Università
degli Studi
della Campania
Luigi Vanvitelli

CORSO DI LAUREA IN TECNICHE DI RADIOLOGIA MEDICA
PER IMMAGINI E RADIOTERAPIA

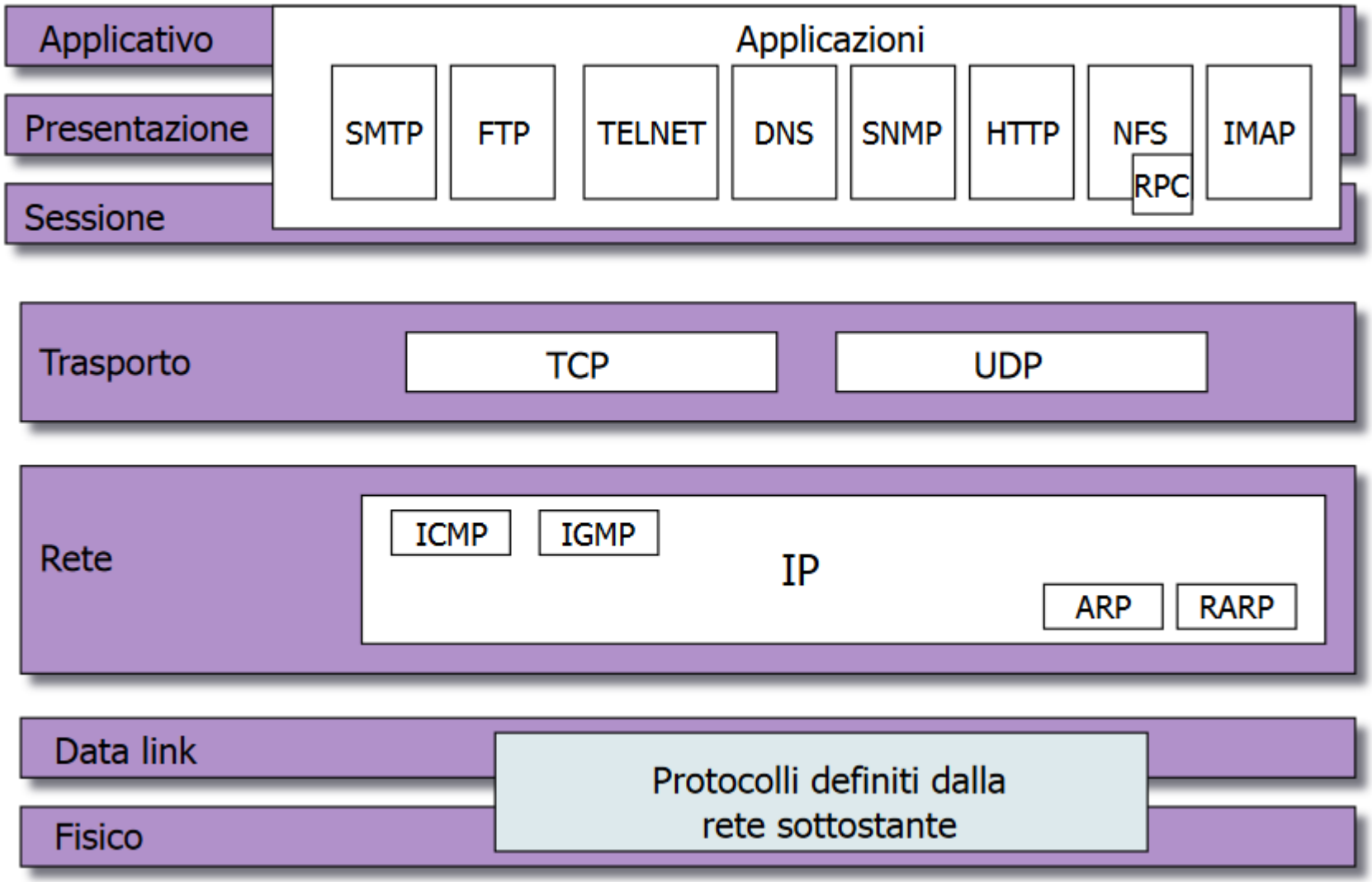
CORSO DI: SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI I

Anno Accademico 2017/2018

Dott. Silvio Pardi

Lezione 4

Il TCP/IP


Applicativo
Presentazione
Sessione
Applicazioni
SMTP
FTP
TELNET
DNS
SNMP
HTTP
NFS
RPC
IMAP
Trasporto
TCP
UDP
Rete
ICMP
IGMP
IP
ARP
RARP
Data link
Fisico
Protocolli definiti dalla
rete sottostante

Protocolli ARP e RARP

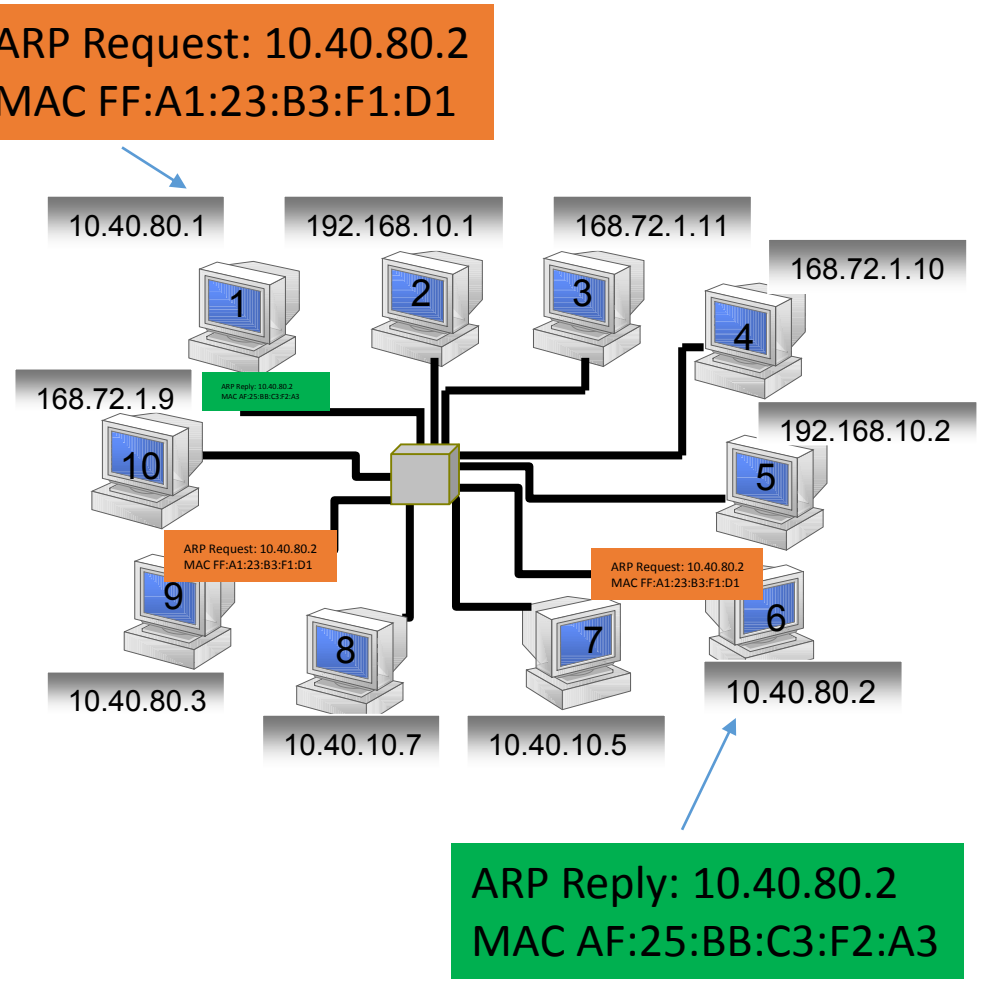
ARP (Address Resolution Protocol) è un protocollo di livello rete che appartiene alla suite di protocolli TCP/IP che ha il ruolo di risolvere l'indirizzo MAC a partire da un indirizzo IP.

RARP (Reverse Address Resolution Protocol) è il protocollo inverso dell'ARP è ha il compito di ottenere l'indirizzo IP assegnato ad un dispositivo a partire dall'indirizzo MAC.

Come Funziona l'ARP

Il dispositivo che vuole conoscere l'indirizzo MAC del dispositivo della rete a cui è assegnato un dato IP invia una richiesta ARP in broadcast sulla rete, ovvero diretta a tutti gli host. Tale richiesta contiene il proprio indirizzo MAC e l'indirizzo IP del destinatario di cui si vuole conoscere il MAC Address.

Tutti i dispositivi della sottorete ricevono la richiesta, ogni host confronta l'IP inivato con il proprio IP. L'host che riconosce il proprio IP invia una risposta (ARP Reply) contenente il proprio MAC direttamente all'host mittente.



Protocollo ICMP

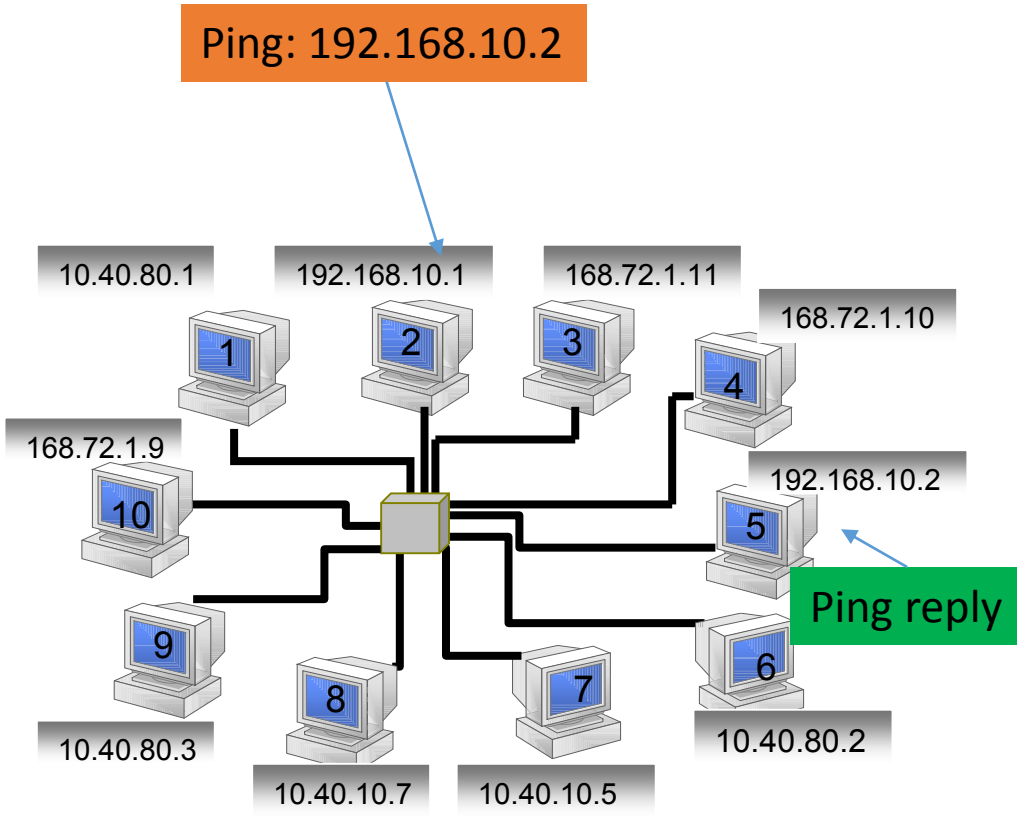
ICMP (Internet Control Message Protocol) è un di diagnosticata che serve a verificare che esista connessione tra due host.

Esso trasmette piccoli pacchetti indirizzati ad host specifici e attende la risposta.

