet Corporation for Assigned Names and Numbers)*** è l'ente che ha la responsabilità di gestire gli indirizzi IP a livello mondiale.
- Come già descritto, l'ICANN gestisce anche i **root server DNS** e si occupa di assegnare i nomi di dominio.
- L'ICANN distribuisce gli indirizzi ad agenzie locali di Internet, che gestiscono gli indirizzi all'interno della loro regione. Queste succursali li assegnano a loro volta agli ISP.
- Infine, per ottenere un blocco di indirizzi IP un amministratore di rete deve contattare un **ISP**, che può assegnargli gli indirizzi IP selezionandoli dagli indirizzi che sono stati ad esso assegnati.
- Ad esempio, un ISP può possedere il blocco di indirizzi **200.23.16.0/20 (2^{12}=4096 indirizzi)**.
- L'ISP, a sua volta, può suddividere questo blocco di indirizzi in blocchi più piccoli e assegnare uno di questi blocchi a delle società clienti.

- L’esempio seguente mostra come un blocco di indirizzi può essere suddiviso in 8 parti uguali di 2^9 = 512 indirizzi ciascuno.

Blocco dell'ISP	**200.23.16.0/20**	11001000 00010111 0001**0000** 00000000
organizzazione 1	200.23.16.0/23	11001000 00010111 0001**000**0 00000000
organizzazione 2	200.23.18.0/23	11001000 00010111 0001**001**0 00000000
organizzazione 3	200.23.20.0/23	11001000 00010111 0001**010**0 00000000
organizzazione 4	200.23.22.0/23	11001000 00010111 0001**011**0 00000000
organizzazione 5	200.23.24.0/23	11001000 00010111 0001**100**0 00000000
organizzazione 6	200.23.26.0/23	11001000 00010111 0001**101**0 00000000
organizzazione 7	200.23.28.0/23	11001000 00010111 0001**110**0 00000000
organizzazione 8	200.23.30.0/23	11001000 00010111 0001**111**0 00000000

Configurazione di un’interfaccia di rete

- Una volta ottenuto un blocco di indirizzi da un ISP, è possibile assegnare indirizzi IP alle interfacce di host e router.
- Per le interfacce dei router l’assegnazione dei numeri IP si esegue manualmente.
- Per gli host, ci sono due modi in cui può essere assegnato un indirizzo IP:
  - ***Configurazione manuale****.* Il numero IP si configura manualmente.
  - ***Configurazione automatica con DHCP (Dynamic Host Configuration Protocol)****.* Il DHCP è un protocollo che permette a un host di ottenere automaticamente un indirizzo IP e le altre informazioni, come l'indirizzo del suo router di default, la netmask e gli indirizzi dei server DNS, necessarie per consentire all’host di comunicare.
- Il DHCP, per le sue caratteristiche *plug-and-play,* è molto utilizzato sia nelle reti LAN che nelle reti wireless.



