Statistiche 2022

- Nella prima metà di 2021, Il 64% di tutto il traffico Internet era automatizzato (il 39% proveniva da bot cattivi e il 25% da bot buoni). Gli esseri umani hanno rappresentato il restante 36%.
- Nel primo trimestre del 2021, i dispositivi mobili (esclusi i tablet) hanno generato il 54.8% del traffico globale del sito web.

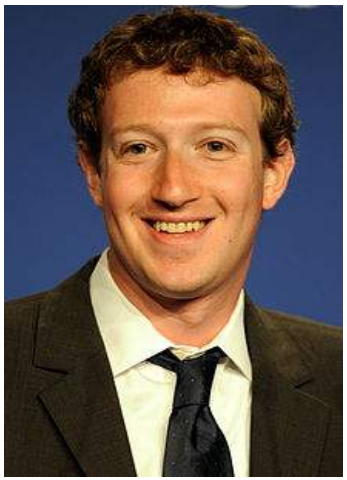
L'era dei social networks

- L'effetto combinato di due marcate tendenze:
  - Diffusione massiva di dispositivi cellulari
  - Incremento delle capacità computazionali sui dispositivi mobili
    - ✓CPU multicore
    - ✓GPU sempre più potenti
    - ✓Facilità di accesso a strumenti come GPS e fotocamera
    - ✓Ridotto consumo di energia (ARM)

  Ha portato ad una enorme diffusione delle tecnologie Internet in moltissimi ambiti
- Lo sviluppo di nuove tecnologie (AJAX, Javascript, HTML5) ha permesso di realizzare siti sempre più interattivi e dinamici, rendendo possibile l'avvento del Social Networking che pervade oggi la vita di molte persone e ci fornisce servizi dei quali non potremmo fare a meno

L'era dei Social Networks

Mark Zuckerberg, CEO di Facebook



- Nel febbraio del 2004 Mark Zuckerberg fonda facebook. Nel 2013 il suo patrimonio è stato stimato in 31.6 miliardi di dollari

Jack Dorsey, CEO di Twitter

- Twitter nasce nel luglio 2006 in modo più rocambolesco, sulle ceneri di una stat-up chiamata Odeo fondata da Noah Glass, Jack Dorsey, Evan Williams e Biz Stone. Twitter si caratterizza per l'invio di messaggi ("tweets") al massimo lunghi 140 caratteri – usati in media 34 - (estesi ora a 280 - usati in media 33). I messaggi sono raggruppati in hashtags (nomi preceduti da “#”) risposte agli utenti sono indicate col simbolo “@”)

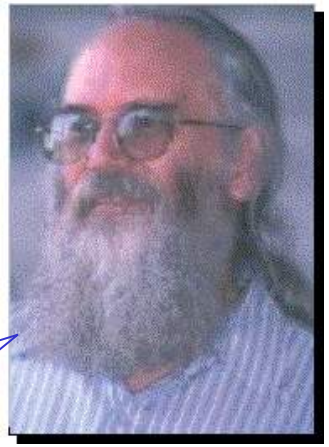
L'era dei Social Networks

- LinkedIn è un social network orientato all'occupazione professionale, nato nel 2002 e lanciato nel maggio 2003. Il sito è disponibile in 20 lingue, nel 2013 ha dichiarato 259 milioni di utenti in 200 paesi. Il CEO è Jeff Weiner.

- Instagram è un altro social network orientato allo scambio di immagini e video. Instagram è stato creato da Kevin Systrom e Mike Krieger e lanciato nell'Ottobre 2010. Anche Flickr usa l'hashtag per identificare utenti e foto. Nel 2012 Instagram è stata acquisita da Facebook ed è stata oggetto di una grossa polemica in rete per aver cambiato i termini del servizio, dichiarando di poter rivendere a terzi le immagini degli utenti senza richiesta preventiva di permesso, successivamente ritirato. E' in programma l'introduzione di annunci pubblicitari.

Internet: definizione

- Internet è una rete globale di reti che abilita i computer di ogni tipo a comunicare direttamente ed in modo trasparente, a condividere servizi attraverso gran parte del mondo.
- Essendo una infrastruttura di enorme importanza, capace di attivare così tante persone ed organizzazioni, costituisce anche una fonte condivisa e globale di informazioni, conoscenza e senso di collaborazione e cooperazione tra diverse e innumerevoli comunità.
- E' definita formalmente nell'RFC1122 (originariamente in RFC760)



Jon Postel, Internet Pioneer

August 6, 1943 October 16 1998

"Be liberal in what you accept, and conservative in what you send." -- jon

"Jon has been our North Star for decades ... He was the Internet's Boswell and its technical conscience." -- Vint Cerf

Internet: definizione

- L' Internet Protocol (IP) fornisce le funzioni necessarie per l'invio di un pacchetto di bit (chiamato Internet datagram) da una sorgente ad una destinazione utilizzando un sistema interconnesso di reti.
- Sorgente e destinazione sono due host (cioè qualsiasi computer: PC, MacIntosh, Workstation, Server, Mainframe) identificati ciascuno da un indirizzo a lunghezza fissa, denominato indirizzo IP.
- L'IP versione 4 fornisce anche i servizi di frammentazione e riassemblaggio di datagram, quando la trasmissione avviene attraverso reti con capacità di trasporto di pacchetti più piccola del pacchetto originale (dovuto alle diverse tecnologie di rete del passato). IP versione 6 abolisce questo comportamento.

Internet: definizione

- Le funzionalità dell'IP sono volutamente limitate alla trasmissione di datagram.
- L'IP è invocato dai protocolli host-to-host (a livello superiore di astrazione).
- L'IP invoca i protocolli di rete locali (a più basso livello di astrazione) per trasportare l'internet datagram al successivo gateway o host di destinazione

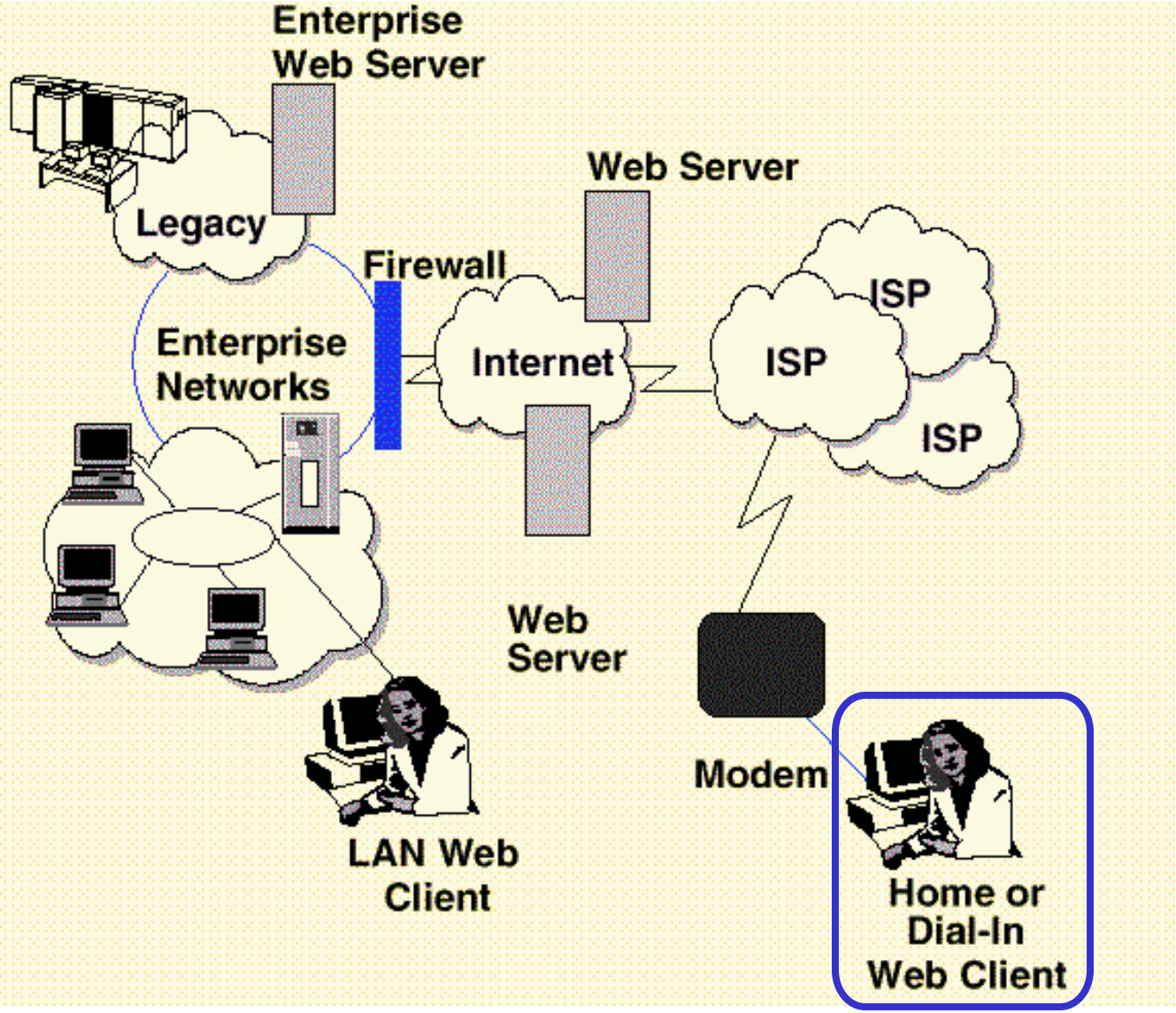
Internet: definizione

- I vari moduli internet usano gli indirizzi presenti nell'internet header per trasmettere i datagram internet verso le loro destinazioni.
- La selezione del cammino da seguire per la trasmissione è chiamato routing
- Il modello operativo prevede che un modulo internet risieda in ogni host impegnato in comunicazioni internet e in ogni gateway che interconnette delle reti.
- Questi moduli condividono delle regole comuni per interpretare i campi dell'indirizzo internet, per frammentare e riassemblare datagram.