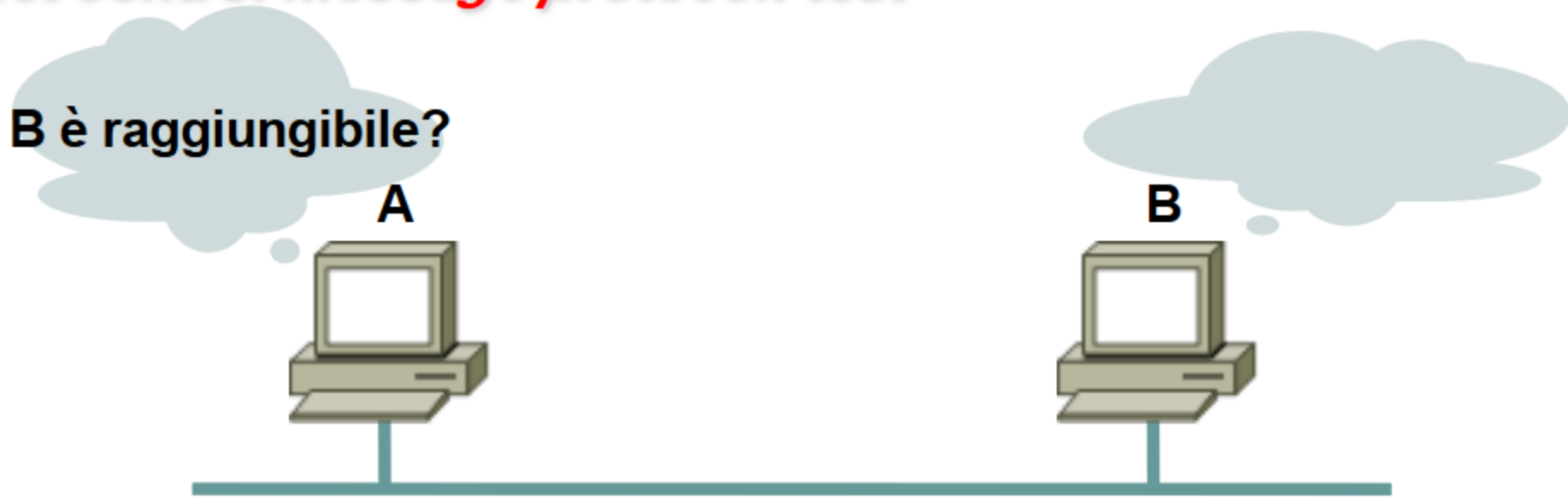
Il comando tipco che utilizza il protocollo ICMP è il comando

PING seguito dall' IP da contattare

Esempio: ping 192.168.10.2

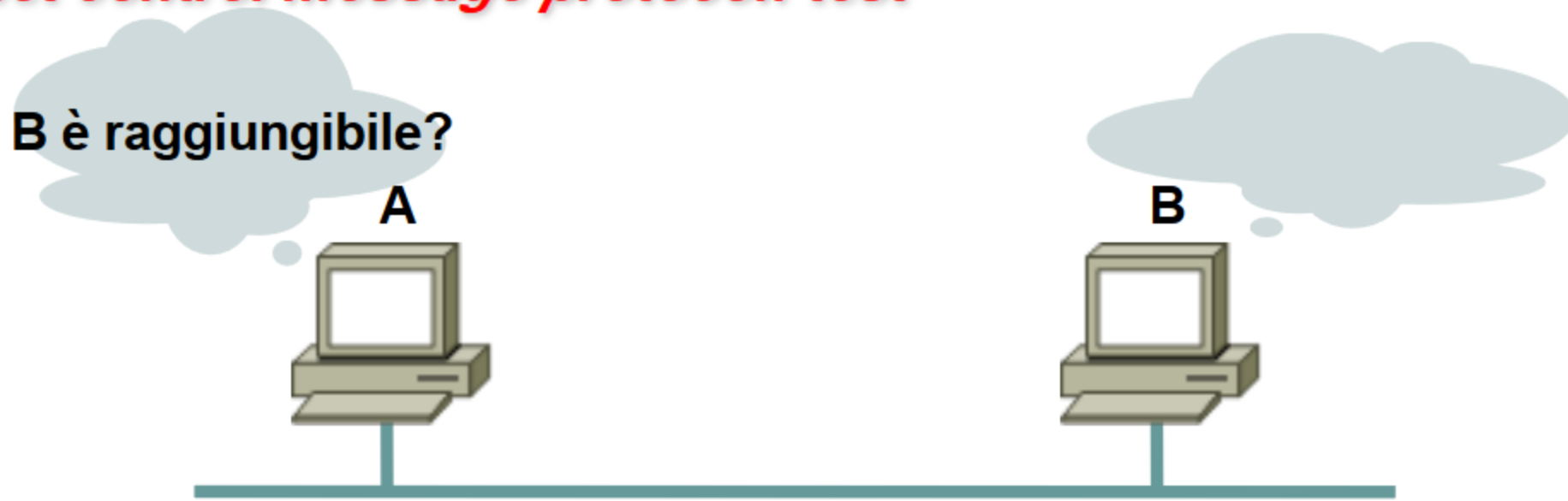


Internet control message protocol: test



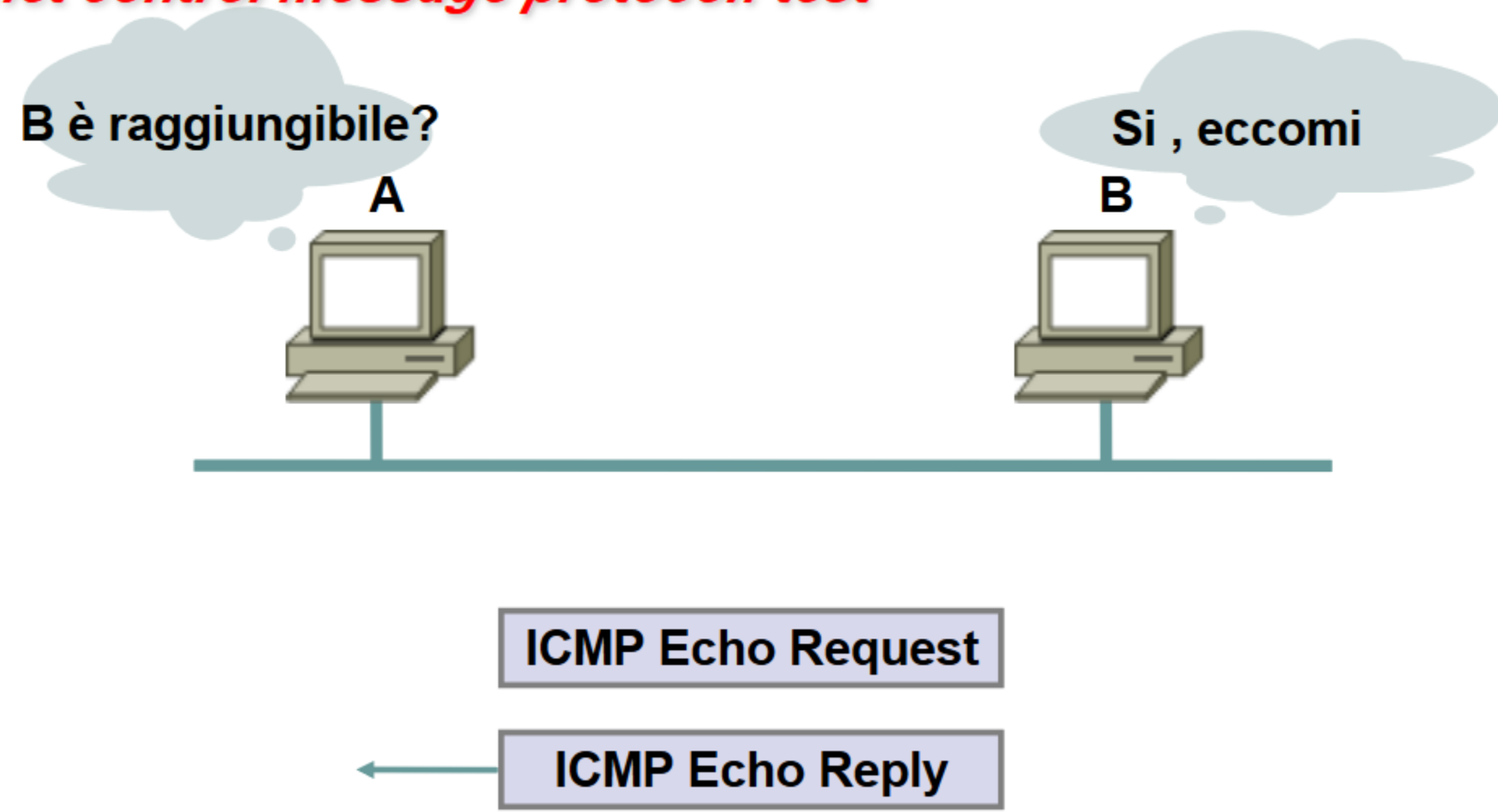
Generato dal comando ping

Internet control message protocol: test



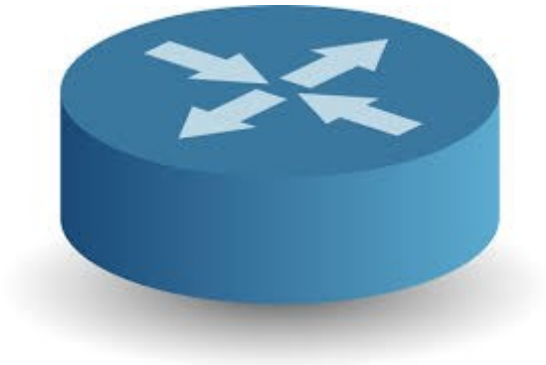
ICMP Echo Request

Internet control message protocol: test



Il Router

Un router è un apparato attivo di rete che ha il compito di connettere più reti tra loro ed effettuare l'instradamento dei pacchetti da un Host di una rete verso Host di alter reti, in maniera ottimale.



ROUTER

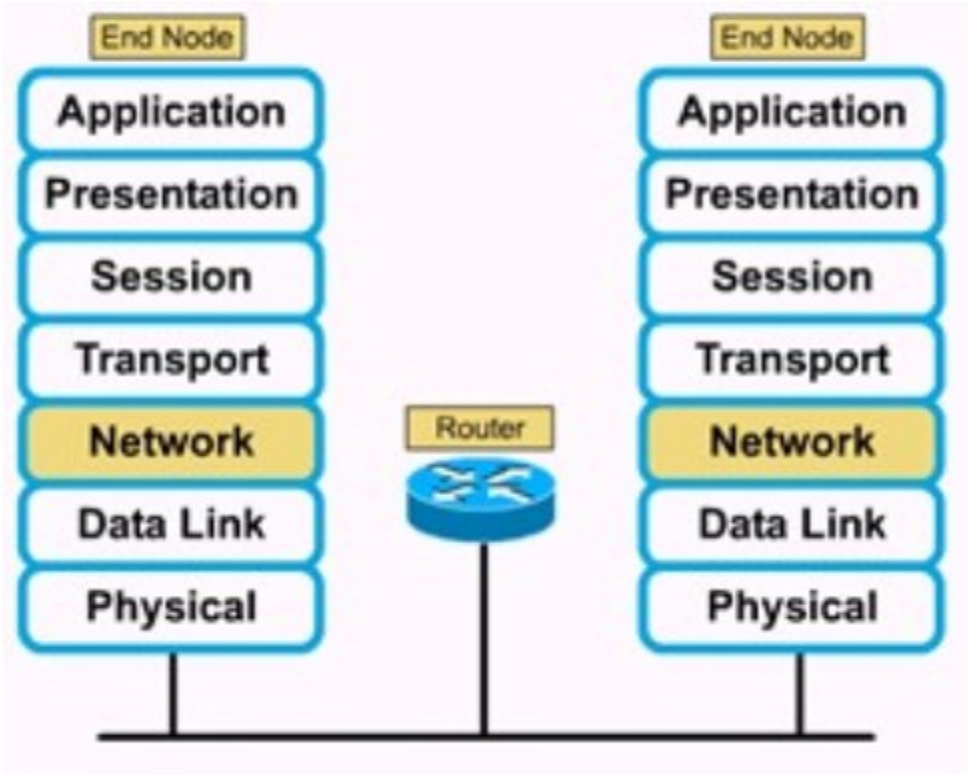
SWITCH

Il Router

Fisicamente sono degli oggetti che somigliano agli switch ma hanno funzionalità diversa.
Hanno un certo numero di porte, chiamate **Interfacce**. Ciascuna serve a connettere una rete.
Hanno una CPU ed una Memoria più potente di uno switch e girano protocolli di routing.
Le interfacce di un router sono dotate di indirizzi IP