Finestra di dialogo per la configurazione manuale in Windows

DHCP *(Dynamic Host Configuration Protocol)*

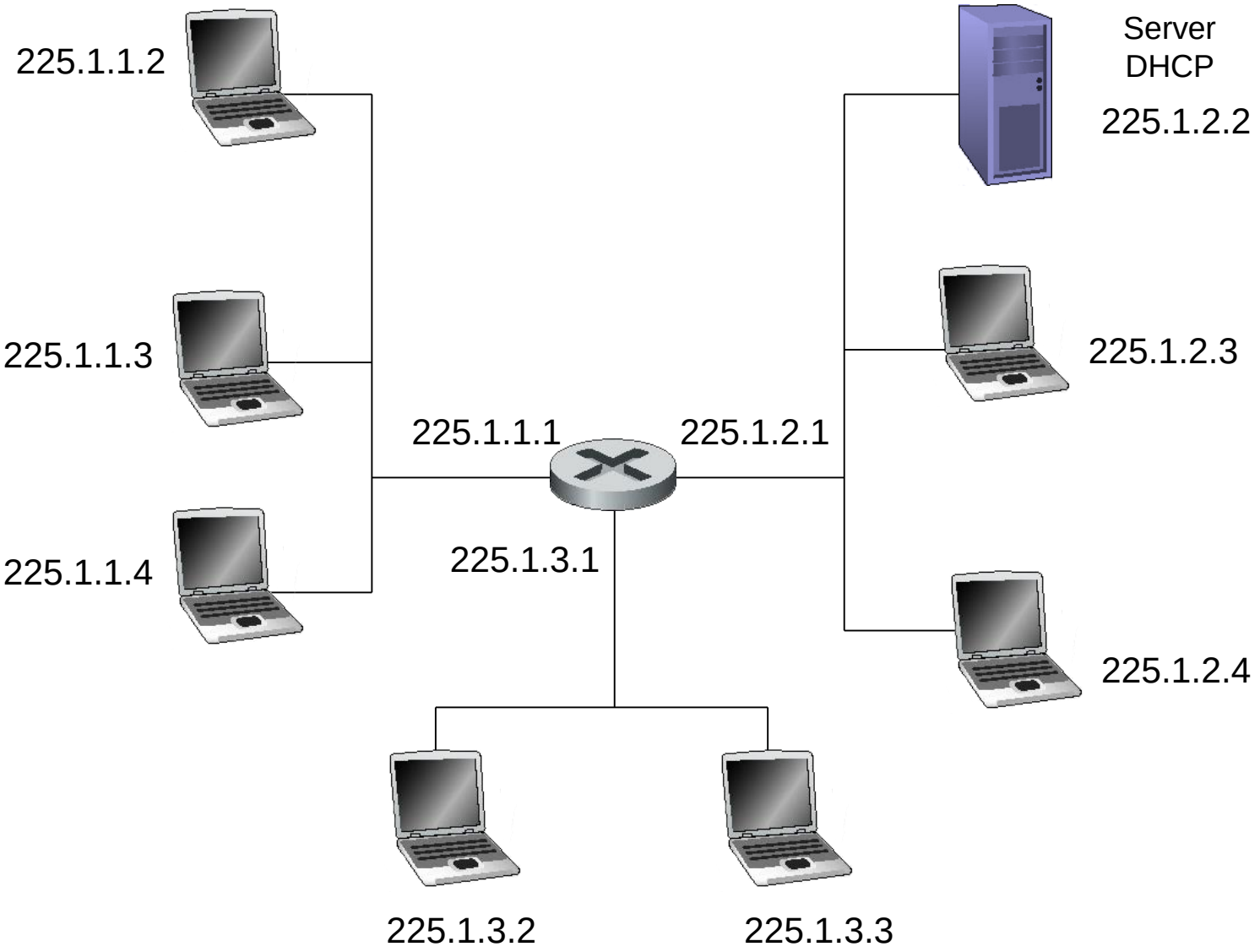
- Il DHCP è un protocollo client/server che utilizza **UDP** e le porte **67** e **68**. Il lato client è implementato sull'host che quando acceso richiede una **configurazione di rete.**
- Un server DHCP può essere configurato in modo che un host riceva un **indirizzo IP permanente**, che userà ogni volta che l'host si connette in rete.
- Generalmente gli ISP per l'accesso residenziale, non possiedono un sufficiente numero di indirizzi IP per tutti i propri clienti. In tal caso, viene utilizzato il DHCP per assegnare a ciascun host che si connette un **indirizzo IP temporaneo**.
- Ad esempio, un ISP residenziale con 3000 clienti, che ha mediamente 1000 clienti connessi nello stesso istante, non ha bisogno di 3000 indirizzi. Infatti, con un server DHCP che assegna gli indirizzi in modo dinamico, all'ISP basta un blocco di 1024 indirizzi (della forma **CIDR a.b.c.d/22**).

- Il server DHCP gestisce una lista di indirizzi IP disponibili che aggiorna ogni volta che un host si connette o si disconnette.
- Quando un host si connette, il server DHCP gli assegna un IP che estrae dalla lista; quando l'host si disconnette, riinserisce il suo numero IP nella lista rendendolo di nuovo disponibile.
- Quando un host si connette, il protocollo DHCP esegue le seguenti quattro fasi:

1. ***Individuazione del server DHCP****.* Il client per trovare un server DHCP invia un ***messaggio di individuazione DHCP (DHCP discover message),*** il messaggio è inviato tramite **UDP** sulla **porta 67**.