Internet: definizione

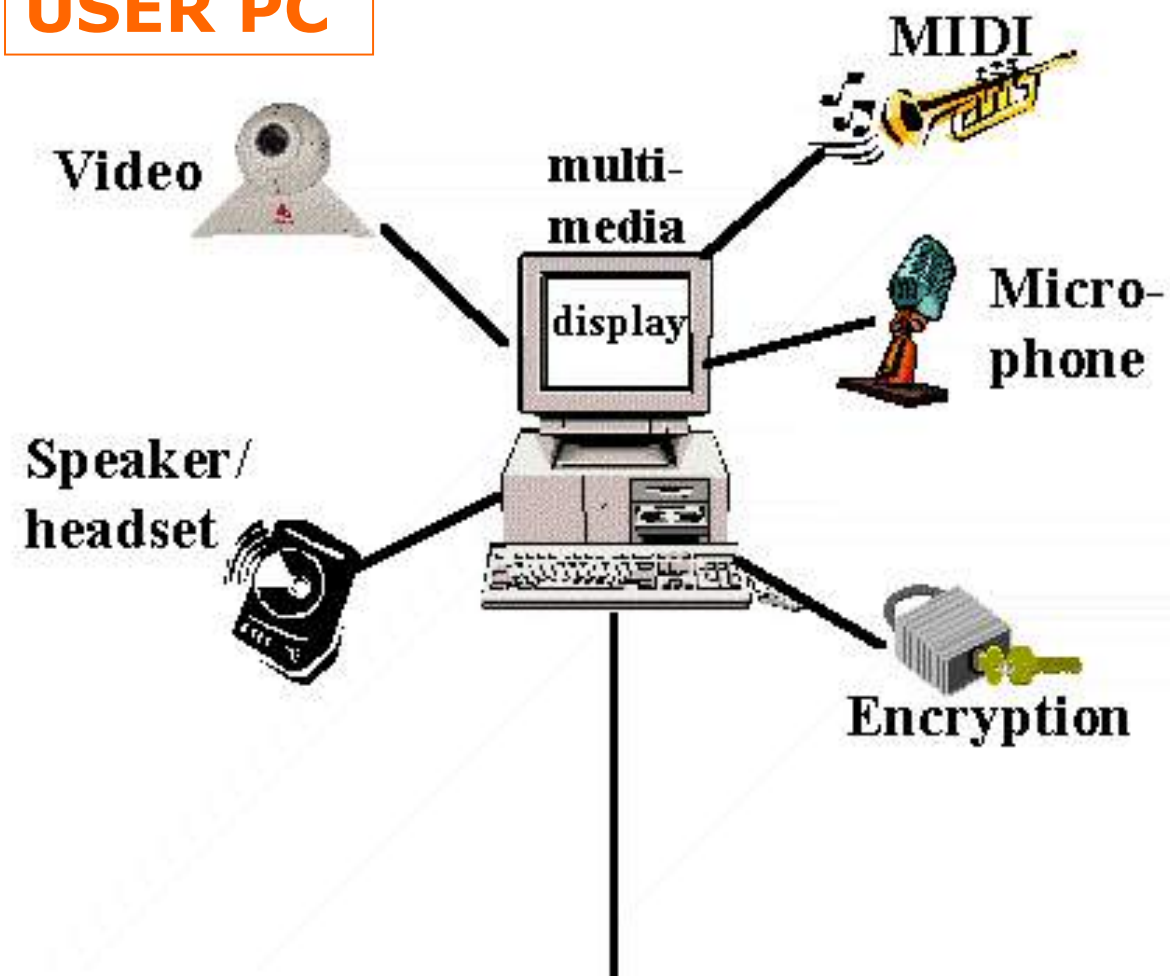
- Inoltre, in particolare i gateway, possiedono procedure per effettuare altre funzioni, in particolare le scelte di routing.
- Il routing è un processo dinamico, che tiene conto delle variazioni istantanee della rete, che viene eseguito avvalendosi dei protocolli di routing dinamici.
- L'IP tratta ogni internet datagram come entità completamente indipendente dagli altri internet datagram.
- Non esistono connessioni o circuiti virtuali

Elementi dell'infrastruttura



Elementi dell'infrastruttura

USER PC



Un PC o dispositivo mobile Multimediale equipaggiato per ricevere e inviare ogni tipo di audio e video:

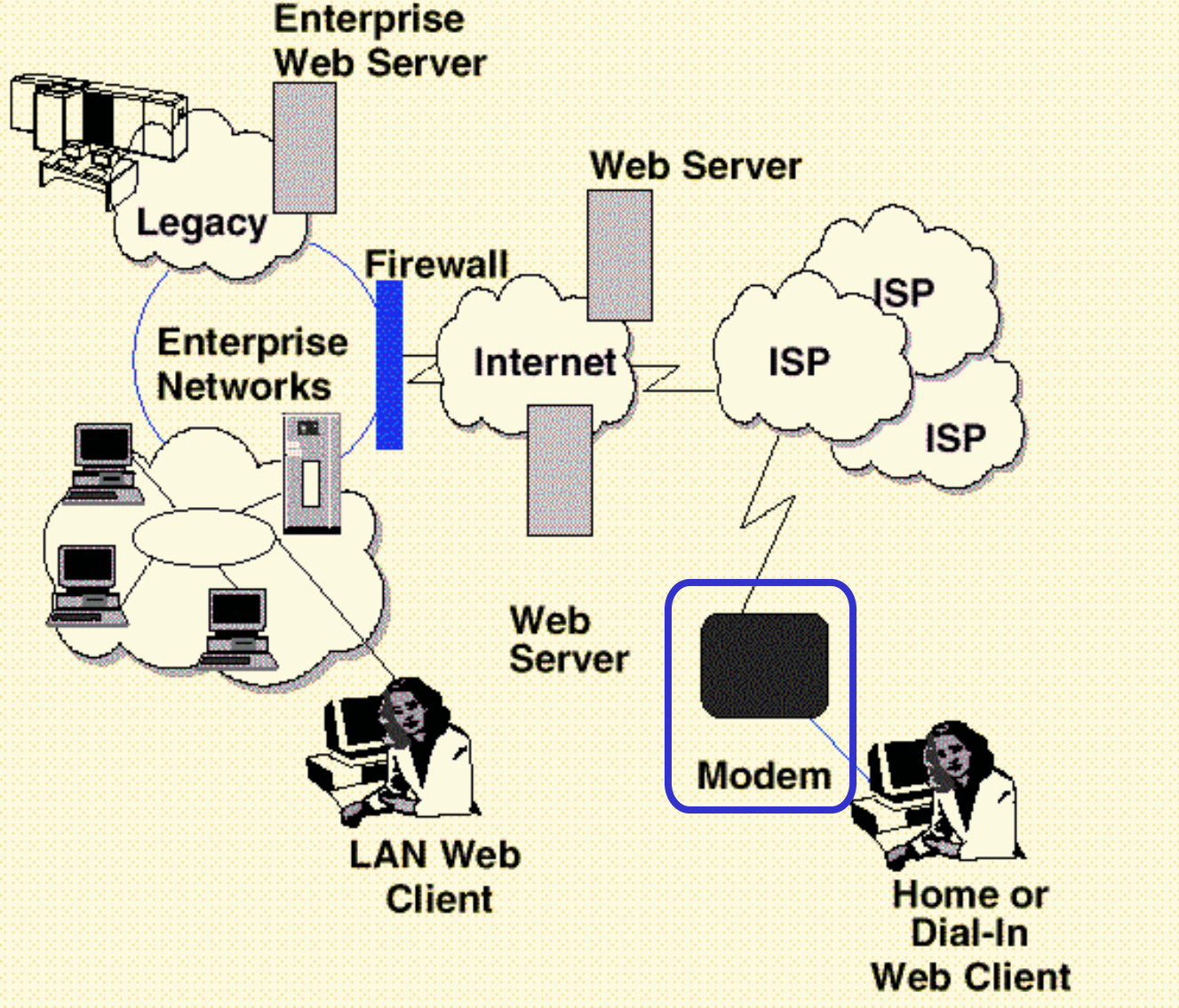
– Scheda audio, Microfono, Casse

– Video, Scheda Grafica (GPU)