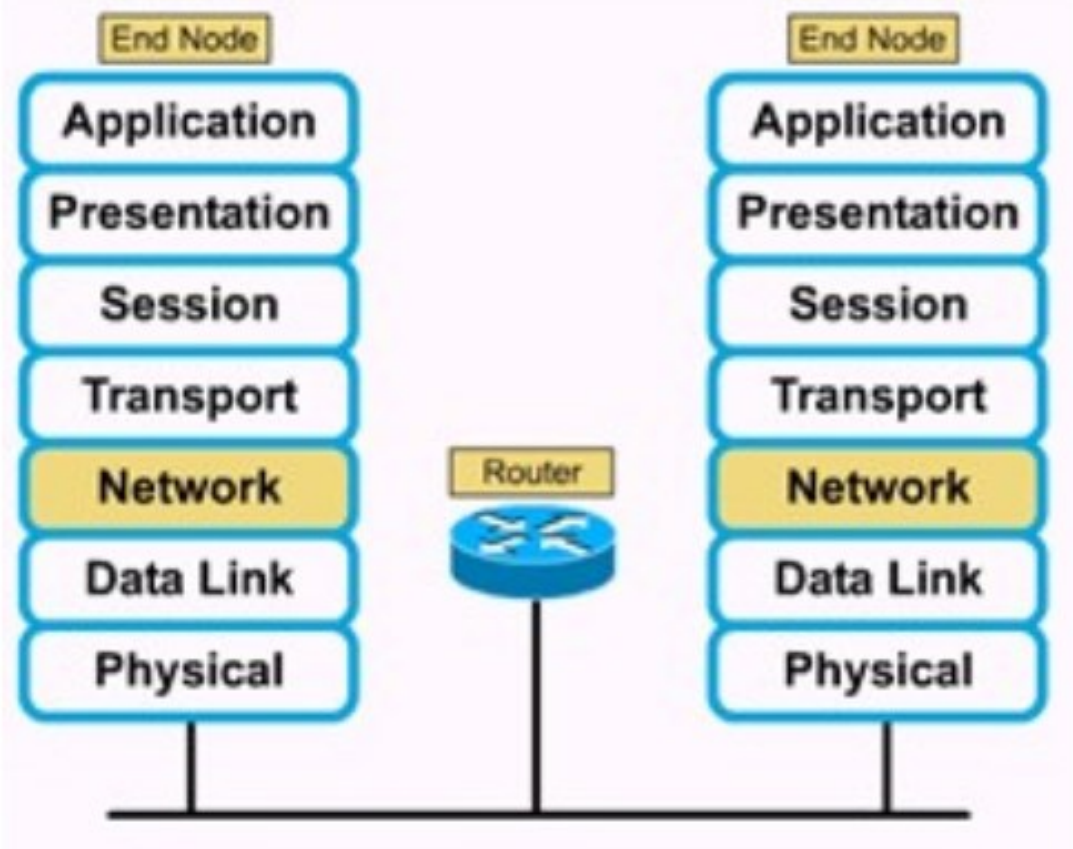
Il Router

- Lo scopo di un router è di esaminare I pacchetti entranti, scegliere il miglior percorso della rete per instradarli verso la destinazione
- Routers lavorano a livello Network.



Il Router

- Un router può connettere differenti reti o sottoreti.
- Un router connette:
  - LAN a LANs
  - LANs a WANs
  - WANs a WANs

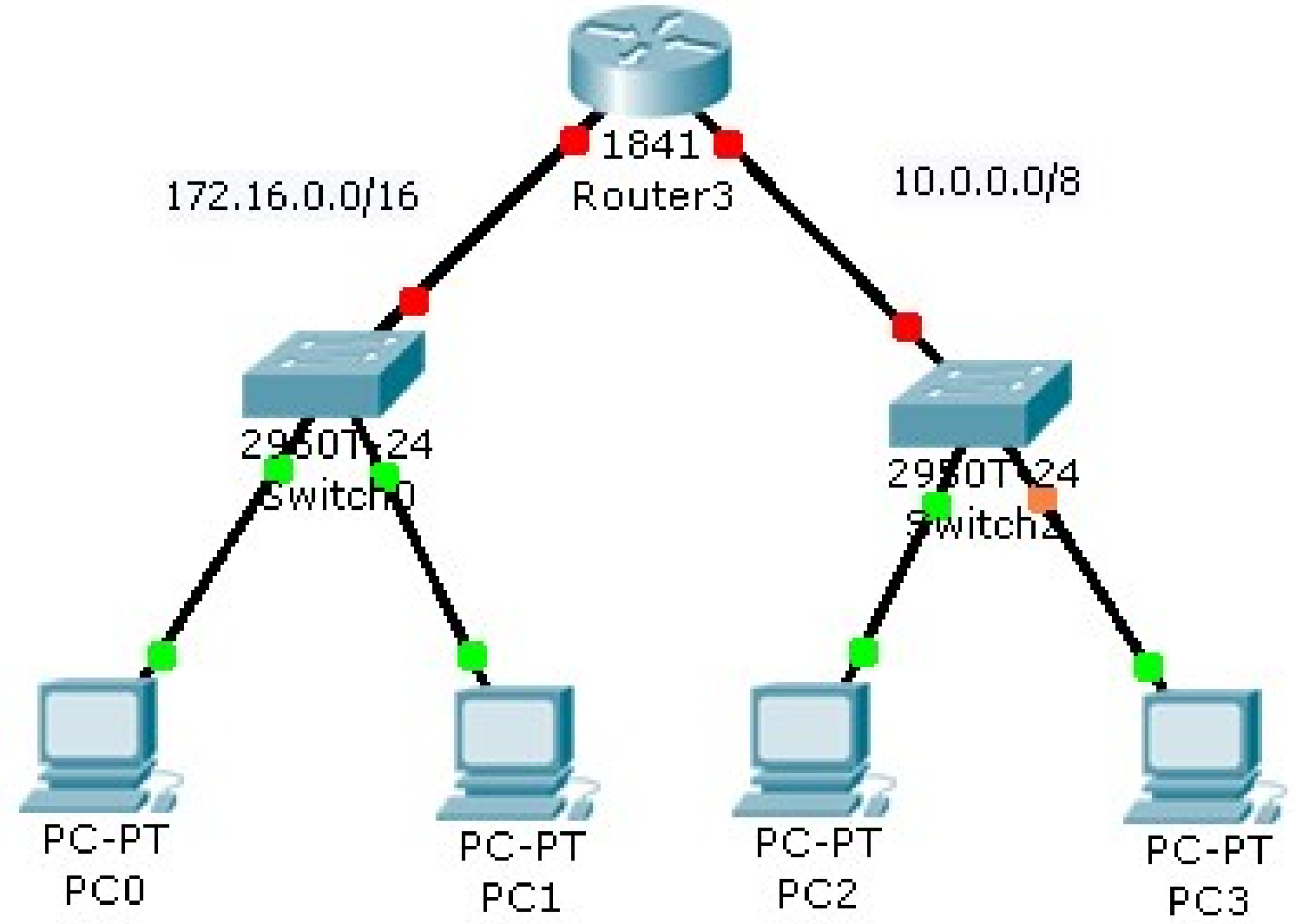


Il Router

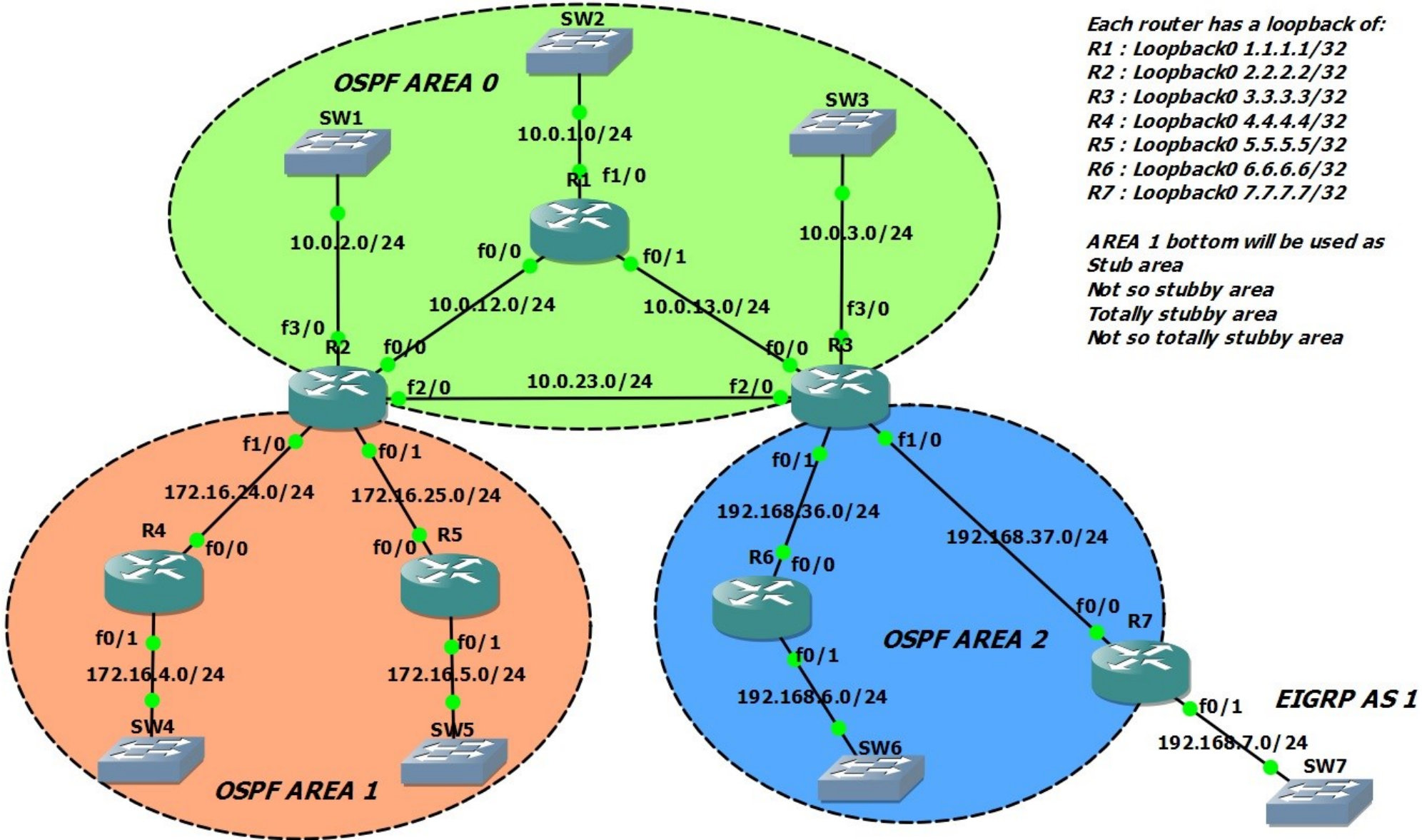
In questa topologia abbiamo
1 router
2 switch
2 reti

- **172.16.0.0/16**
- **10.0.0.0/8**

4 Host



Il Router


OSPF AREA 0
SW2
SW1
SW3
10.0.1.0/24
R1
f1/0
10.0.2.0/24
f0/0
f0/1
10.0.3.0/24
10.0.12.0/24
10.0.13.0/24
f3/0
f3/0
R2
f0/0
f0/0
R3
f2/0
10.0.23.0/24
f2/0
f1/0
f0/1
f1/0
f0/1
172.16.24.0/24
172.16.25.0/24
192.168.36.0/24
192.168.37.0/24
R4
f0/0
f0/0
R5
R6
f0/0
f0/0
R7
f0/1
f0/1
f0/1
OSPF AREA 2
172.16.4.0/24
172.16.5.0/24
192.168.6.0/24
f0/1
EIGRP AS 1
192.168.7.0/24
SW4
SW5
SW6
SW7
OSPF AREA 1
Each router has a loopback of:
R1 : Loopback0 1.1.1.1/32
R2 : Loopback0 2.2.2.2/32
R3 : Loopback0 3.3.3.3/32
R4 : Loopback0 4.4.4.4/32
R5 : Loopback0 5.5.5.5/32
R6 : Loopback0 6.6.6.6/32
R7 : Loopback0 7.7.7.7/32
AREA 1 bottom will be used as
Stub area
Not so stubby area
Totally stubby area
Not so totally stubby area

Il Router

Per decidere quale strada deve seguire un pacchetto per raggiungere l'host di destinazione, il router si avvale di una tabella creata secondo degli algoritmi, nella quale inserisce le reti che conosce e il percorso migliore per raggiungerle.