   Il client DHCP invia il messaggio di individuazione in broadcast usando l'indirizzo di destinazione broadcast **255.255.255.255** e usa come indirizzo sorgente l'indirizzo speciale **0.0.0.0** ("*questo host*").

   Il messaggio di individuazione sarà ricevuto da tutti i server DHCP connessi in rete.


225.1.1.2
Server
DHCP
225.1.2.2
225.1.1.3
225.1.2.3
225.1.1.1
225.1.2.1
225.1.1.4
225.1.3.1
225.1.2.4
225.1.3.2
225.1.3.3

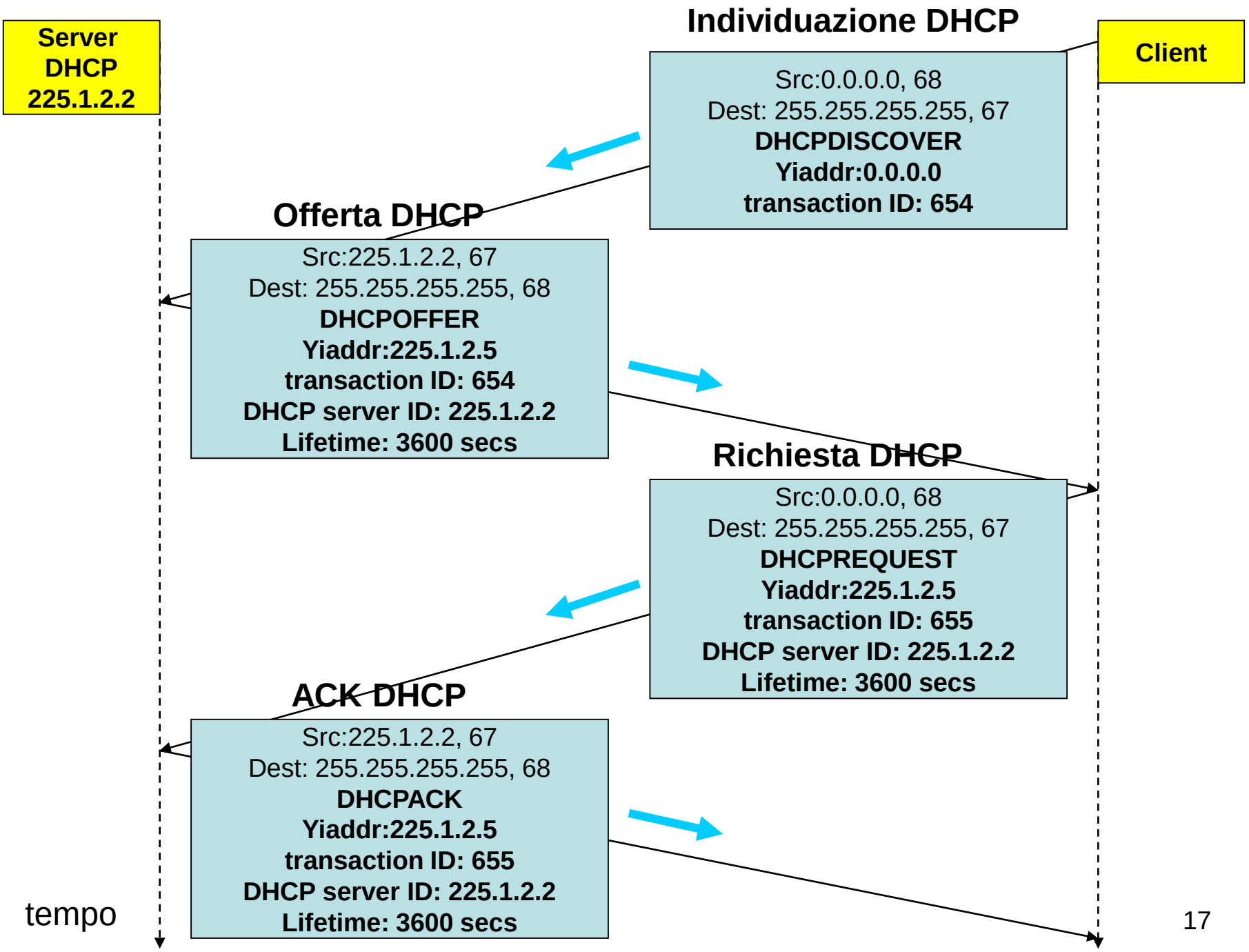
Il *messaggio di individuazione* contiene un ***identificativo di transazione*** che permette di collegare la richiesta alle successive risposte.