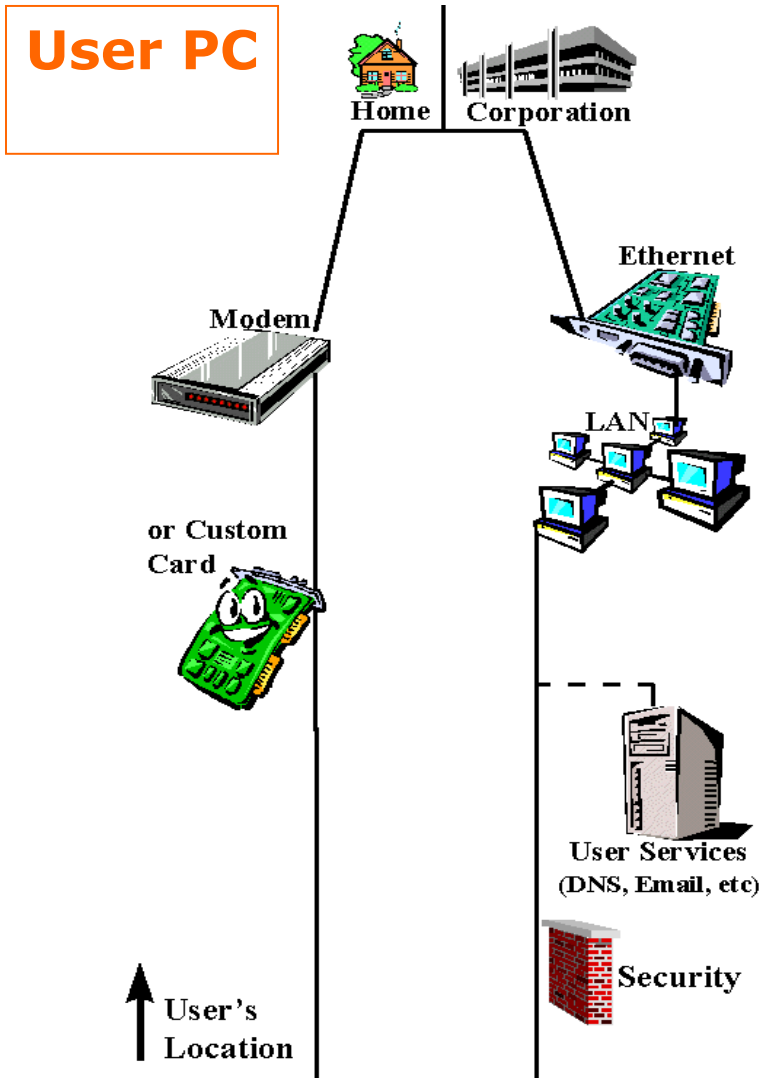
– Video camera, Webcam

– Riconoscitori Vocali

Elementi dell'infrastruttura



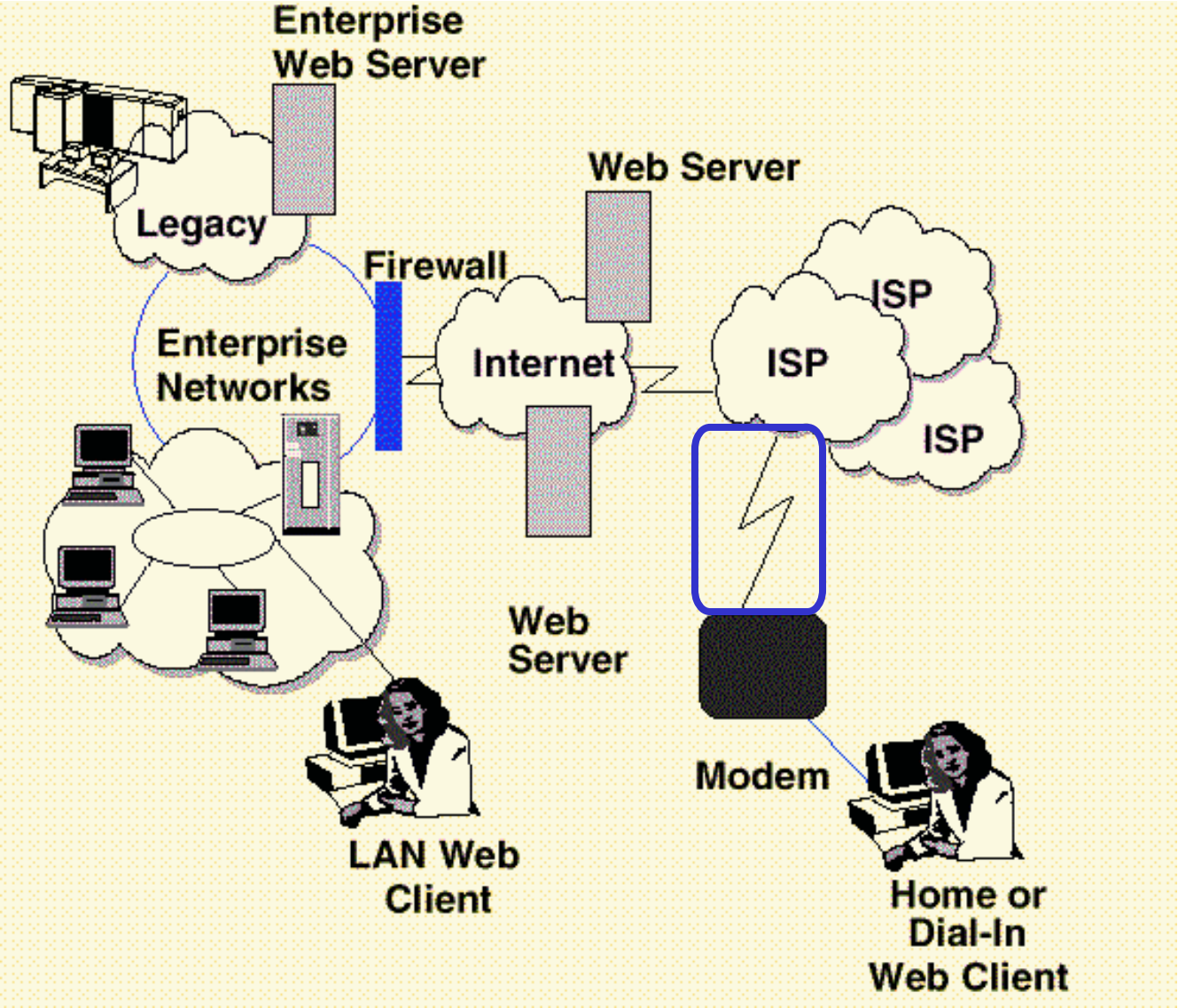
Elementi dell'infrastruttura



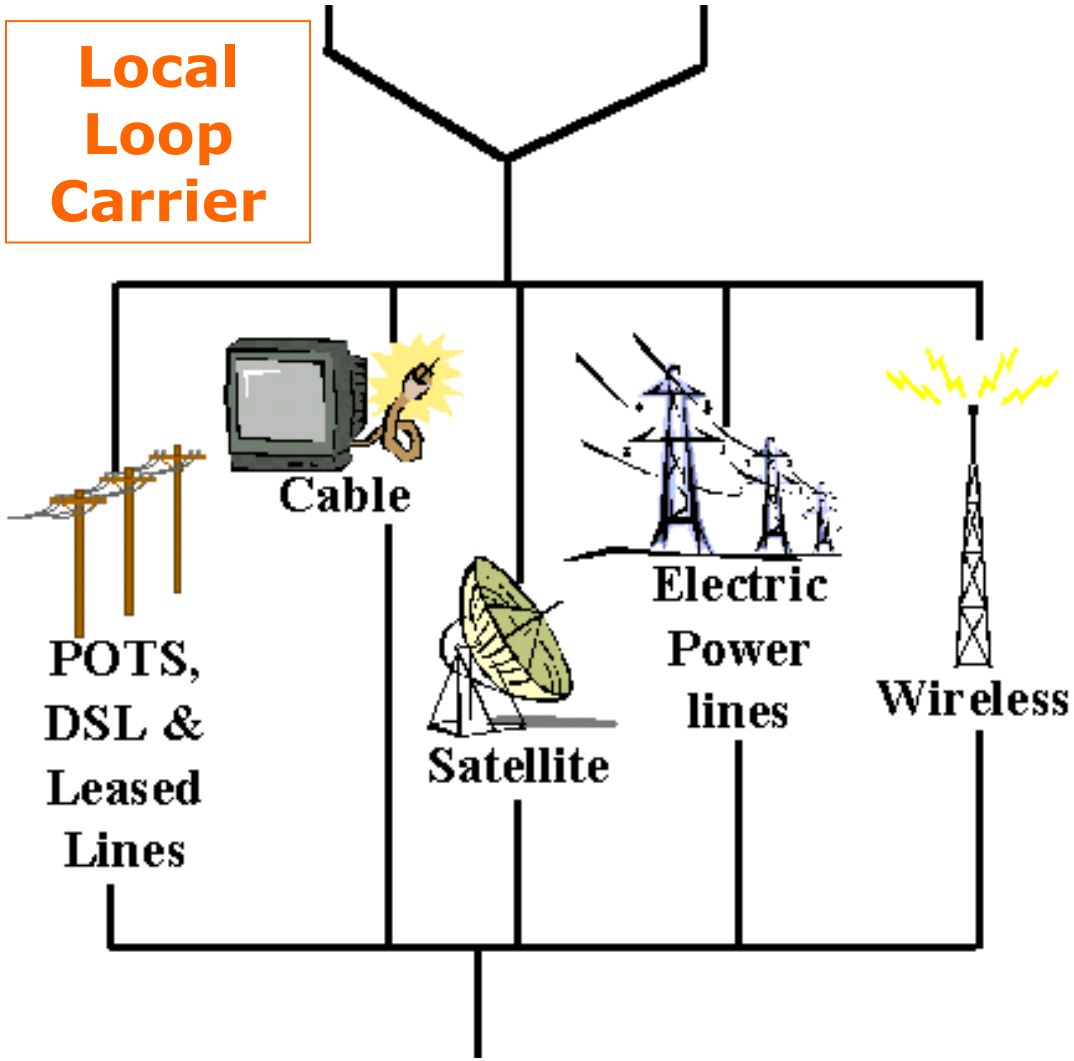
Sono gli apparati localizzati in casa dell'utente per connettere il PC dell'utente al "Local Loop" (Customer Premise Equipment - CPE)

- **Linea telefonica - Modem Analogico (v.90=56K)**
- **Linea telefonica -ISDN(128K)**
- **Linea telefonica - ADSL (ADSL Forum)**
- **Linea elettrica (1 MB) (Nortel)**
- **Satellite (400 Kb) (DirecPC)**
- **LAN - (3com)**
- **Router - (Cisco, Ascend, Bay Networks)**
- **Firewalls**

Elementi dell'infrastruttura



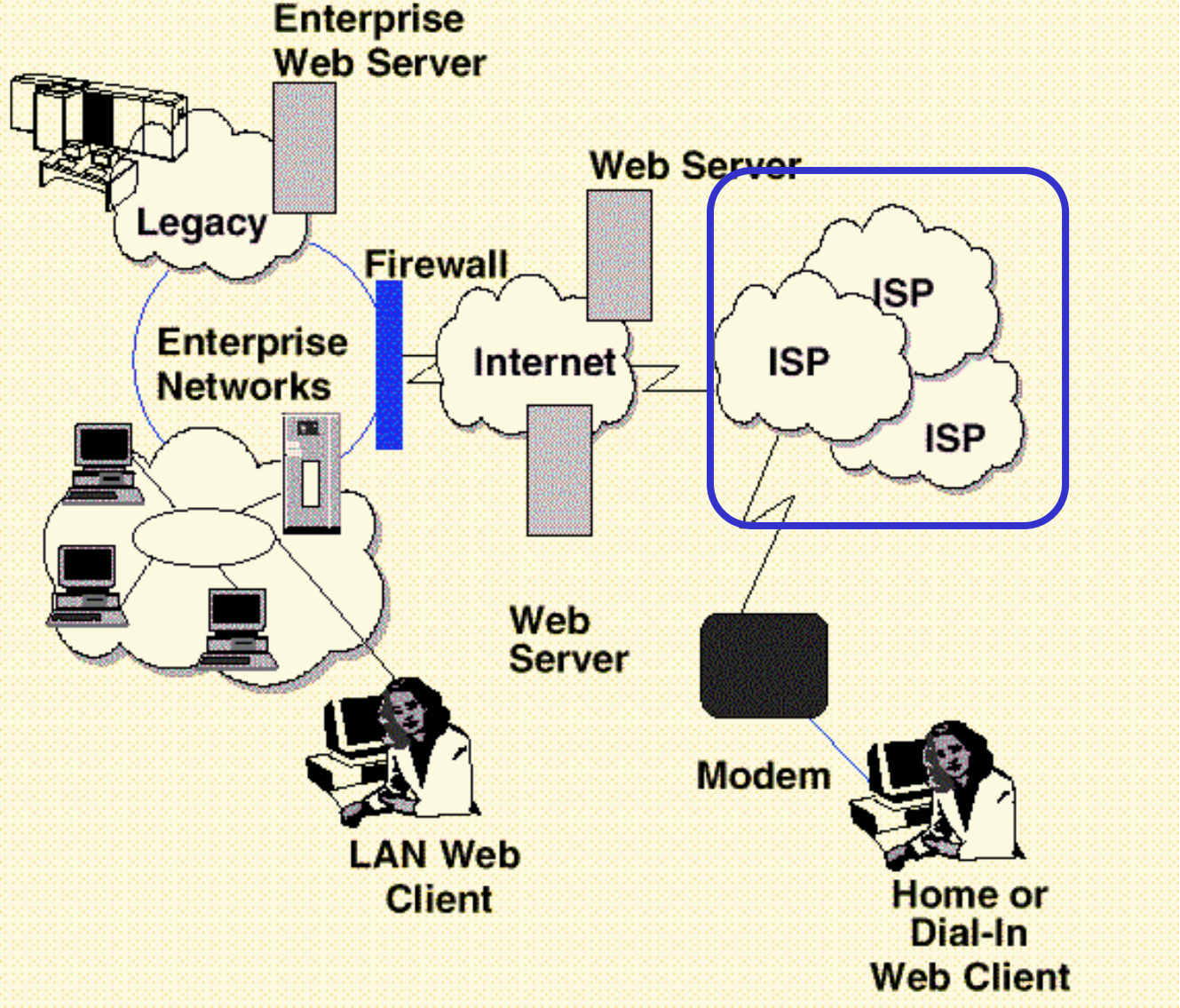
Elementi dell'infrastruttura



Connette la casa dell'utente al POP (Point of Presence) dell'ISP:

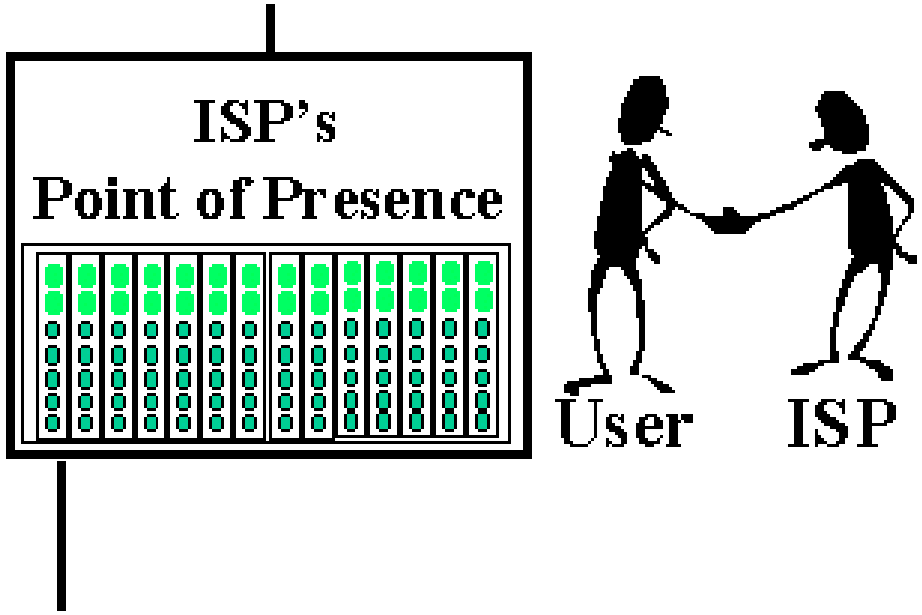
- **Linee di Communicazione (PSTN, ISDN, DSL, CDN)**
- **Cavo**
- **Satellite - (DirecPC)**
- **Linea elettrica - (Digital PowerLine by Nortel)**
- **Wireless**