Il numero di router che deve attraversare un pacchetto per Raggiungere la destinazione viene detto Metrica.
Mentre il Next Hop è il router al quale verrà inoltrato un pacchetto qualora non ci sia una connessione diretta.

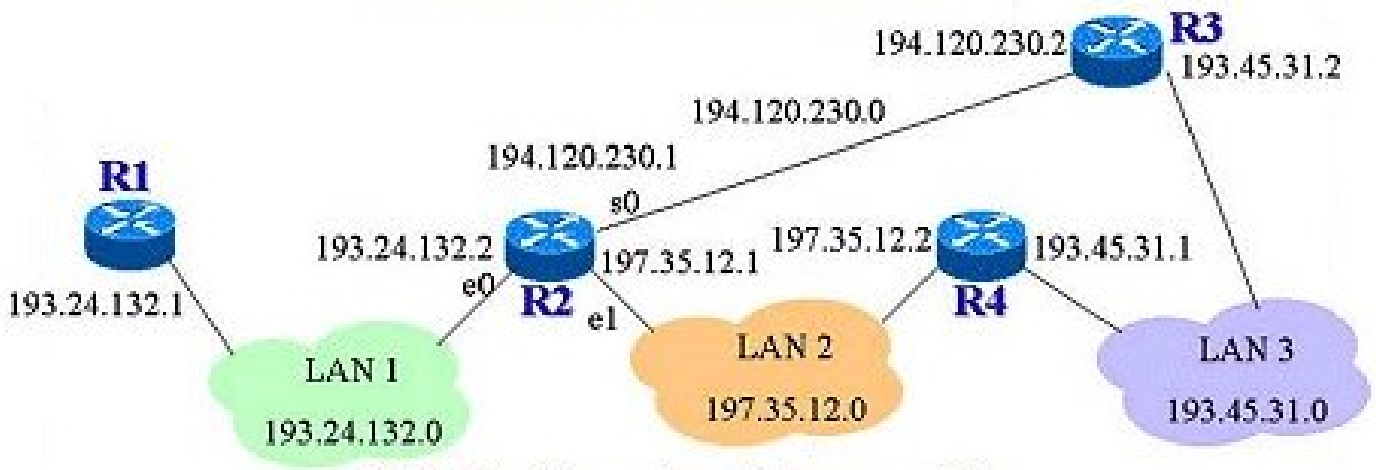
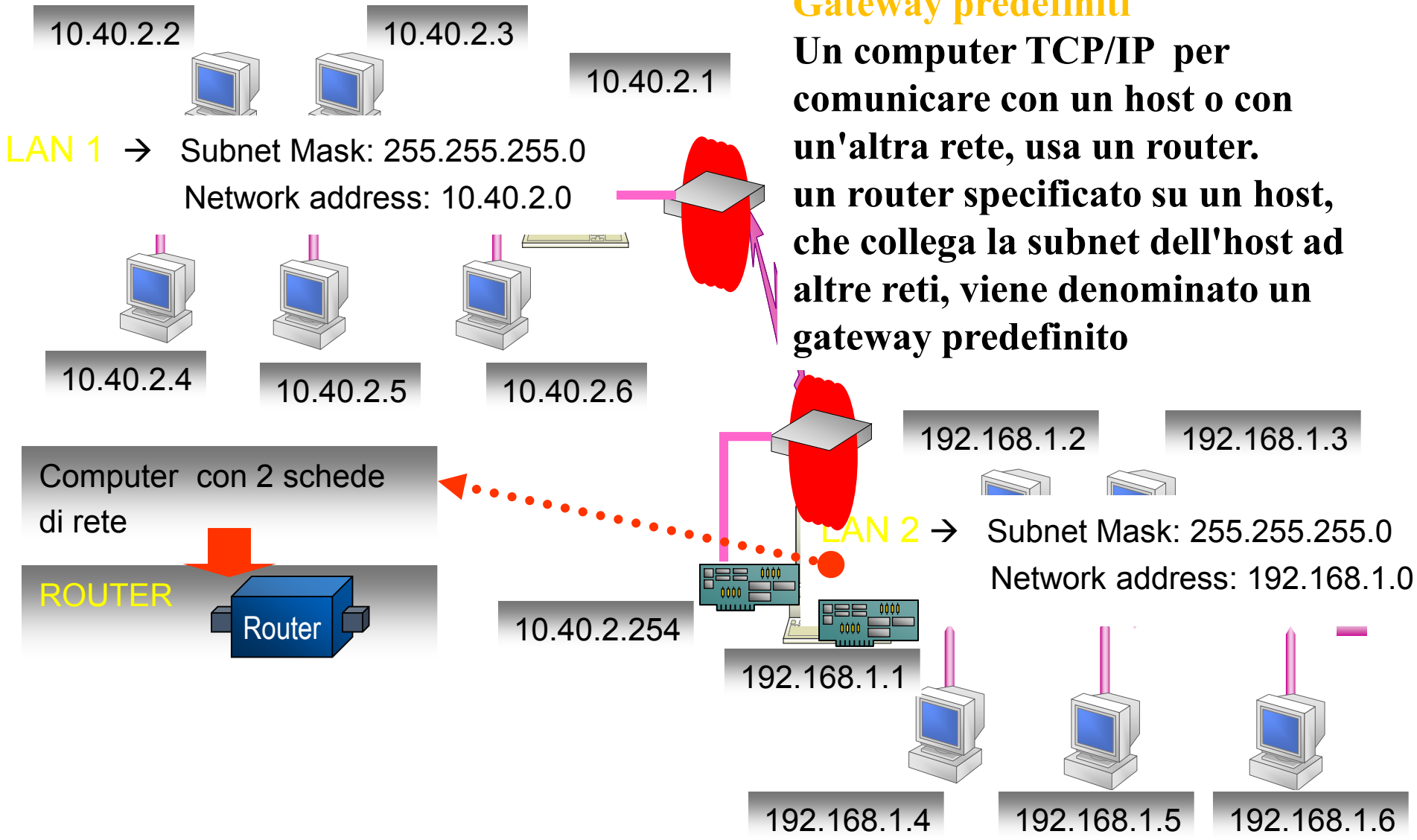


Tabella di routing del router R2

Network	Interface	Next Hop	Metric
193.24.132.0	Ethernet 0	———	0
197.35.12.0	Ethernet 1	———	0
195.45.31.0	Ethernet 1	197.35.12.2	1
195.45.31.0	Serial 0	194.120.230.2	1

Meccanismo di comunicazione tra reti diverse

Internetworking: come comunicano due reti differenti?



Gateway predefiniti

Un computer TCP/IP per comunicare con un host o con un'altra rete, usa un router.
un router specificato su un host, che collega la subnet dell'host ad altre reti, viene denominato un gateway predefinito

Il Router

Il default router è il router di riferimento al quale un host invia un pacchetto se non è in grado di trovare la destinazione direttamente sulla propria rete.

Il default router viene a volte indicato come **default gateway** o semplicemente come **gateway**.

Chiamiamo **Sistema Autonomo** (Autonomous System, AS), un gruppo di router e reti sotto il controllo di una singola e ben definita autorità amministrativa.

Il Router

Il router crea la sua tabella di routing tramite dei protocolli chiamati **Protocolli di Routing**.
Tali protocolli individuano i percorsi migliori per instradare i pacchetti utilizzando parametri diversi.
In genere i protocolli di routing si dividono in

- Distance Vector
- Link State

I protocolli *distance vector* ricevono e mandano informazioni per creare le tabelle di routing solo ai router adiacenti mentre i *link state* le mandano a tutti i router del proprio sistema autonomo.

Il Router

Interior Gateway Protocol(IGP): Per instradare pacchetti tra router all'interno di uno stesso AS (IGP),

Exterior Gateway Protocol (EGP): Per router che collegano tra loro più AS

Il Router

Protocolli interni al sistema autonomo (IGP)

- Protocolli Distance Vector (o di Bellman-Ford)
  - RIP Routing Information Protocol
  - IGRP Interior Gateway Routing Protocol
- Protocolli Link State
  - IS-IS Intermediate System to Intermediate System
  - OSPF Open Shortest Path First
- Protocolli ibridi
  - EIGRP Enhanced Interior Gateway Routing Protocol

Protocolli esterni al sistema autonomo (EGP)

- EGP Exterior Gateway Protocol, obsoleto
- BGP Border Gateway Protocol

Il protocollo NAT

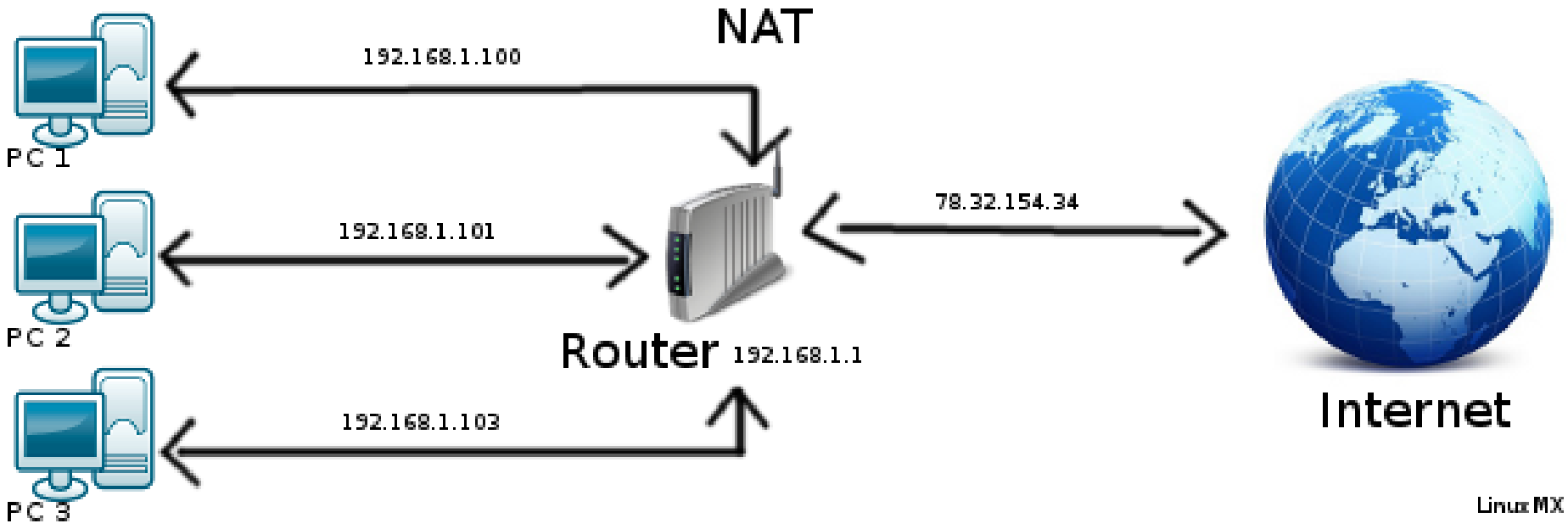
NAT Network address translation è un protocollo che consente di modificare l'indirizzo IP dei pacchetti in transito su apparati attivi di una rete.