2. ***Offerte dei server DHCP****.* Un server DHCP che riceve un *messaggio di individuazione DHCP* risponde al client inviando in broadcast un ***messaggio di offerta DHCP****.* Dato che possono essere presenti sulla rete vari server DHCP, il client può ricevere diversi messaggi di offerta.

   Un messaggio di offerta contiene vari parametri tra i quali:
   - **l'ID di transazione** del messaggio di individuazione ricevuto,
   - **l'indirizzo IP** proposto per il client,
   - la **maschera di rete (net mask)**,
   - L'indirizzo IP del router di default,
   - gli indirizzi IP dei DNS
   - un **tempo di durata di validità dell'indirizzo IP** (tipicamente da parecchie ore a giorni).

3. ***Richiesta DHCP***. L'host sceglierà uno dei messaggi di offerta dei server e risponderà in broadcast all'offerta selezionata con un messaggio di ***richiesta DHCP***, che contiene i parametri di configurazione ricevuti, compreso il numero IP del server DHCP scelto. Il messaggio di richiesta viene ricevuto anche dagli altri server non scelti i quali chiudono la transazione dopo aver verificato che l'indirizzo del server scelto non corrisponde al proprio.
4. ***Conferma (ACK) DHCP***. Il server scelto risponde al messaggio di *richiesta DHCP* con un messaggio ***ACK DHCP***, che conferma i parametri richiesti.

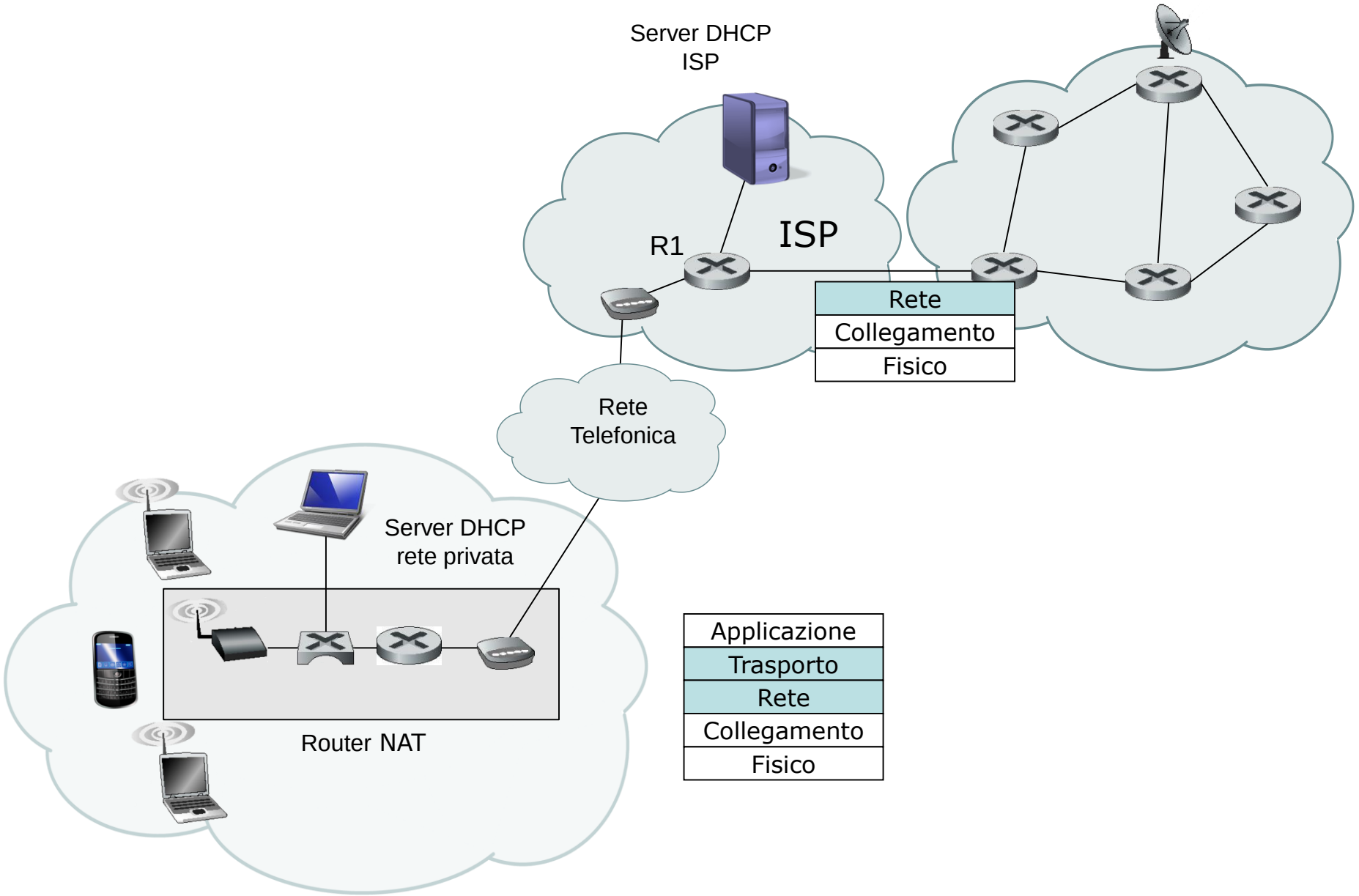
- A questo punto il client può utilizzare l'indirizzo IP assegnato dal server per la durata stabilita. Il DHCP (se configurato opportunamente) permette a un client di rinnovare la durata di un indirizzo IP.
- Nella figura, **yiaddr** (your Internet address) indica l'indirizzo che viene assegnato al client in arrivo.
- La figura mostra un server DHCP connesso alla rete 225.1.2/24.