Elementi dell'infrastruttura



Elementi dell'infrastruttura

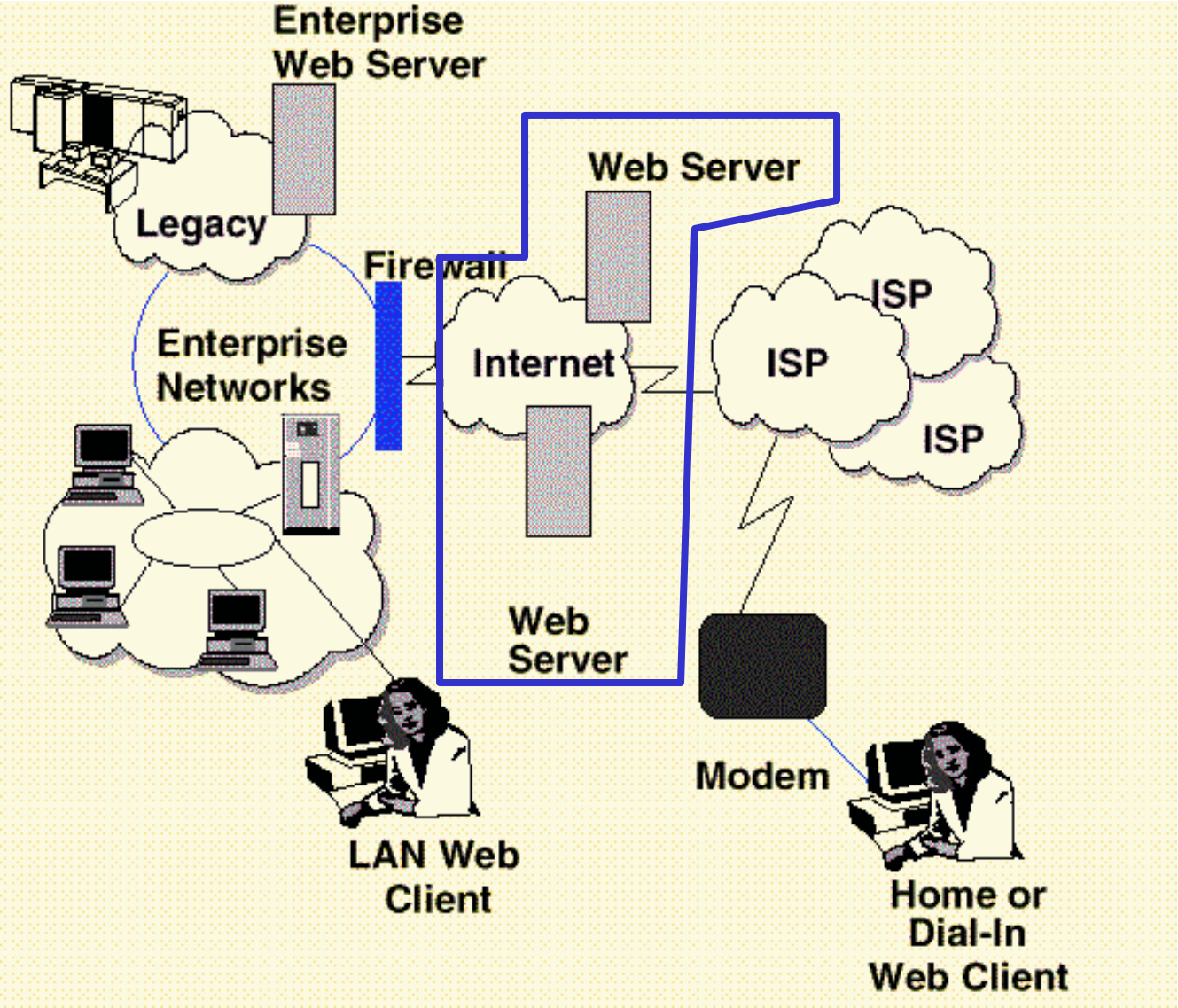
ISP's POP



E' il punto perimetrale della rete dell'ISP. Le connessioni dell'utente sono accettate e autenticate in questo punto.

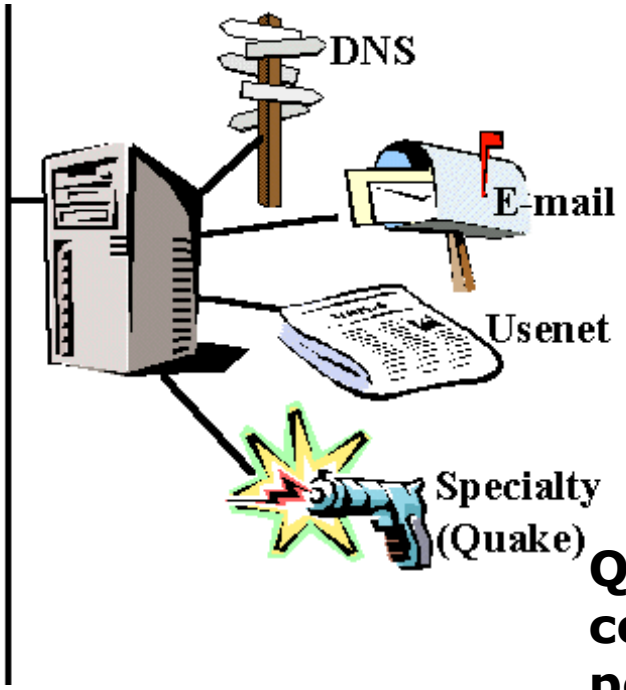
- **Access Server**

Elementi dell'infrastruttura



Elementi dell'infrastruttura

User Services

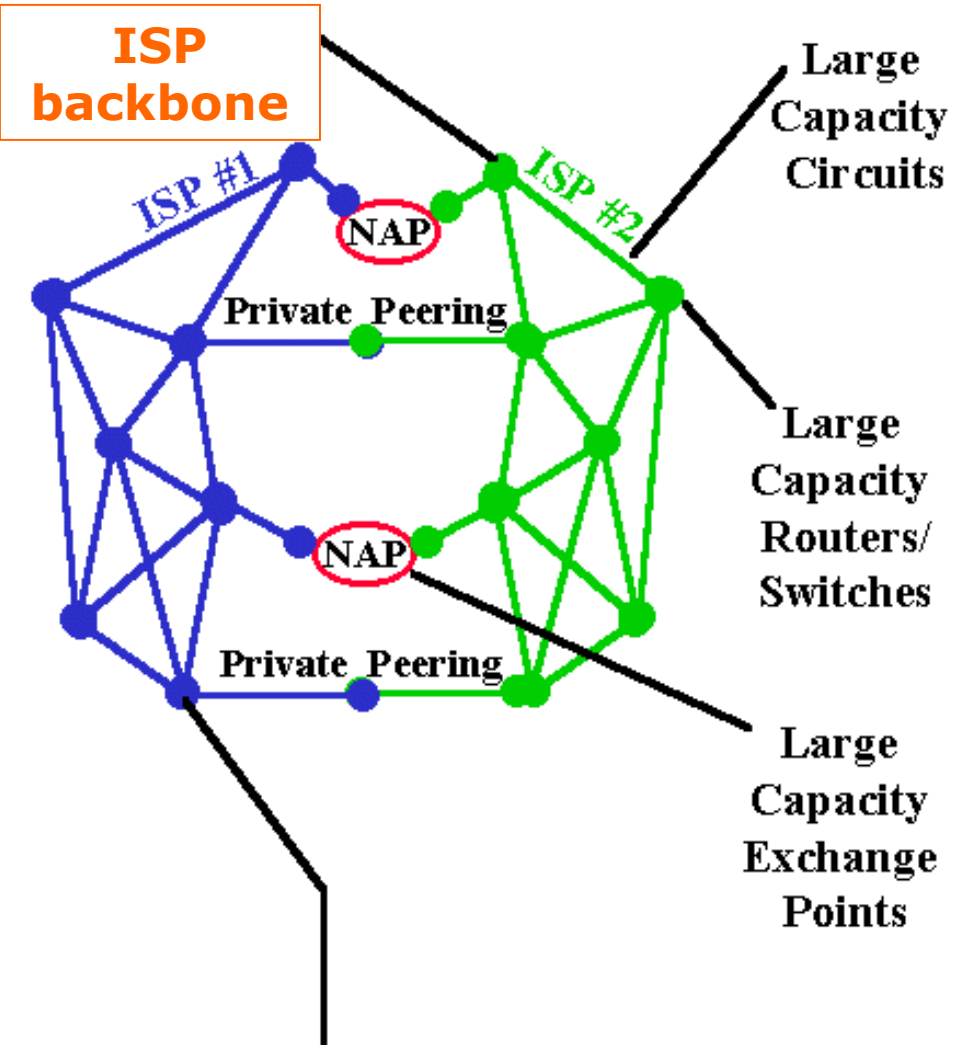


Sono i servizi che gli utenti usano durante l'accesso ad Internet.

- **Domain Name Server - BIND, DNS Resources Directory.**
- **Email Host - Sendmail,**
- **Usenet Newsgroups (NNTP) - INN**
- **Servizi Speciali quali SSH**
- **User Web Hosting**

Questi server richiedono collegamenti veloci, processori potenti e grandi quantità di memoria. Devono essere *fault tolerant* e *load balanced*.