La necessità del NAT nasce dal fatto che gli indirizzi IP pubblici sono andati ad esaurimento, tramite il meccanismo di NAT è possibile attribuire ad host di una LAN indirizzi IP privati e far si che in uscita dal delfault router cambino indirizzo con un IP pubblico (ad esempio)

Il protocollo NAT

Il NAT utilizza un gateway con almeno un'interfaccia connessa alla rete interna e almeno un'interfaccia di rete connessa alla rete esterna.

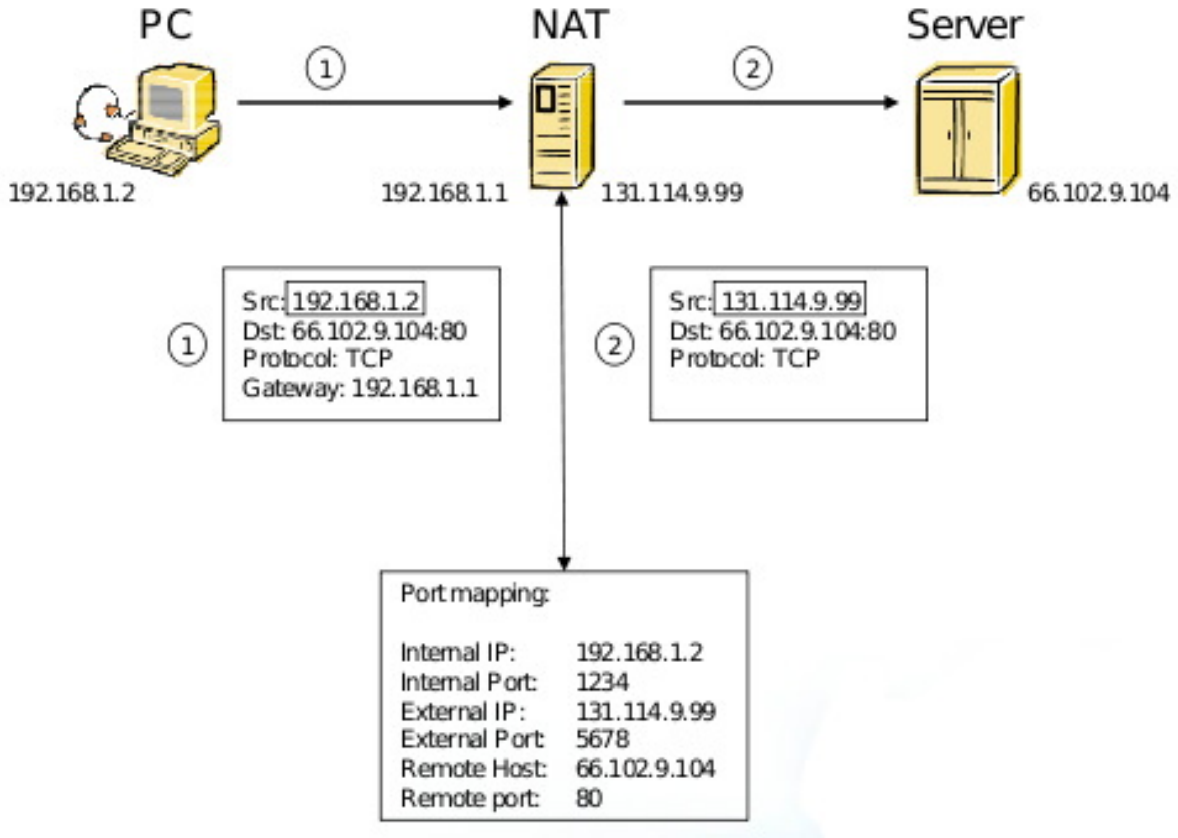
Con questa tecnica tutti i dispositivi connessi alla LAN potranno accedere a Internet utilizzando, e quindi “consumando”, un singolo indirizzo IP pubblico.



Il protocollo NAT

Il gateway lavora da Server NAT effettuando una traduzione degli indirizzi IP dei pacchetti in transito attraverso il router stesso:

- Quando un terminale della rete interna effettua una richiesta verso Internet, l'indirizzo IP di partenza risultante sarà quello, pubblico, del gateway stesso e non quello privato del dispositivo che effettua la richiesta;
- Per i pacchetti in ingresso il gateway si occupa di reindirizzare il traffico verso i dispositivi di destinazione appartenenti alla rete modificando l'IP di destinazione di conseguenza.



Il protocollo DHCP

Dynamic Host Configuration Protocol (DHCP) è un protocolli di livello rete che assegna in maniera automatica indirizzi IP ad host che stanno sulla sua rete fisica e che ne fanno richiesta.

Il DHCP oltre ad assegnare l'inidrizzo IP, comunica all'host la sua subnet mask, il default gateway, e il DNS (che vedremo successivamente)

Può dare altre istruzioni all'host.

Il protocollo DHCP: Indirizzi Dinamici

Il protocllo DHCP può assegnare indirizzi IP in vari modi

In maniera Dinamica:

Il server DHCP dispone di un range di indirizzi ad esempio

192.168.0.1 – 192.168.0.253

Il primo host che fa richiesta prenderà uno degli IP liberi e così via fino ad esaurimento.

Quando un host viene spento o decide di rilasciare l'IP assegnatogli questo disponibile e riassegnabile dal server DHCP

Il protocollo DHCP: Indirizzi Statici

Il protocollo DHCP può rilasciare indirizzi IP in maniera statica.

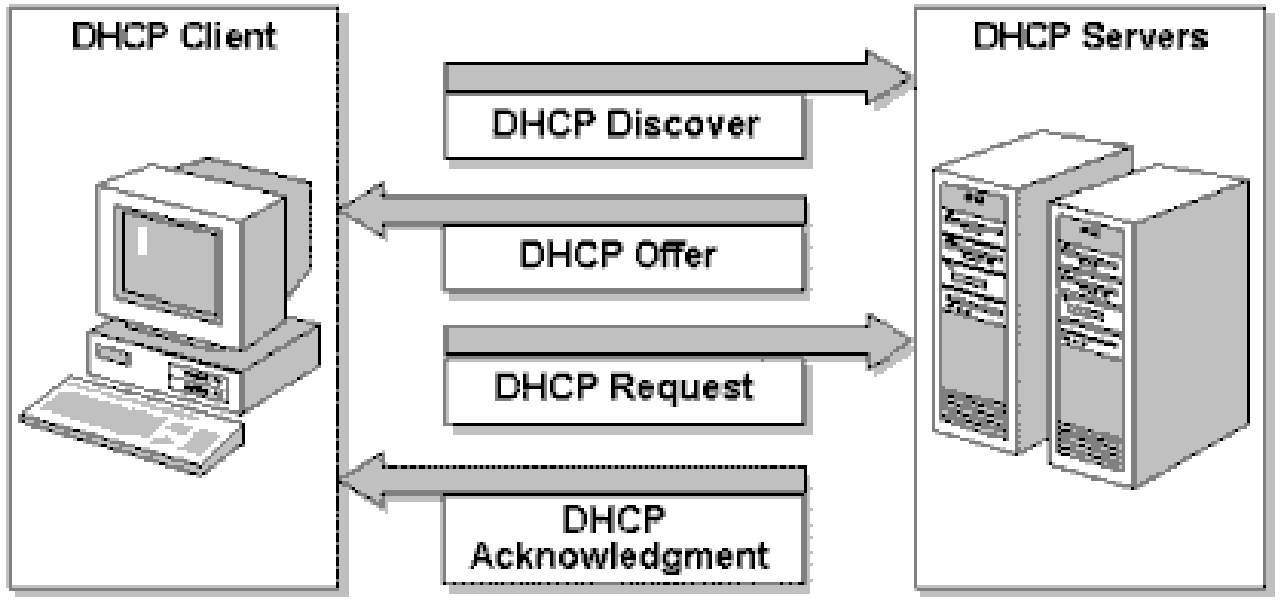
Questo viene fatto mantenendo all'interno del server una tabella MACADDRESS - > IP assegnato

In questo caso solo gli Host il cui indirizzio MAC è incluso nella tabella potranno ottenere un indirizzo IP dal server.

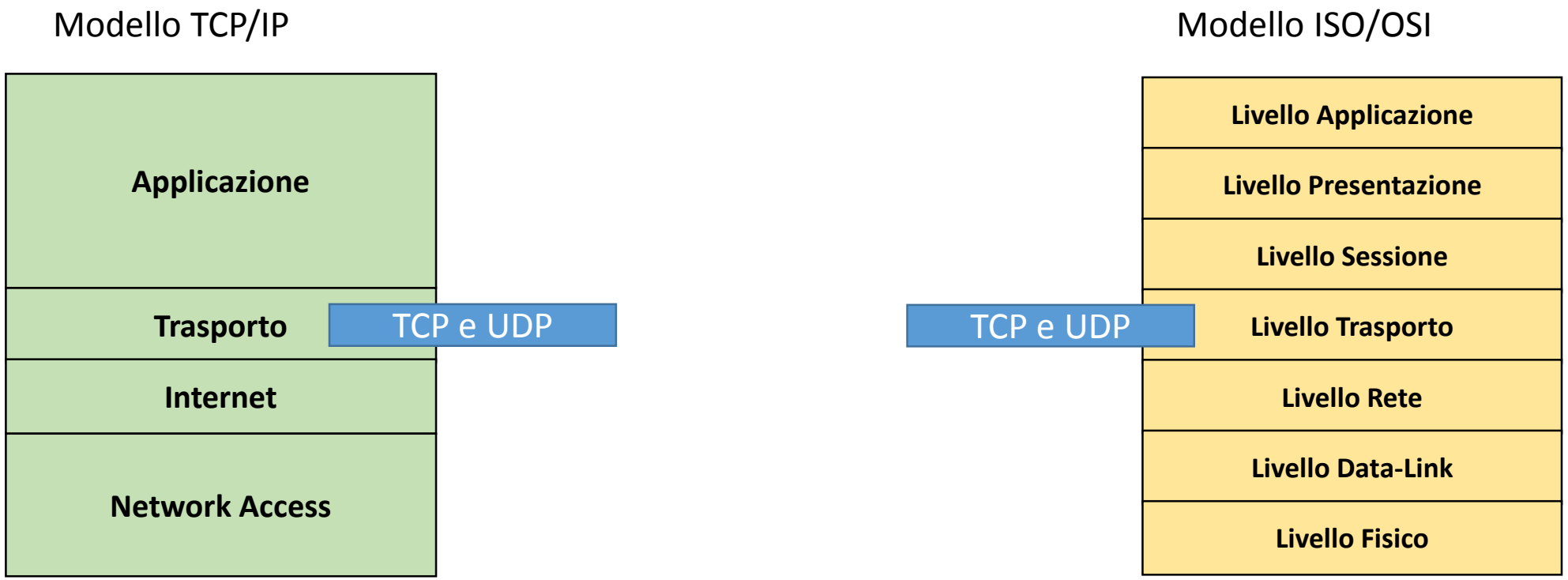
Il protocollo DHCP

Dinamica in vari step:

- L'host, privo di IP, manda un messaggio di discovery in broardcast per individuare se c'è un server DHCP.
- Il serve DHCP intercetta la richiesta e risponde al client con l'offerta di un IP
- Il client accetta l'IP
- Il server risponde un messaggio di conferma



Livelli trasporto



Livelli trasporto

Trasporto: al di sopra di IP crea una connessione end to end (canale virtuale nonostante la divisione in pacchetti) tra applicazione sorgente e destinazione

- **TCP** controlla la corretta trasmissione dei dati sotto forma di pacchetti, occupandosi dell'eventuale ritrasmissione di pacchetti persi (Protocollo connesso)
- **UDP**(USER DATA PROTOCOL): non garantisce la corretta trasmissione dei pacchetti perché non usa i pesanti meccanismi di controllo del TCP: meno affidabile, più efficiente (protocollo non connesso)

Il protocollo TCP

- Fu progettato esplicitamente per fornire un flusso affidabile end-to-end a partire da un internet inaffidabile
- Ogni macchina che supporta TCP possiede un'entità di trasporto TCP che gestisce i flussi di dati TCP e si interfaccia col livello IP
- Un'entità TCP riceve flussi di dati dai processi locali, li spezza in unità larghe al più 64 KB (ma generalmente di circa 1500 byte) e spedisce queste unità come datagram IP separate
- Ogni datagram che arriva al destinatario viene passato all'entità TCP che ricostruisce il flusso originario dei dati
- Il livello IP non fornisce alcuna garanzia sulla consegna corretta dei datagram: quindi è compito di TCP ritrasmetterli quando necessario