Server DHCP 225.1.2.2
Individuazione DHCP
Client
Src:0.0.0.0, 68
Dest: 255.255.255.255, 67
DHCPDISCOVER
Yiaddr:0.0.0.0
transaction ID: 654
Offerta DHCP
Src:225.1.2.2, 67
Dest: 255.255.255.255, 68
DHCPOFFER
Yiaddr:225.1.2.5
transaction ID: 654
DHCP server ID: 225.1.2.2
Lifetime: 3600 secs
Richiesta DHCP
Src:0.0.0.0, 68
Dest: 255.255.255.255, 67
DHCPREQUEST
Yiaddr:225.1.2.5
transaction ID: 655
DHCP server ID: 225.1.2.2
Lifetime: 3600 secs
ACK DHCP
Src:225.1.2.2, 67
Dest: 255.255.255.255, 68
DHCPACK
Yiaddr:225.1.2.5
transaction ID: 655
DHCP server ID: 225.1.2.2
Lifetime: 3600 secs
tempo

Traduzione degli indirizzi di rete

- Il crescente aumento del numero di reti ad accesso residenziale ha causato il quasi esaurimento degli indirizzi IP gestiti dagli ISP.
- Una soluzione all'insufficienza di numeri IP, che si è diffusa in questi anni è la tecnologia **NAT (*network address tra**slation,* traduzione degli indirizzi di rete *),*** [RFC 2663 e 3022] implementata in dispositivi, spesso chiamati router NAT.
- Un router NAT è un dispositivo usato per connettere una piccola rete privata con la rete di un ISP.
- I numeri IP privati, utilizzati in queste reti appartengono ai blocchi 10.0.0.0/8 o 172.16.0.0/12 oppure 192.168.0.0/16.
- I router NAT non funzionano come i router ordinari, ma sono visti dalla rete Internet come un **dispositivo** con un ***unico*** **indirizzo IP.**

- Il router NAT ottiene l'indirizzo IP pubblico dal server DHCP dell'ISP. Inoltre, sul router NAT è implementato il lato server DHCP per assegnare gli indirizzi privati agli host della rete privata.
- La figura mostra il funzionamento di un router NAT.
- In questo esempio, le interfacce della rete privata hanno indirizzi IP appartenenti al blocco 192.168.1.0/24.
- Nell'esempio seguente, tutti i pacchetti inviati dal router NAT verso Internet hanno l'indirizzo IP origine 151.27.85.10, e tutti i pacchetti in ingresso al router hanno lo stesso indirizzo come destinazione.
- In pratica, il router NAT nasconde la rete privata al mondo esterno; gli indirizzi IP privati non sono visti al di fuori della rete privata.