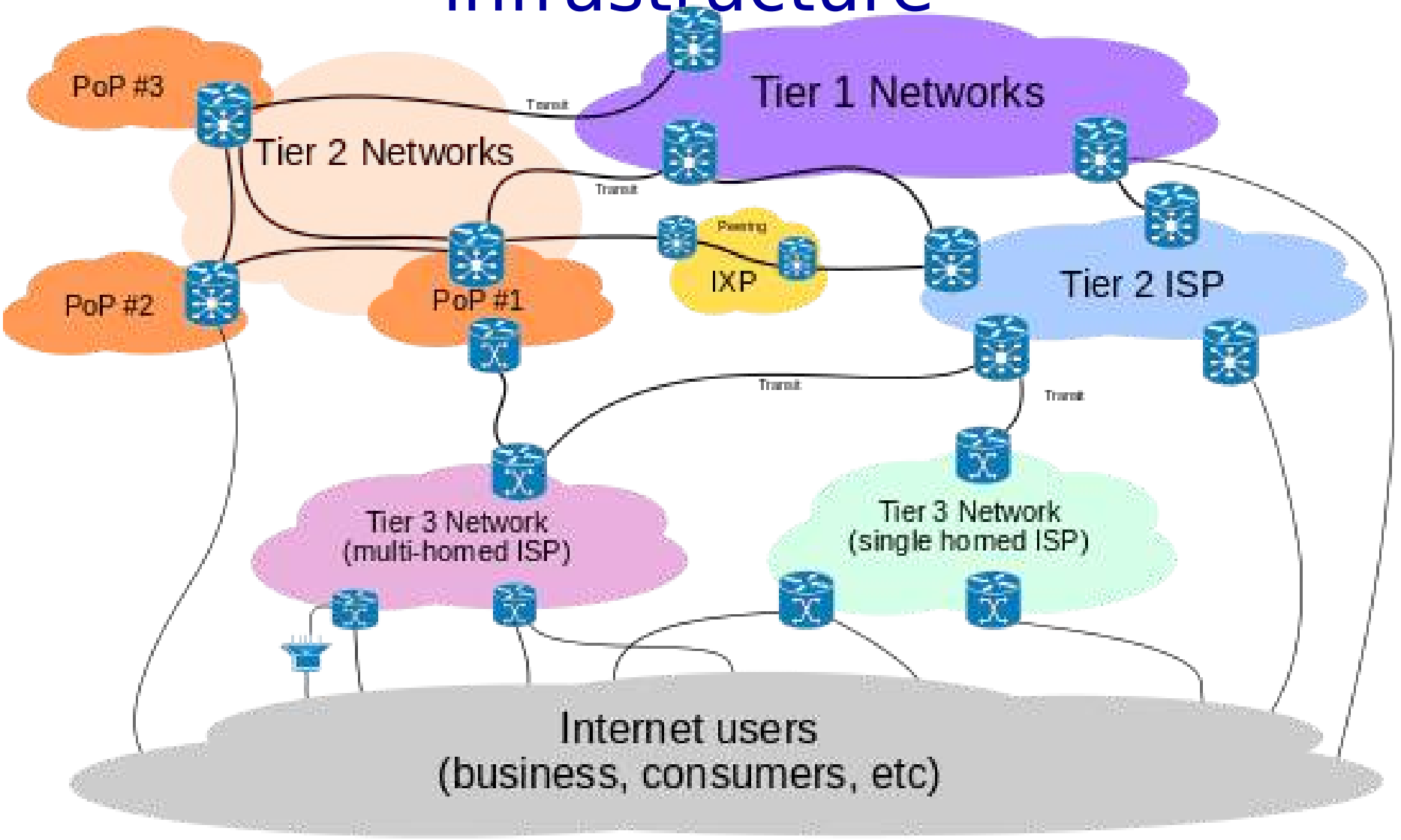
Elementi dell'infrastruttura



Il backbone dell'ISP interconnette i POP dell'ISP. ogni ISP agli altri ISP e al contenuto online.

- **Backbone Providers**
- **Large Circuits - fiber Circuit carriers**
- **Routers**
- **ATM Switches - (Fore, Newbridge, Lucent, Ascend)**
- **Sonet/SDH Switches - (Nortel, Fujitsu, Alcatel.Tellabs , Lucent, Positron Fiber Systems)**
- **Gigaswitch - (3com, Dec)**
- **Network Access Points**

Architecture of the Internet infrastructure



Elementi dell'infrastruttura

Online content

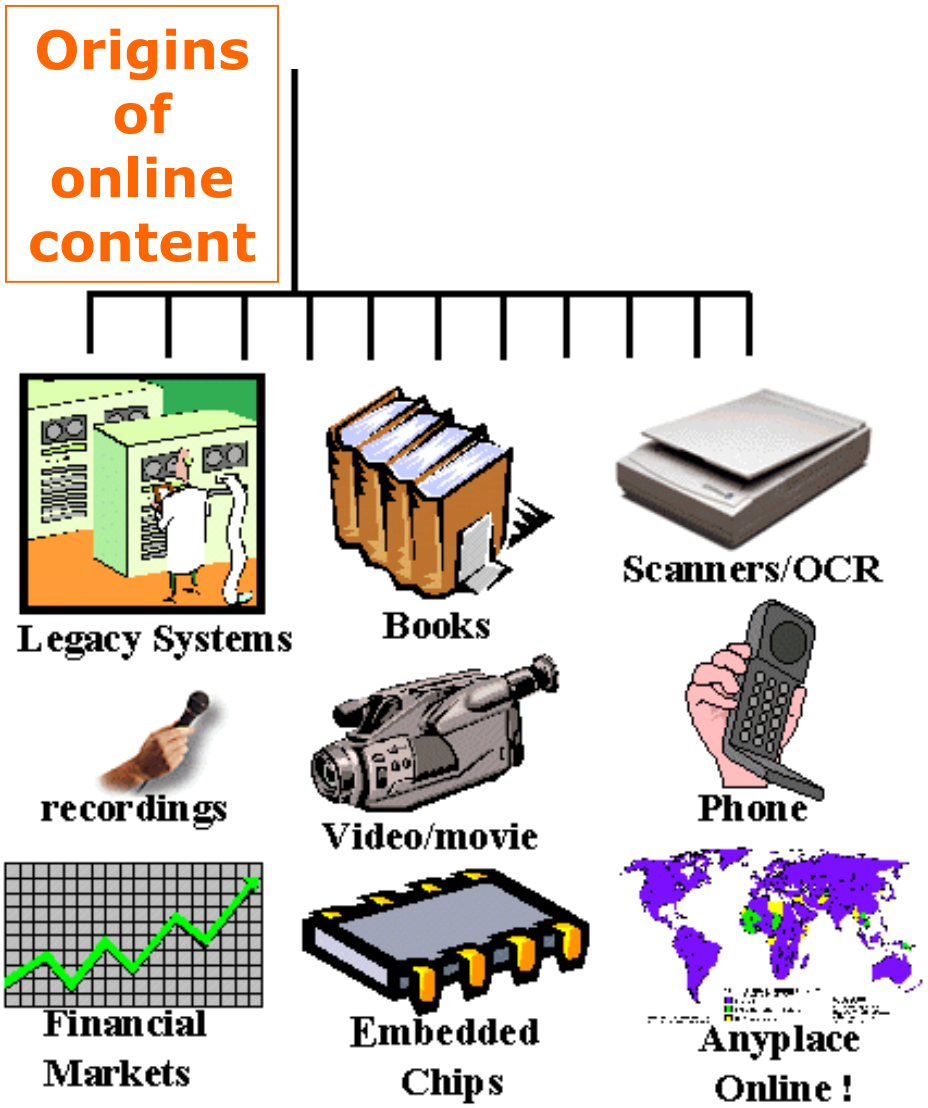
Hosting
Platform
(web, audio,video)

Sono gli host con cui interagiscono gli utenti.

- **Web Server platforms**
- **Hosting Farms**

Questi server richiedono collegamenti veloci, processori potenti e grandi quantità di memoria. Devono essere *fault tolerant* e *load balanced*.

Elementi dell'infrastruttura



Sono le sorgenti di informazioni del mondo reale

- **Le informazioni elettroniche esistenti sono connesse con i *legacy systems*** (sistemi basati su tecnologie obsolete, ma dei quali non si può fare a meno per le lora caratteristiche in termini di affidabilità, sicurezza)**.**
- **Le risorse stampate sono acquisite con scanner e trasformate in formato elettronico**
- **Molti tipi di informazioni audio e video sono trasmesse in broadcast su Internet.**
- **La telefonia via internet è un fenomeno importantissimo**

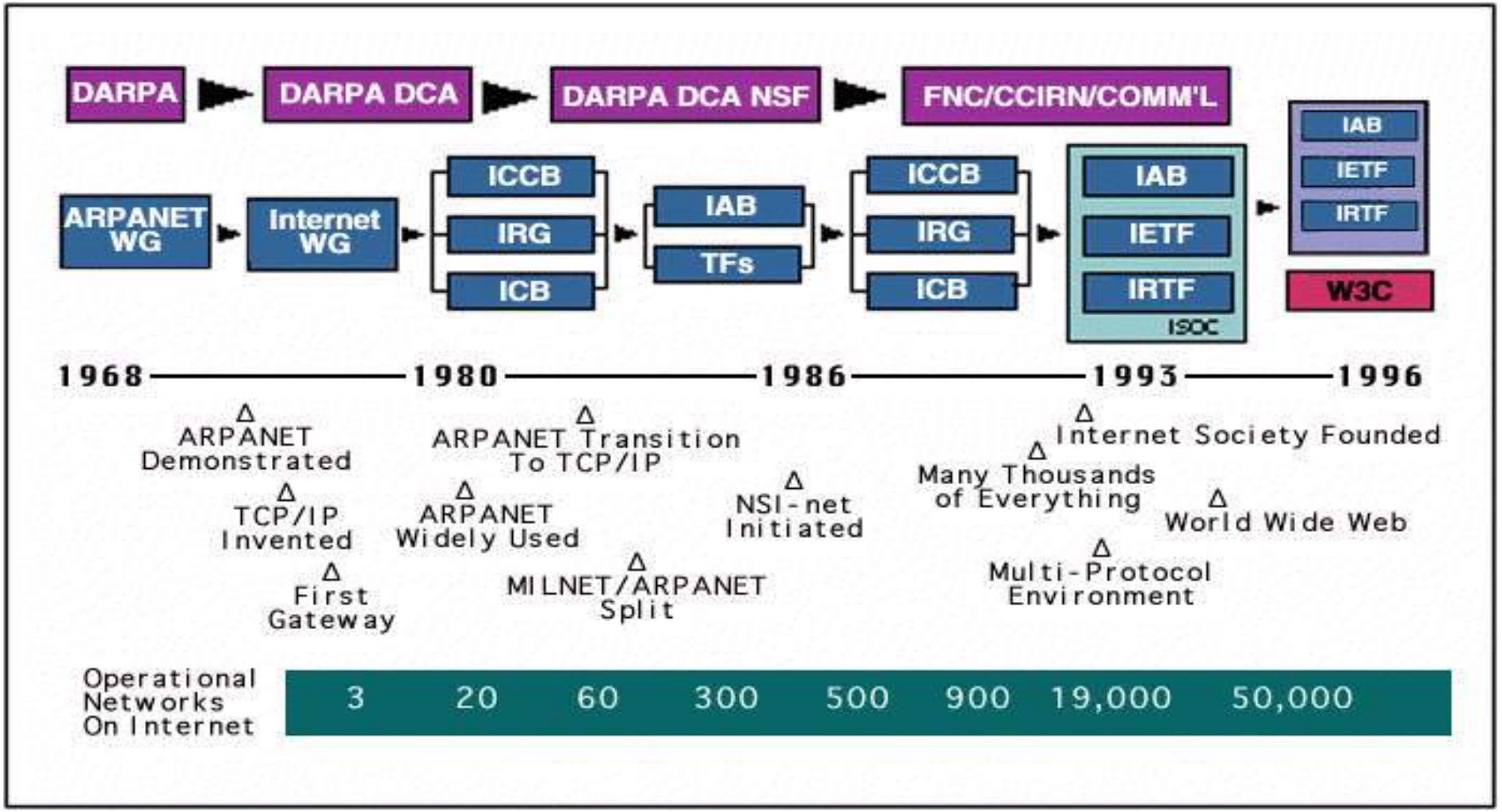
Ma chi c'è dietro Internet?