Il protocollo TCP

- Il servizio di TCP si ottiene mediante la creazione, da parte dell'utente e del ricevente, di punti di accesso (**socket**)
- Ogni socket è caratterizzato da un identificatore (indirizzo), consistente nell'indirizzo IP dell'host, e di un numero di 16 bit locale all'host, detto **porta**
- Una porta è una Transport Service Access Point (TSAP)
- Un socket può essere utilizzato contemporaneamente da più connessioni
- Una connessione è caratterizzata dai socket degli interlocutori, cioè dalla coppia (s1, s2)
- Le porte inferiori alla 256 sono chiamate **porte ben note**, e vengono usate per servizi standard
- Ad es., nell'ambito di un processo di scambio file (FTP) TCP usa la porta 21, per il login remoto (TELNET) usa la porta 23

Il protocollo TCP

- TCP trasferisce flussi di dati e non di messaggi. Ovvero TCP non ha idea del significato dei byte trasmessi, e di come vanno letti
- Quando un processo passa dati a TCP, questi potrebbe spedirli immediatamente oppure salvarli in un buffer per un invio successivo (magari insieme ad altri dati)
- E' possibile forzare l'invio immediato dei dati usando il flag PUSH
- Dati urgenti: vengono inviati in seguito all'utilizzo del flag URGENT

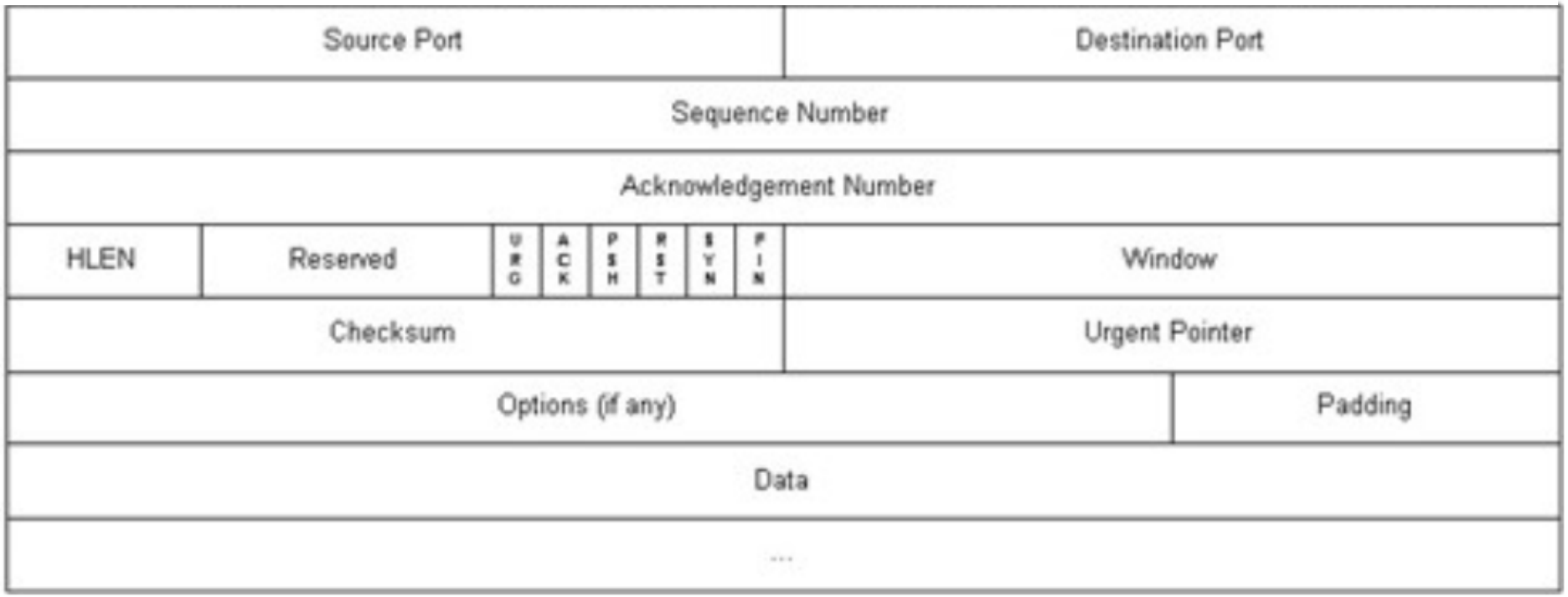
Il protocollo TCP

- Le entità TCP mittente e ricevente si scambiano dati sotto forma di segmenti
- Un segmento consiste in un preambolo fisso di 20 byte (più alcune parti opzionali) seguito da 0 o più byte di dati
- Il software TCP decide la dimensione dei segmenti
- Limite 1: ogni segmento, preambolo incluso, deve entrare in un pacchetto IP di 65536 byte
- Limite 2: ogni rete possiede un Maximum Transfer Unit (MTU, lungo generalmente poche migliaia di byte) e ogni segmento deve entrare in un MTU
- Un segmento può arrivare ad una rete con un MTU più piccolo della dimensione del segmento: in questo caso il segmento viene frammentato dal router di confine della rete

Il protocollo TCP

- Ogni byte di una connessione TCP possiede un proprio **numero di sequenza**
- Al momento di trasmettere un segmento, il mittente inizializza un timer
- Quando il segmento arriva a destinazione, il ricevente spedisce indietro un segmento che contiene un numero di **ack** (conferma di ricezione) uguale al successivo numero di sequenza che attende di ricevere
- Se il timer del mittente scade prima che il messaggio sia ricevuto, il segmento viene ritrasmesso

Header del protocollo TCP



Source port,destination port: identificano gli end point (locali ai due host) della connessione. Essi, assieme ai corrispondenti numeri IP, formano i due TSAP.
Sequence number: il numero d'ordine del primo byte contenuto nel campo dati.
Ack. Number: il numero d'ordine del prossimo byte aspettato.
TCP header length: quante parole di 32 bit ci sono nell'header (necessario perché il campo options è di dimensione variabile).
URG: 1 se urgent pointer è usato, 0 altrimenti.
ACK: 1 se l'ack number è valido (cioè se si convoglia un ack), 0 altrimenti.

Il protocollo TCP

Gli indirizzi del livello trasporto sono le porte.

La porta è un numero intero che indirizza un servizio in ascolto.

La scrittura

192.168.1.1:8080

Sta ad indirizzare la porta TCP 8080 sull'host con indirizzo IP 192.168.1.1

Il protocollo TCP

Ci sono due fondamentali approcci per l'assegnazione delle porte, usando:

Central Authority: due computers che devono interoperare tra di loro, si accordano per permettere ad un'autorità centrale di assegnare i numeri di porta (*Well-known ports*) che necessitano e di pubblicare la lista di tutte le assegnazioni (*Universal assignment*). Il software che gestisce le porte sarà realizzato in base a tale lista.

Dynamic Binding: in questo approccio le porte non sono universalmente conosciute; infatti, se un programma necessita di una porta, è il software di rete ad assegnargliela. Per sapere la porta corrente assegnata su un altro computer, è necessario inviargli una richiesta del numero di porta assegnata al servizio di interesse.

Il protocollo TCP

Decimal	Keyword	UNIX Keyword	Description
7	ECHO	echo	Echo
9	DISCARD	discard	Discard
11	USERS	systat	Active Users
20	FTP-DATA	ftp-data	File Transfer Protocol (data)
21	FTP	ftp	File Transfer Protocol
23	TELNET	telnet	Terminal connection
25	SMTP	smtp	Simple Mail Transport Protocol
42	NAMESERVER	name	Host Name Server
43	NICNAME	whois	Who is
53	DOMAIN	nameserver	Domain Name Server

Tabella well-Know port TCP

Il protocollo TCP

Le porte del TCP sono molto più complesse rispetto a quelle dell'UDP, perchè un dato numero di porta non corrisponde ad un singolo oggetto. Infatti nel TCP gli oggetti da identificare sono delle connessioni di circuito virtuali tra due programmi applicativi, e non delle particolari porte.
Il TCP usa la connessione, e non la porta di protocollo, come sua fondamentale astrazione; le connessioni sono identificate da una coppia di **end points**, ognuno dei quali è costituito da due interi **host,port**, dove l'*host*è l'indirizzo IP dell'host e *port*è il numero di porta TCP su quell'host (per esempio: l'end point **128.10.2.3,25** specifica la porta 25 sulla macchina di indirizzo 128.10.2.3).
Poichè il TCP identifica una connessione con una coppia di valori, uno dato numero di porta può essere condiviso da più connessioni su una stessa macchina, senza che si crei ambiguità. Perciò la macchina identificata da **128.10.2.3,53** può comunicare simultaneamente con le macchine identificate da **128.2.254.139,1184** e **128.9.0.32,1184**.
Si possono così creare servizi concorrenti con connessioni multiple simultanee, senza dover riservare un numero di porta locale per ogni connessione. Per esempio, alcuni sistemi forniscono un accesso concorrente al loro servizio di posta elettronica, permettendo a più utenti di spedire un E-mail contemporaneamente.

Il protocollo UDP

Lo User Datagram Protocol (UDP) è definito in RFC 768

- UDP è un servizio del livello di trasporto di Internet
- UDP è un servizio senza connessione
- UDP non è un protocollo affidabile
- UDP si basa sul protocollo di rete IP
- UDP offre un servizio del tipo best effort

Il protocollo UDP

Il servizio UDP offre i seguenti vantaggi:

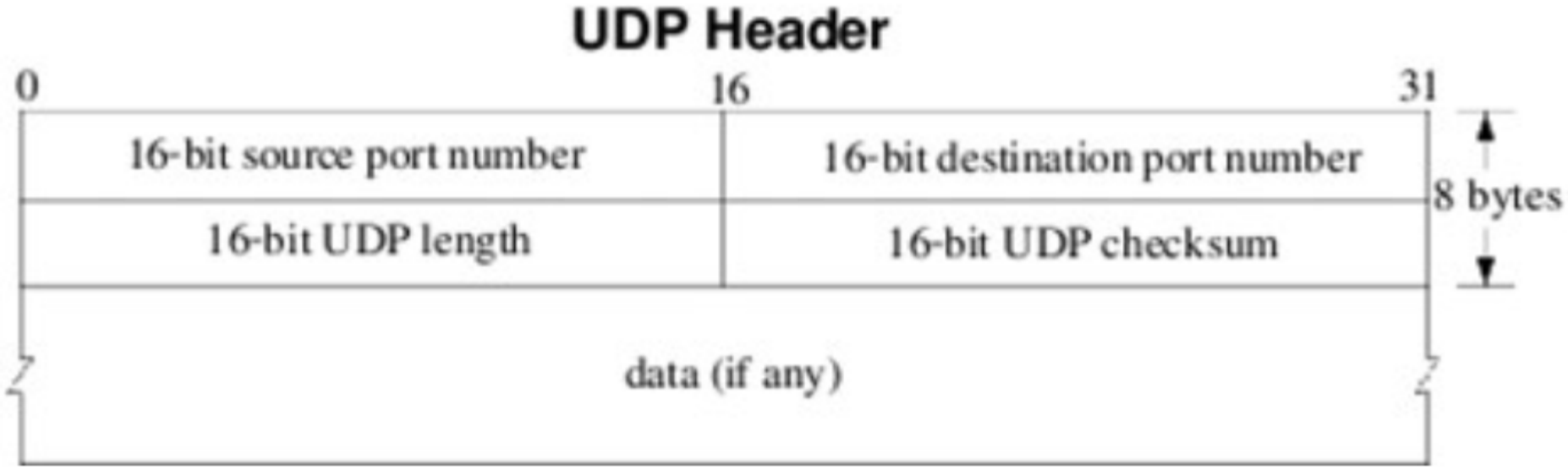
- non viene creata alcuna connessione
  - un messaggio viene inviato direttamente al nodo senza scambio preliminare di pacchetti per sincronizzare i due partecipanti alla comunicazione
  - quindi l'UDP non introduce nessun ritardo per impostare la comunicazione