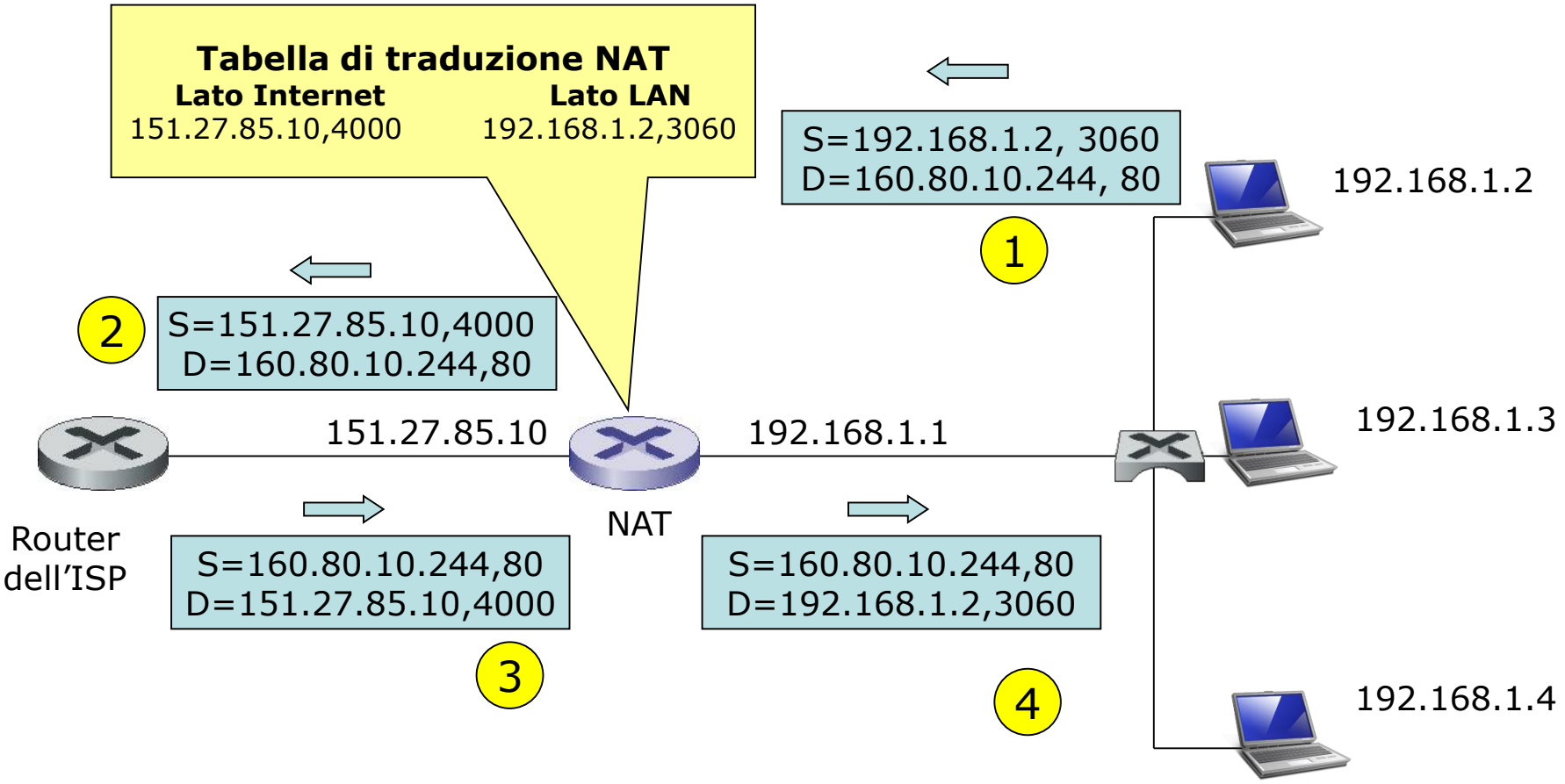

Server DHCP
ISP
R1
ISP
Rete
Collegamento
Fisico
Rete
Telefonica
Server DHCP
rete privata
Router NAT
Applicazione
Trasporto
Rete
Collegamento
Fisico

- Dato che tutti i pacchetti in arrivo al router NAT dalla rete Internet hanno lo stesso indirizzo IP di destinazione descriviamo in che modo il router riesce a inviare i datagram ai diversi host della rete privata.
- La soluzione consiste nell'utilizzare una tabella di traduzione nel router NAT e utilizzare nelle righe di tale tabella i numeri di porta e gli indirizzi IP.