Chi la governa e decide le cose?

Internet governance

- E' una struttura complessa ed estremamente meritocratica
- Ci sono i leader storici, i quali coordinano I vari organismi di standardizzazione
- Ci sono i rappresentanti dei governi (dei più forti, ovviamente)
- Ci sono le aziende che hanno il core business in questo mondo
- Ci sono i tecnici e gli sviluppatori che mantengono e sviluppano i principali software
- Ci sono gli utenti, che con i loro canoni che pagano per usare la rete immettono denaro fresco nelle casse delle aziende

Evoluzione del governo di Internet



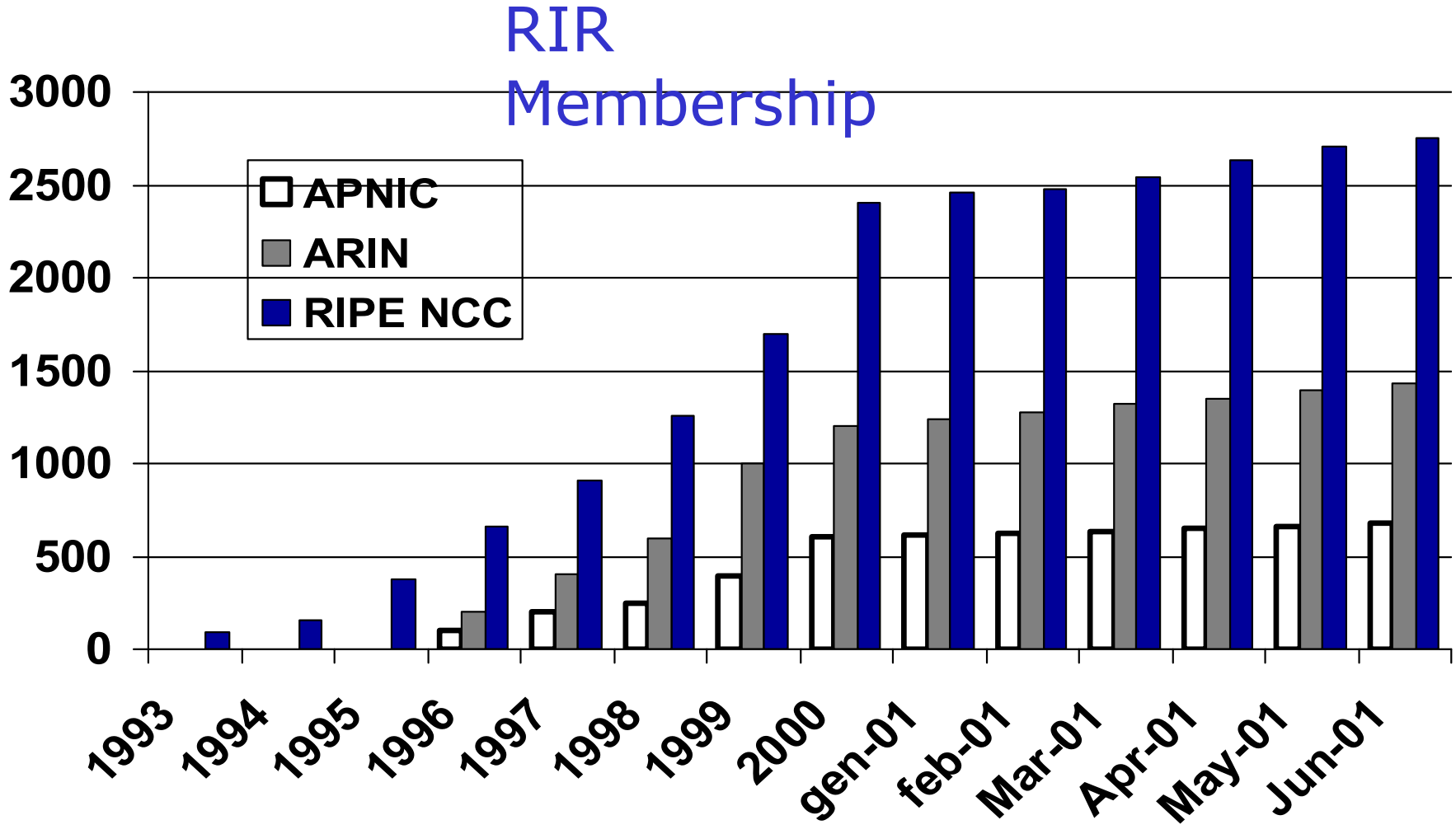
Un ente storico: IANA

- Alcuni Standard di Internet richiedono una forma organizzativa per funzionare correttamente, come per esempio la gestione dello spazio di indirizzamento IP e dei nomi a dominio, dei numeri di Autonomous System, dei numeri di protocollo IP.
- La responsabilità complessiva di ciò è storicamente stata assegnata all'Internet Assigned Numbers Authority (IANA)(**www.iana.org**)

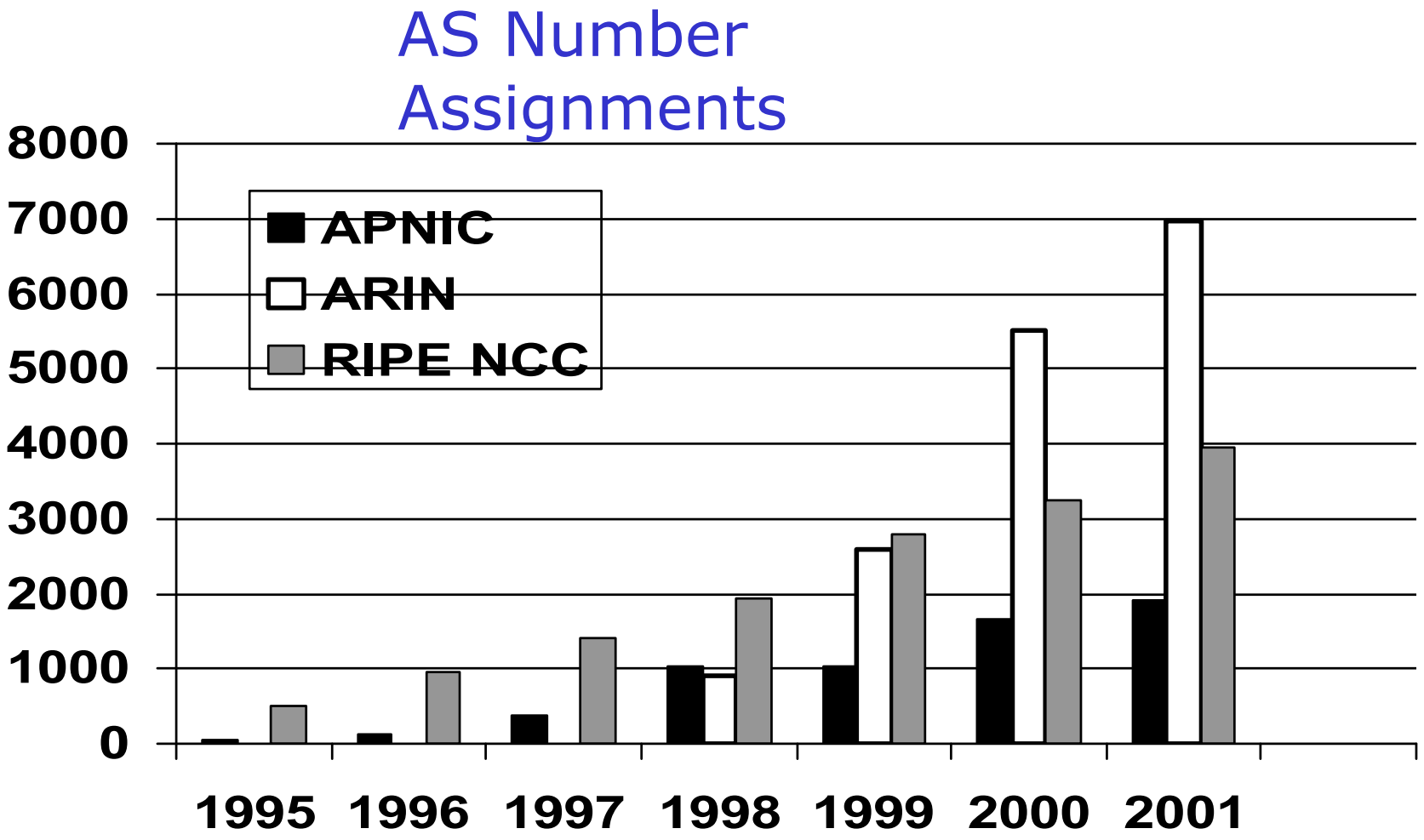
Local Registries

- IANA ha delegato ad alcune entità regionali la gestione locale:
  - ARIN (**www.arin.net**) per le Americhe
  - RIPE NCC (**www.ripe.net**) per l'Europa
  - Asia-Pacific-NIC (APNIC)(**www.apnic.net**) per l'area Asia-Pacifico
- Attualmente la materia è oggetto di completa ristrutturazione sotto la responsabilità dell' Internet Corporation for Assigned Name and Numbers (ICANN) (**www.icann.org**) che ha una struttura più partecipata e democratica rispetto a IANA.

Amministrazione di Internet



Amministrazione di Internet



Operatività di Internet

- Le operazioni di Internet sono coordinate a livello mondiale dall' Internet Engineering Planning Group (IEPG) (**www.isc.org/iepg**) il quale ha la funzione di coordinare le attività e l'interoperabilità tra i vari Internet Service Operators mondiali.
- La missione di IEPG è definita nell'RFC1690:
  - Facilitare le operazioni di gestione dei servizi globali di Internet
  - Promuovere l'introduzione di nuovi servizi Internet entro l'Internet globale
  - Collegamenti con i gruppi Operativi Internet e con i gruppi di Sviluppo Tecnico.

Standards di Internet

- Internet esiste a livello tecnico e di sviluppo attraverso la creazione, la verifica e l'implementazione di Standard Internet.
- Gli Standard sono sviluppati dall' Internet Engineering Task Force (IETF) (`www.ietf.org`)
- Gli Standard sono poi esaminati dall' Internet Engineering Steering Group (IESG) (`www.ietf.org/iesg.html`) e poi promulgati dalla Internet Society (ISOC) (`www.isoc.org`) come standard internazionali
- L'RFC Editor è poi responsabi[le] [della] preparazione e organizzazione dello standard nella forma finale

Sviluppo di Internet

- L' Internet Research Task Force (IRTF) (**www.irtf.org**) ha lo scopo di promuovere la ricerca e lo sviluppo di Internet coordinando le attività di idversi Gruppi di Ricerca
- L'IRTF lavora sotto il controllo dell'Internet Research Steering Group. Il coordinatore di IRTF fa parte del comitato di gestione di IRSG.
- Il coordinatore dell'IRTF è nominato dall'Internet Activity Board (IAB) (**www.iab.org**)
- Le finalità di IRTF sono definite nell'RFC2014.