- nessuno stato della connessione
  - non dovendo memorizzare informazioni per la connessione, un server UDP può supportare un numero maggiore di client attivi

- poco sovraccarico dovuto alla dimensione dell'intestazione
  - essendo minimale, di soli 8 byte, l'intestazione UDP introduce un aggravio nel consumo di banda che è solitamente trascurabile

- – controllo di livello applicativo più fine
  - i messaggi vengono inoltrati non appena richiesto di farlo
  - la mancanza di controllo di flusso e di congestione permette all'applicazione di controllare quando e con che ritmo inviare i messaggi

Il protocollo UDP



Il segmento UDP è composto da due parti: l'intestazione ed il corpo:

- Il corpo contiene i dati ed ha una lunghezza massima teorica di 65535 byte
- L'intestazione è composta da quattro campi, ciascuno di 16 bit

Il protocollo UDP

Per verificare l'integrità di un segmento, il protocollo UDP calcola un valore hash, detto checksum, a partire dal contenuto completo del segmento stesso.
Il checksum viene calcolato sia sui dati che sull'intestazione.
Il checksum è un valore hash:

- piccole variazioni nel contenuto del segmento modificano sensibilmente il valore di checksum

- il valore di checksum permette di controllare la presenza di errori di trasmissione

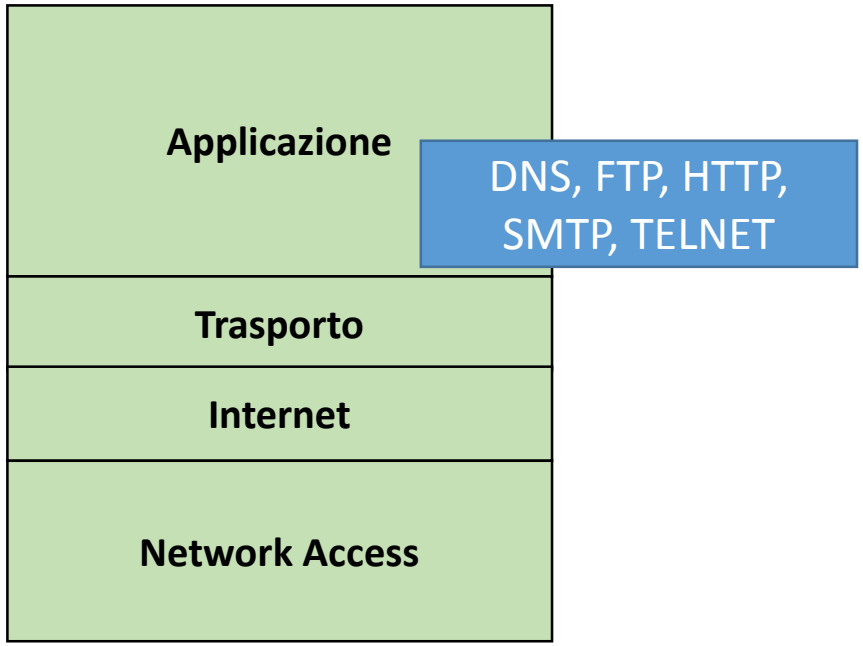
Un valore di checksum corretto non significa che il pacchetto sia integro, ma piuttosto che il pacchetto ha una probabilità insignificante di essere errato.
Il controllo di integrità confronta il valore di checksum calcolato dal trasmittente con quello calcolato dal ricevente

Il protocollo UDP

Tabella porte well-know UDP			
Decimal	**Keyword**	**UNIX Keyword**	**Description**
7	ECHO	echo	Echo
9	DISCARD	discard	Discard
11	USERS	systat	Active Users
42	NAMESERVER	name	Host Name Server
43	NICNAME	whois	Who is
53	DOMAIN	nameserver	Domain Name Server
69	TFTP	tftp	Trivial File Transfer

Livelli Applicazione

Modello TCP/IP



Modello ISO/OSI

Livello Application

Protocolli di livello Application, poggiano sul trasporto e permettono il funzionamento delle diverse applicazioni su Internet.

Esempi:

HTTP su TCP, permette il funzionamento del web

SMTP su TCP, permette l'invio di posta elettronica

POP3 su TCP, permette la ricezione di posta elettronica

RTP su UDP, permette la trasmissione della TV su Internet

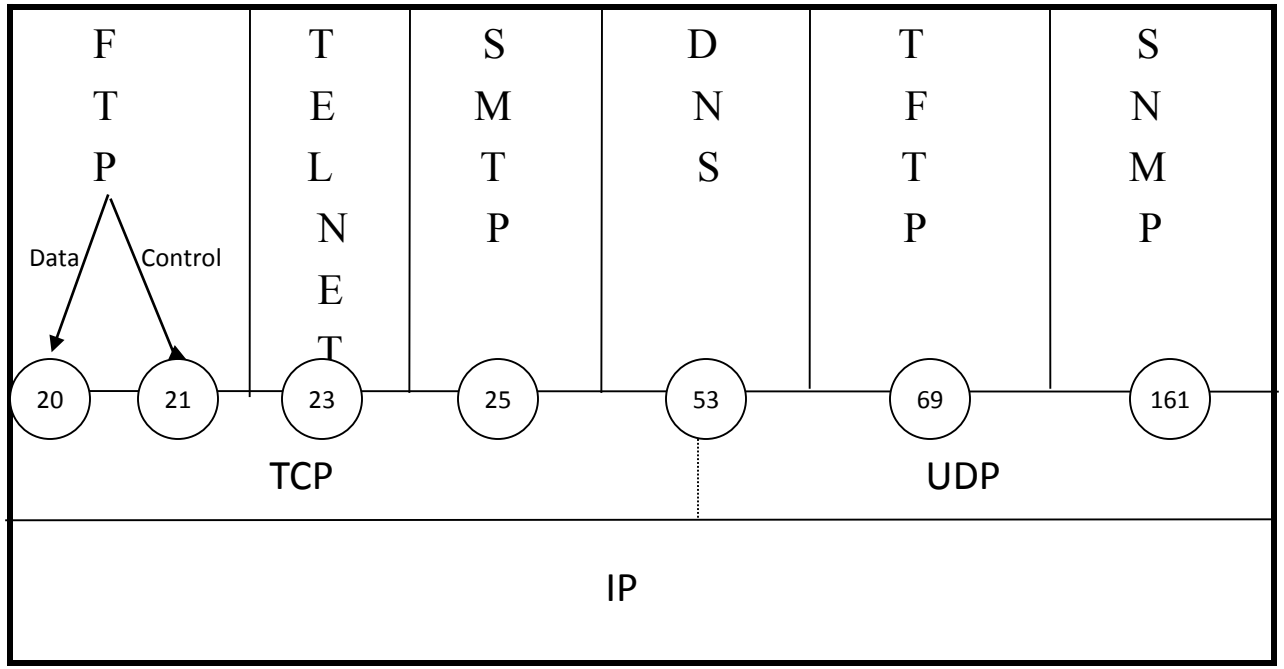
PROTOCOLLI DI TRASPORTO PER IL LIVELLO APPLICATION

Usano le porte per passare le informazioni agli strati superiori.
I protocolli di trasporto sono due :

-TCP;

-UDP.

TCP e' un protocollo orientato alla connessione,mentre UDP non e' orientato alla connessione.
Cio' vuol dire che TCP risulta piu' sicuro nel trasporto dei pacchetti,rispetto ad UDP.



Protocollo DNS

DNS (Domain Name System/ Server): è un servizio di livello applicazione che consente di tradurre i nomi simbolici in indirizzi IP.

Indirizzi IP solo poco adatti per essere memorizzati da utenti umani ⇒ per questo è stata introdotta la possibiltà di associare nomi simbolici agli hosts della rete, ad esempio **studenti.dipartimentomagrassi.unina2.it**

Indirizzi IP hanno lunghezza fissa e possono essere gestiti in modo semplice dai routers. Inoltre hanno struttura gerarchica in modo da favorire l'instradamento nei routers.

I nomini simbolici umanamente leggibili e a lunghezza variabile adatti per gli utenti

Protocollo DNS

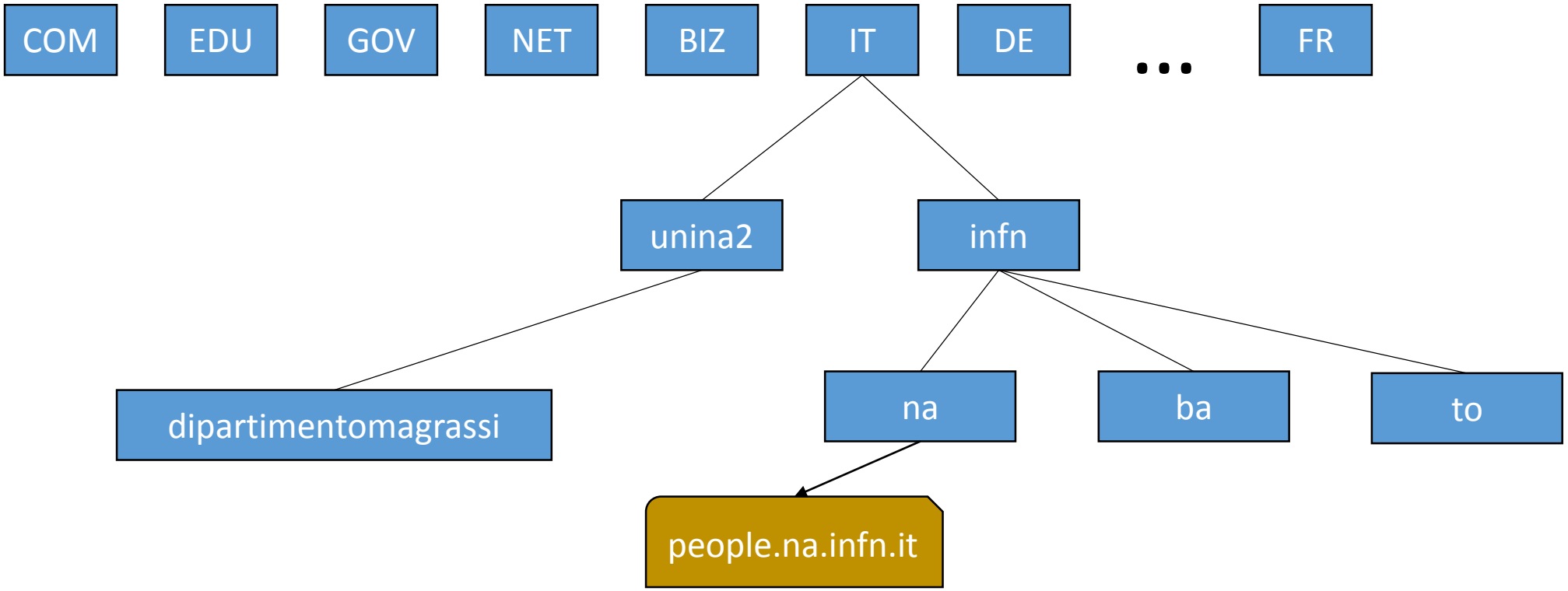
Al fine di rendere e user-friendly la tecnologia IP sono stati implementati alcuni servizi associano un nome leggibile, e più semplice da ricordare, a un indirizzo IP:

Il DNS è un servizio di directory utilizzato per la risoluzione dei nomi dei server da indirizzi logici e testuali (URL) in indirizzi IP.

Permette ad una qualsiasi entità di cambiare o riassegnare il proprio indirizzo IP, senza dover notificare tale cambiamento a nessuno, tranne che al proprio server DNS di riferimento.