IP Internet	Porta Internet	IP LAN	Porta LAN
151.27.85.10	4000	192.168.1.2	3060
151.27.85.10	4001	192.168.1.3	2050
151.27.85.10	5000	192.168.1.3	6700

- Facciamo riferimento alla figura seguente e supponiamo che l'host 192.168.1.2 si connetta a un server web (porta 80) con indirizzo IP 160.80.10.244.

- Esempio di traduzione degli indirizzi di rete



S=sorgente
D=destinazione

- Il TCP nell'host 192.168.1.2 assegna automaticamente il numero di porta sorgente, ad esempio 3060.
- Quando il router NAT riceve il datagram, estrae dall'intestazione IP il numero IP dell'host mittente e dall'intestazione TCP il numero di porta mittente.
- Scandisce la tabella per verificare se esiste già una riga con questi valori; se non esiste, inserisce una nuova riga avente il valore del campo *IP internet* l'indirizzo IP del dispositivo NAT (151.27.85.10); genera per il datagram un nuovo numero di porta origine, ad esempio 4000, che non sia già presente nelle righe della tabella; negli altri due campi inserisce il numero IP privato dell'host (192.168.1.2) e il numero di porta locale (3060) usato dal processo nell'host.
- Prima di rinviare il datagram verso Internet, sostituisce l'indirizzo IP origine (192.168.1.2) con il proprio indirizzo IP sul lato Internet 151.27.85.10 e sostituisce il numero di porta origine 3060 con il nuovo numero 4000. Il resto del datagram resta invariato.

- Il server web risponde con un datagram con l'indirizzo IP del router NAT come destinazione e il cui numero di porta destinazione è 4000. Quando questo datagram arriva al router NAT, quest'ultimo scandisce la tabella di traduzione NAT usando, come chiave, il numero di porta destinazione per ottenere l'appropriato l'indirizzo IP (192.168.1.2) e il numero di porta destinazione (3060) del browser nella rete privata. Il router, quindi, riscrive l'indirizzo di destinazione del datagram e il suo numero di porta di destinazione, e rinvia il datagram nella LAN privata.
- Notiamo che, essendo il campo numero di porta di 16 bit, il NAT può supportare fino a 65.536 **connessioni** simultanee con un solo indirizzo IP sul lato Internet relativo al router.

UPnP (Universal Plug and Play)

- UPnP è un protocollo che consente ad un host di individuare e configurare un router NAT.
- UPnP consente ad un'applicazione in esecuzione su un host della rete privata di inserire nella tabella del router NAT una corrispondenza tra i propri ***(numero IP privato, numero di porta privato)*** e **(numero IP pubblico, numero di porta pubblico).** In tal modo gli host esterni possono instaurare connessioni TCP o UDP verso l'host della rete privata**.** Inoltre, UPnP consente alle applicazioni di conoscere il **numero IP pubblico e il numero di porta pubblico.**
- Ad esempio, supponiamo che sull'host con indirizzo privato 192.168.1.2 sia in esecuzione un'applicazione P2P che utilizza la porta **4662** TCP, come porta di ascolto per le richieste. Supponiamo che l'indirizzo IP pubblico del NAT sia 151.27.85.10. L'applicazione P2P, mediante UPnP chiede al router NAT di aggiungere una riga nella tabella che fa corrispondere (192.168.1.2, 4662) a (151.27.85.10,5001) dove il numero di porta pubblica 5001 viene scelta in modo che non sia già in uso nel router.

- In tal modo, un pari esterno può connettersi con il pari della NAT usando l'indirizzo 151.27.85.10 e la porta 5001.