Iniziative di Internet

- 

  Global Internet Policy Initiative:

- E' una iniziativa che propone l'adozione nei paesi in via di sviluppo di piattaforme legislative e politiche per la realizzazione di un'accesso ad Internet aperto e democratico.
- GIPI ha siglato un protocollo di intesa con United Nations Development Program (UNDP) (`www.undp.org`) al fine di promuovere le Internet and Communications Technologies (ICT) nei paesi in via di sviluppo
- E' un progetto congiunto di Internews (`www.internews.org`) e del Center for Democracy and Technology (CDT) (`www.cdt.org`)

Aziende e Internet

Intranet aziendali

- Intranet è il termine che descrive l'uso delle tecnologie Internet all'interno di una organizzazione, invece che per le connessioni esterne con l'Internet globale.
- Ciò viene realizzato trasferendo la mole di informazione aziendale ad ogni individuo con un costi, tempo e sforzo minimi
- L'impatto della Intranet influenza le operazioni della compagnia, la sua efficienza, la ricerca e lo sviluppo.
- Prerequisiti per l'attivazione di una Intranet aziendale:
  - rete locale che interconnetta i computer
  - informatizzazione diffusa dei vari settori

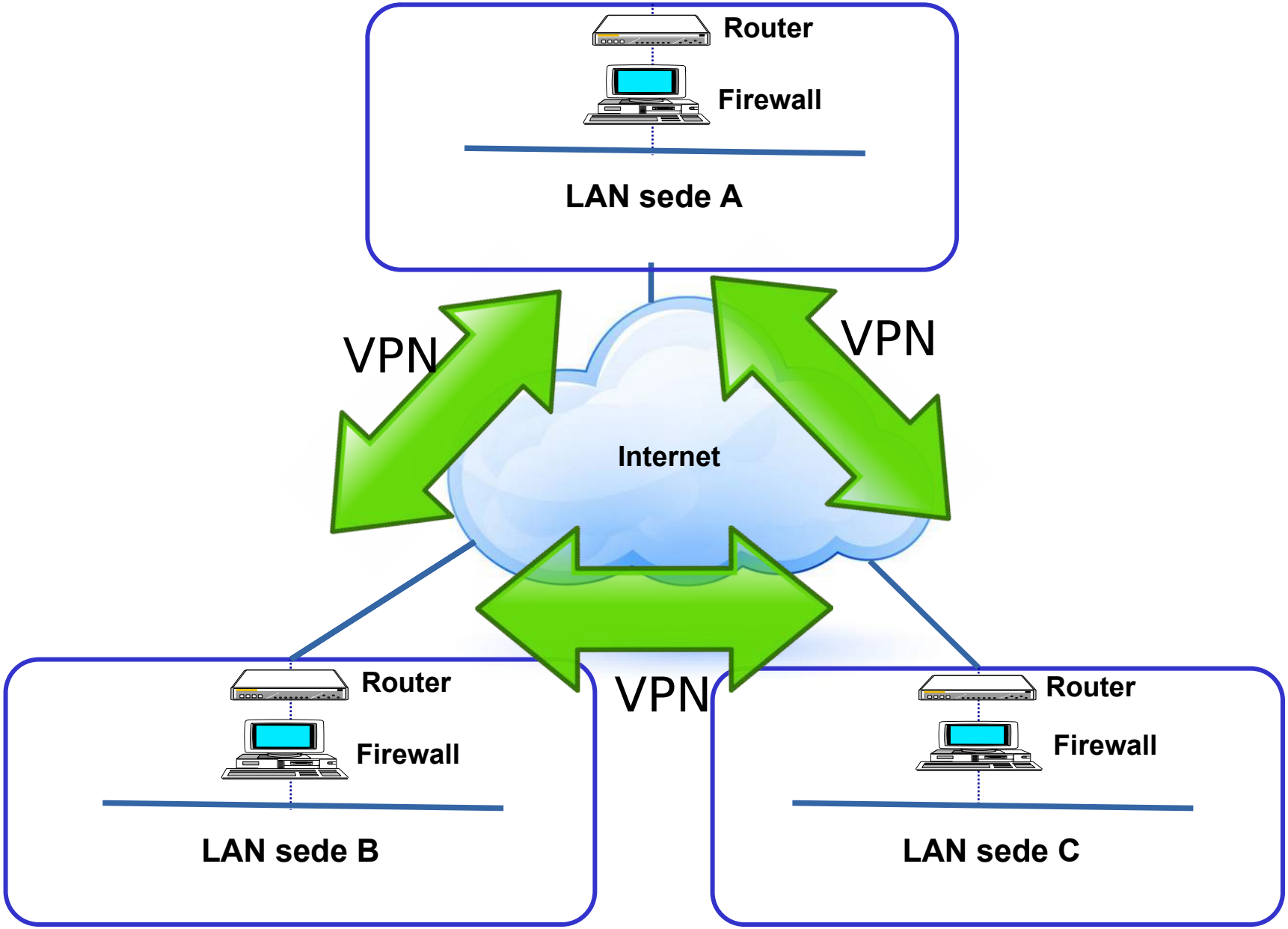
Intranet

Vantaggi

- Con la Intranet le tecnologie telematiche ed i servizi di Internet si diffondono orizzontalmente e verticalmente nella struttura aziendale divenendo momento di
  - grande partecipazione
  - formazione
  - aggiornamento.

- Internet ha come periferica un computer e da qui origina la sua straordinaria capacità e potenzialità di trasmettere, integrare, rappresentare qualsiasi tipo di informazione.

Intranet



Intranet

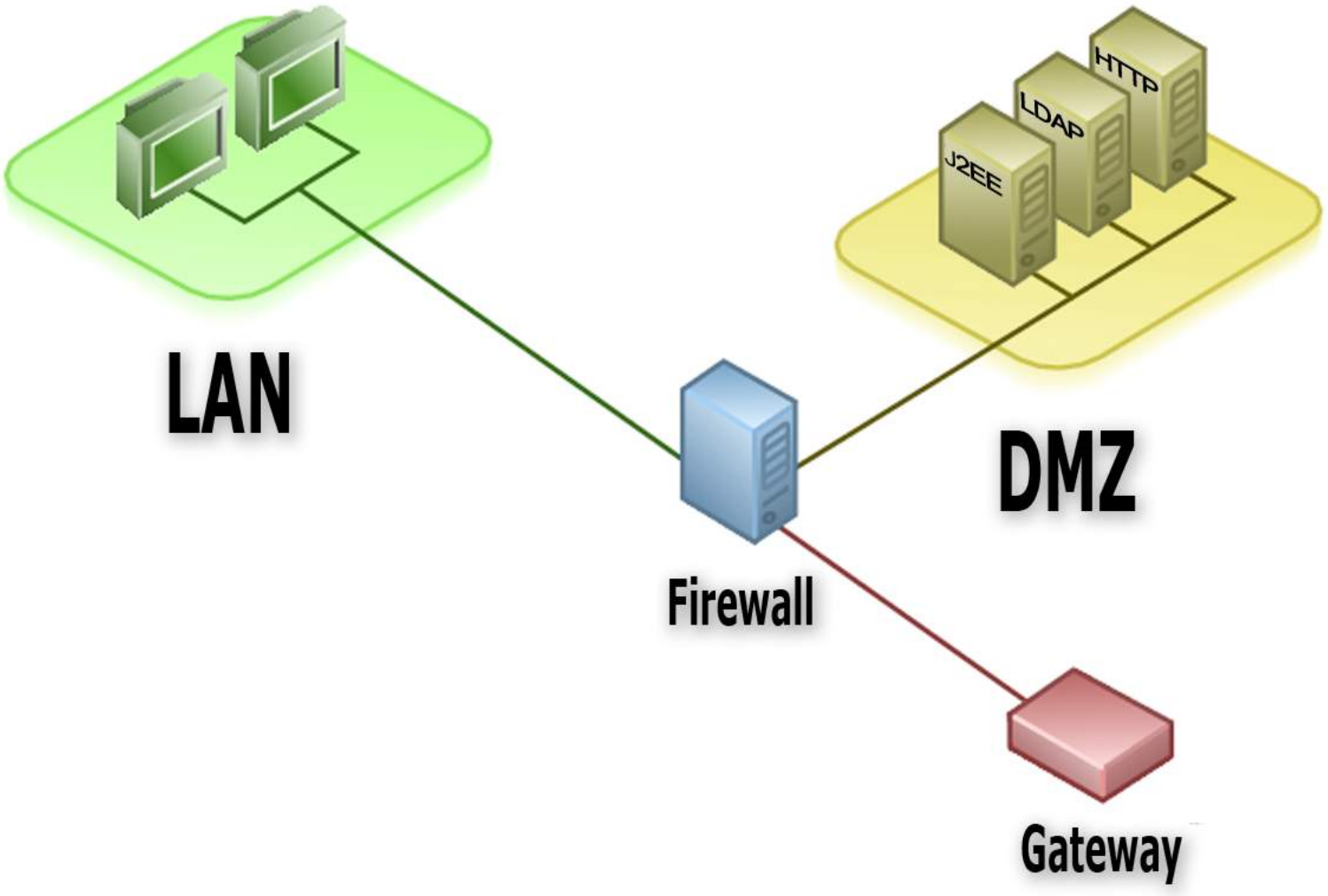
- Il router svolge le seguenti importanti funzioni:
  - instrada i dati tra i computer della rete aziendale e Internet
  - consente l'attivazione di una politica di controllo degli accessi alla rete locale.
  - Consente l'accesso controllato e selettivo a computer e servizi
- Mediante la realizzazione della Intranet, le tecnologie telematiche ed i servizi di Internet penetrano nella struttura aziendale divenendo momento di grande partecipazione, formazione ed aggiornamento.
- Sono tecnologie che portano alla ottimizzazione e riduzione dei costi di comunicazione e marketing

Extranet

- Con questo termina si identificano le risorse hardware e software che realizzano la presenza visibile in Internet di una organizzazione
  - data mining
  - data warehouse
  - e-commerce
  - servizi Web

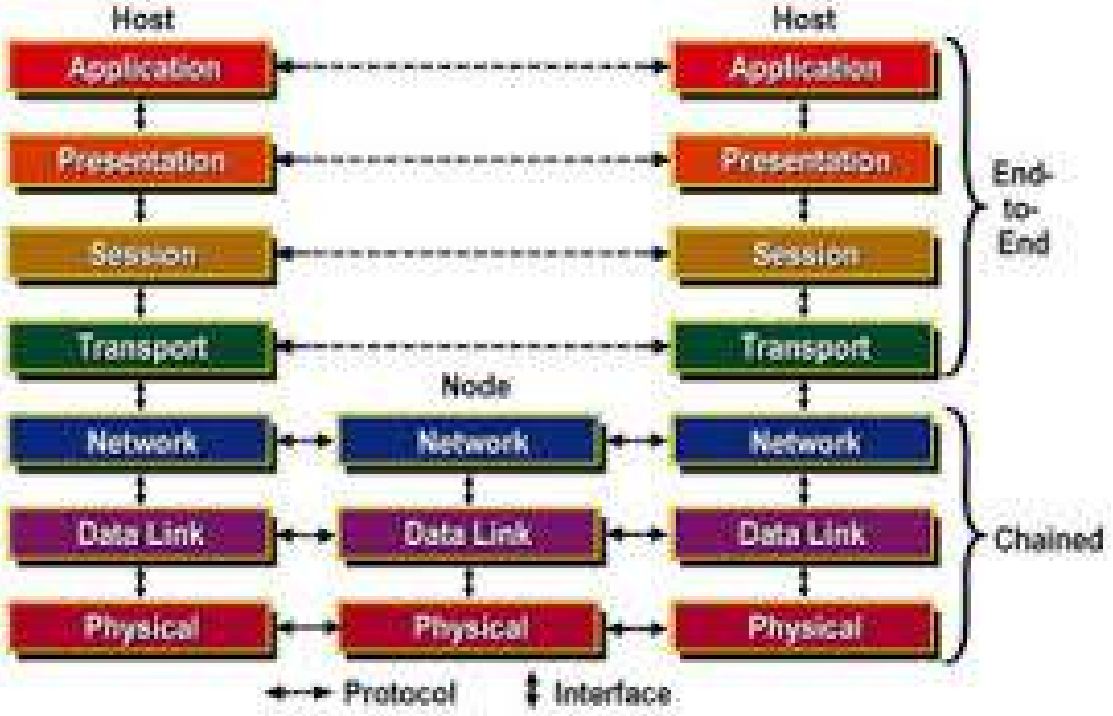
- normalmente sono servizi che vengono posti in una speciale area, in cui il controllo del firewall è più lasco: De-Militarized Zone (DMZ). I server in quest'area non sono ritenuti critici, i servizi in genere replicati da server protetti