Protocollo DNS

- Sistema gerarchico suddiviso in zone = sottoalberi
- Ad ogni zona corrisponde un name server (authoritative name server) che si occupa di quella parte della gerarchia



Domini Top Level

Sono stati individuati un insieme di domini di primo livello su base geografica o in base alla funzione

- **COM Organizzazioni commerciali**
- **EDU Istituzioni didattiche**
- **GOV Istituzioni statali (americane)**
- **MIL Gruppi militari (americani)**
- **NET Centri di supporto di Internet**
- **ORG Altre organizzazioni**
- **INT Organizzazioni internazionali**
- **IT, US, UK, DE, RU Codici di nazione (due lettere)**

Protocollo DNS

Ordinamento gerarchici I domini sono organizzati logicamente come un albero invertito

- **people.na.infn.it** – specifica completa della macchina che offre il servizio WEB del nostro corso presso l'istituto nazionale di fisica nucleare (INFN)
- **na.infn.it** – il dominio di Napoli dell'INFN
- **infn.it** – il dominio Nazionale dell'INFN
- **it** – sottodominio del dominio root

Suddivisione in zone, responsabilità delegate L'Internet Corporation for Assigned Names and Numbers (ICANN) sovraintende agli assegnamenti dei nomi di dominio

Regole sintattiche

- L’intero spazio dei nomi è rappresentato come una zona senza nome
- Le etichette dei vari livelli gerarchici sono separate con un “.”
- Non c’è differenza fra maiuscole e minuscole I livelli gerarchici sono ordinati da destra a sinistra
- il primo livello in genere è omesso (Es. dipartimentomagressi.unina2.IT.)

Name Server Locale

In Name server Locale è Associato ad un ad una organizzazione (università, dipartimento, industria,…).

contiene le associazioni (nomeindirizzo IP) per tutti gli host della organizzazione

la ricerca dell'inizio IP associato ad un nome simbolico inizia sempre dela name server locale.

se il name server locale non riesce a risolvere il nome, inoltra la richiesta ad un root name server

l'indirizzo IP del name server locale può essere impostato da ogni host

Root Name Server

interrogato dai name servers locali

ne esistono un numero limitato su INTERNET

modo di operare:

- se riesce a risolvere il nome, lo invia al name server locale che lo inoltra all'host che aveva fatto richiesta.
- se non risolve il nome, lo invia ad un altro name server che possiede il mapping ricercato o conosce l'indirizzo IP di un altro DNS in grado di risolvere il nome

I ROOT NAME SERVER

- i.root-servers.net. 5d22h39m28s IN A 192.36.148.17
- e.root-servers.net. 5d22h39m28s IN A 192.203.230.10
- d.root-servers.net. 5d22h39m28s IN A 128.8.10.90
- a.root-servers.net. 5d22h39m28s IN A 198.41.0.4
- h.root-servers.net. 5d22h39m28s IN A 128.63.2.53
- c.root-servers.net. 5d22h39m28s IN A 192.33.4.12
- g.root-servers.net. 5d22h39m28s IN A 192.112.36.4
- f.root-servers.net. 5d22h39m28s IN A 192.5.5.241
- b.root-servers.net. 5d22h39m28s IN A 128.9.0.107
- j.root-servers.net. 5d22h39m28s IN A 192.58.128.30
- k.root-servers.net. 5d22h39m28s IN A 193.0.14.129
- l.root-servers.net. 5d22h39m28s IN A 198.32.64.12
- m.root-servers.net. 5d22h39m28s IN A 202.12.27.33

Interrogazioni Inverse

- **Utilizzata per recuperare il nome associato ad un indirizzo IP utilizzata da alcuni server per verificare la correttezza delle informazioni ottenute dal client**
- **Implementata come la ricerca di un nome tutti gli indirizzi IP sono rappresentati come nomi nel dominio in-addr.arpa**
- **Es. 192.168.203.2 2.203.168.192.in-addr.arpa**
- **I root name server mantengono un database di tutti gli indirizzi IP validi e dei name server che li possono risolvere**

Telnet

Telnet è un protocollo per la comunicazione tra sistemi indipendentemente dal sistema operativo e dall'hardware degli host in gioco.

Viene utilizzato per fornire all'utente sessioni **di login** remoto ad un host sulla rete.

- Telnet costruito su TCP/IP
- Connessione TCP con architettura client/server
- Gestione eterogeneità tramite interfaccia di terminale virtuale
- Client e Server negoziano le opzioni del collegamento
- Protocollo prevede l'autenticazione a mezzo di login e password

SSH

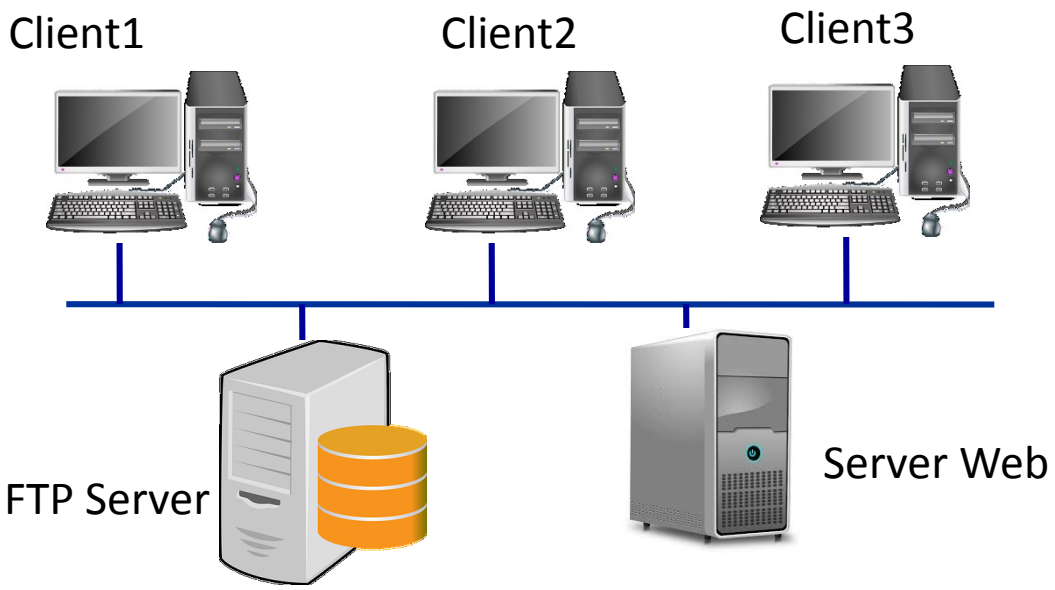
Il protocollo SSH (Secure SHell, shell sicura) è un protocollo che permette di stabilire una **sessione remota cifrata** tramite interfaccia a riga di comando con un altro host.

SSH fornisce una versione «sicura» del servizio di Telnet grazie al supporto di cifratura

FTP

File Transfer Protocol (FTP) è un protocollo per il trasferimento file di livello applicazione.

FTP utilizza un architettura client/server



FTP

- Con FTP permette di copiare file dal proprio PC o da un altro dispositivo in rete in un computer remoto (operazione di upload) e dal server remoto al proprio PC (operazione di download).

- Per eseguire queste operazioni un server FTP può richiedere un processo di autenticazione a mezzo di username e password.

- Questo al fine di identificare l'utente che tenta di eseguire un operazione di upload o download e verificare che abbia effettivamente i diritti di eseguire le operazioni richieste sullo specifico server.

- FTP consente altresì **l'accesso anonimo** per condividere in rete file di domino pubblico.

FTP e tftp

Nella implementazione del protocollo FTP tramite le porte 20 e 21, un client FTP comunica con il server FTP mediante un linguaggio vicino a quello naturale.

FTP usa TCP come protocollo di trasporto grazie al quale consente di avere più client connessi allo stesso server, nello stesso momento.

Comandi di trasferimento file

- put local-file [remote-file] memorizza un file locale sulla macchina remota
- get remote-file [local-file] trasferisce un file remoto sul disco locale
- mget e mput utilizzano metacaratteri nei nomi dei file
- altri comandi: help, dir, ls, cd, lcd, ...

tfpt (Trivial FTP) più semplice e con meno possibilità

- (uso di UDP)

SFTP ed SCP

Come nel caso dei protocolli di login esiste una versione sicura del FTP **chiama SSH File Transfer Protocol (SFTP)** essa rappresenta un protocollo di rete che prevede il trasferimento dei dati più funzionalità di manipolazione (rename, move, delete, crate directory). È tipicamente usato con il protocollo SSH-2 che utilizza un trasferimento dei file sicuro, anche se è utilizzabile con un qualsiasi altro protocollo.

SCP (Secure CoPy) è un protocollo per il solo trasferimento file da un computer locale a uno remoto in modalità sicura usando il protocollo Secure Shell (SSH).

Il termine SCP può riferirsi ad una delle due seguenti cose tra loro correlate: il protocollo SCP o il programma SCP.

HTTP

- HTTP é un protocollo client-server generico e stateless utilizzato per lo scambio di documenti ipertestuali, ma anche per una moltitudine di applicazioni, incluso name server e sistemi object-oriented distribuiti.
- Caratteristiche di HTTP sono
  - la negoziazione del formato di dati, per l'indipendenza del sistema dal formato di rappresentazione dei dati.
  - Specifiche di politiche di caching sofisticate a seconda del tipo di connessione
  - Specifiche di autenticazione dell'utente di varia sofisticazione.

HTTP

- Client-server
  - In HTTP esistono due ruoli specifici: il *client* attiva la connessione e richiede dei servizi. Il server accetta la connessione, nel caso identifica il richiedente, e risponde alla richiesta. Alla fine chiude la connessione.
- Protocollo generico
  - HTTP è indipendente dal formato dati con cui vengono trasmesse le risorse. Può funzionare per documenti HTML come per binari, eseguibili, oggetti distribuiti o altre strutture dati più o meno complicate.
- Statelessness
  - Il server non è tenuto a mantenere informazioni che persistano tra una connessione e la successiva sulla natura, identità e precedenti richieste di un client. Il client è tenuto a ricreare da zero il contesto necessario al server per rispondere.

HTTP

- HTTP è un protocollo di comunicazione piuttosto semplice, basato sulla comunicazione tra due applicazioni, il browser, che manda richieste di documenti, ed il server, che risponde.
- In realtà i ruoli sono un po' più precisi:
  - **Client**: un'applicazione che stabilisce una connessione HTTP, con lo scopo di mandare richieste.
  - **Server**: un'applicazione che accetta connessioni HTTP, e genera risposte

HTTP

- In generale un proxy si pone come intermediario tra client e server e decide se e come rispondere al client. I proxy sono trasparenti (non cambiano la risposta) o non trasparenti (possono cambiare la risposta)
- **Proxy trasparenti**
  - **Proxy di cache**: Richieste multiple agli stessi URL possono essere salvate in una locazione intermedia per una maggiore efficienza nella gestione delle risposte
  - **Proxy di filtro**: Esigenze di sicurezza o di controllo degli abusi di una rete possono richiedere l'effettiva esecuzione della richiesta solo in certi casi, e altrimenti la risposta con un generico messaggio di mancata autorizzazione.
- **Proxy non trasparenti**
  - Un proxy trasparente esegue tutte le richieste e fornisce tutte le risposte, ma in certi casi può convertire o modificare la risposta. Ad esempio fornire link a vocabolari, togliere i banner, convertire i formati ignoti, ecc.
  - Ad esempio, WBI di IBM (http://www.almaden.ibm.com/cs/wbi/)
  - http://www.unina2.it/index.php?option=com_content&view=article&id=186&Itemid=320

HTML

HTML è l'acronimo di **HyperText Markup Language** ed è il linguaggio col quale vengono create le pagine web. Si tratta di un linguaggio di pubblico dominio sviluppato in seno al **W3C**, ovvero il *World Wide Web Consotium*, cioè il consorzio che presiede allo sviluppo del web e dei linguaggi ad esso connessi.

Questo linguaggio è stato sviluppato da un ricercatore del CERN - *Tim Berners Lee* - verso la fine degli anni ottanta parallelamente alla definizione del protocollo HTTP.

Documento HTML

```
<!doctype html>
<html lang="it">
<head><title>Ciao Mondo!</title></head>
<body>
    <h1>Corso di Laurea in Tecniche di Radiologia Medica per Immagini e Radioterapia </h1>
    <p>SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI I</p>
</body>
</html>
```