DMZ



Modello di Riferimento ISO/OSI

Modello di Riferimento ISO/OSI



Standards

- L'importanza degli *standards* ed il lavoro delle *organizzazioni di standardizzazione* è stato fondamentale per lo sviluppo delle TLC.
- Definiscono le caratteristiche fisiche ed operative degli apparati di rete.
- L'adozione di standard aiuta la vendita dei prodotti
- Il processo di standardizzazione favorisce l'interconnessione e l'integrazione di hardware prodotto da diversi costruttori
- Esistono standard
  - ***de jure*** (cioè codificati da organismi nazionali o internazionali)
  - ***de facto*** (massiccia adozione da parte degli utenti)

Organizzazioni: IEEE

- L'Institute of Electrical and Electronic Engineers (IEEE) è molto attivo nello sviluppo di standard di comunicazione dati (Communication Society, COMSOC).
- Il sottocomitato 802 ha iniziato i lavori nel 1980, prima che fosse stabilito un valido mercato per le reti locali, segnando comunque un avanzamento teorico fondamentale.
- Il progetto 802 è concentrato sull'interfaccia fisica degli apparati e sulle procedure richieste per stabilire, mantenere e terminare connessioni tra dispositivi di rete, inclusa:
  - la definizione del formato dei dati
  - il controllo dell'errore
  - attività per il controllo del flusso dell'informazione

CCITT - ITU

- Il Consultative Committee for International Telephone and Telegraph (CCITT) è ora un gruppo dell'International Telecommunications Union (ITU), un'agenzia specializzata dell'ONU in ambito telecomunicazioni
- è costituito da 15 gruppi di studio

- Il lavoro è articolato in periodi quadriennali, chiamati *Study Period*, al termine dei quali ha luogo un'assemblea plenaria nel corso della quale vengono emanate le raccomandazioni. Es:
  - V.21 Duplex 300 bits/s modem modulation.
  - V.22 Duplex 1200 bits/s modem modulation.
  - V.22bis Duplex 2400 bits/s modem modulation.
  - V.32 Duplex modem modulation up to 9600 bits/s.
  - V.32bis Duplex modem modulation up to 14400 bits/s.
  - V.34 Duplex modem modulation up to 28800 bits/s.

ISO

- L’ International Standards Organization è un organo consulente dell’ONU
- Il suo scopo è *promuovere lo sviluppo di standards nel mondo, con l’obiettivo di favorire lo scambio internazionale di cose e servizi*
- Sono membri oltre 100 organizzazioni standard nazionali
- Il maggior successo dell’ISO nel campo delle telecomunicazioni è stato il concepimento del modello a sette livelli ***Open Systems Interconnection (OSI) Reference Model***

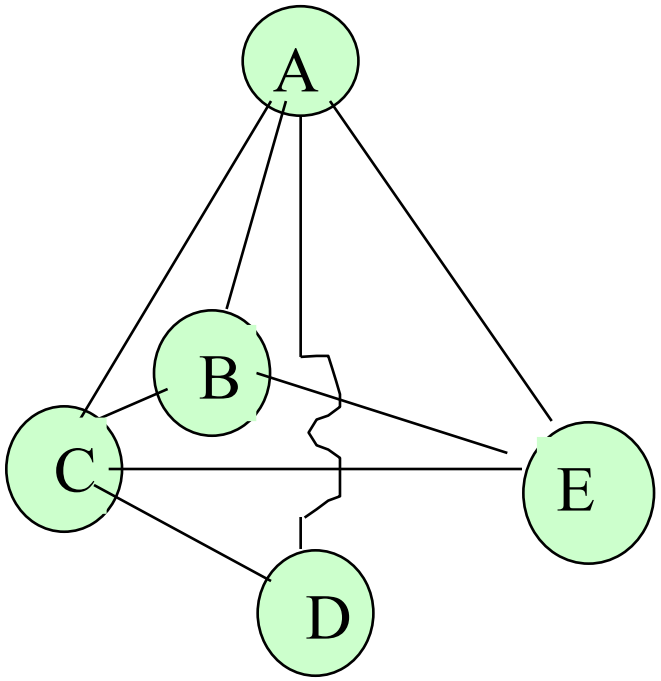
ISO OSI Reference Model

- Definisce un impianto concettuale sulla base del quale è possibile definire le modalità di interconnessione di sistemi informatici
- Fornisce un modello di riferimento per confrontare diverse implementazioni di protocolli di rete proprietari e non
- Rimane fondamentalmente uno strumento teorico e concettuale con uno scarsissimo numero di implementazioni di servizi. Es:
  - ✓ ISO/IEC 10021 per la posta elettronica (X.400)
  - ✓ ISO/IEC 9594 per i servizi di Directory (X.500)

ISO OSI Reference Model

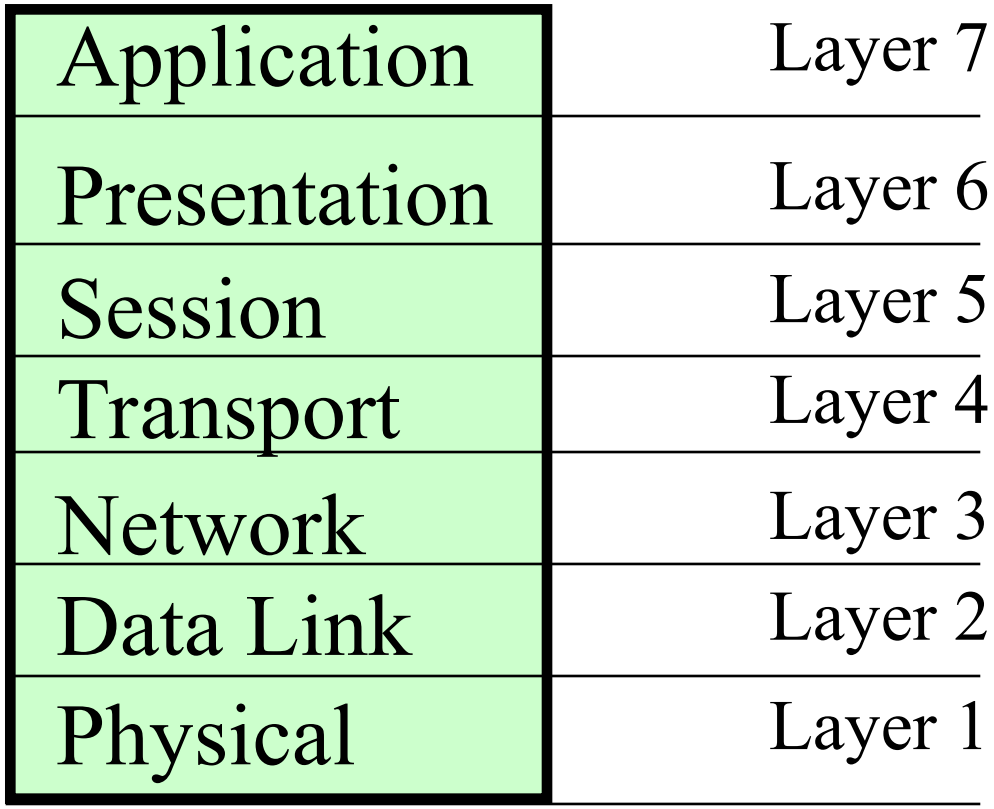
- OSI introduce il concetto di sistema:
  - risorse hardware
  - risorse software
  - periferiche
  - programmi
- e di applicazione:
  - programma che elabora i dati ed eroga servizi
- OSI si preoccupa dello scambio di informazioni tra sistemi

Definizioni



- La figura illustra una tipica struttura di rete
- I cerchi rappresentano i *nodi della rete*
- I nodi sono connessi tra loro mediante dei *communication path*
- I percorsi tra due nodi sono *information path*

ISO Reference model *



***CCITT Recommendation X.200**

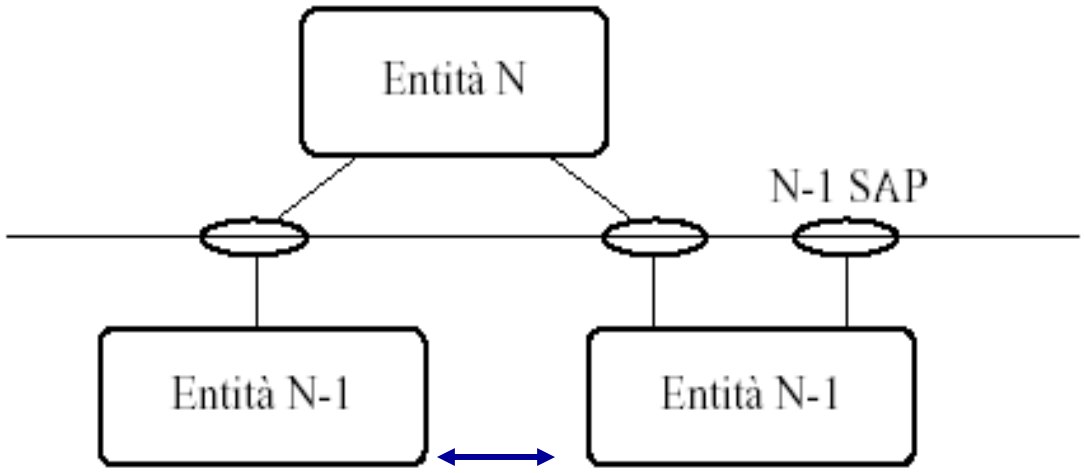
Architettura a livelli

- La suddivisione in livelli del modello adotta l'approccio scientifico di dividere un problema complesso in più sottoproblemi, più agevoli da risolvere
- Risultano 7 livelli, ciascuno deputato ad uno specifico insieme di servizi, specifici per le finalità del livello
- Ad eccezione dei livelli 1 e 7, ciascun livello è collegato ai livelli precedente e successivo
- Ciascun livello sfrutta i servizi del livello immediatamente inferiore
- Un dispositivo deve potersi connettere con un qualsiasi altro dispositivo in rete

ISO OSI Reference Model (i)

- Livelli adiacenti comunicano attraverso le loro interfacce
- Ogni livello è costituito da una o più entità
- Entità appartenenti allo stesso livello in sistemi diversi vengono dette peer entities
- Le entità usano i servizi del livello inferiore e forniscono servizi al livello superiore mediante il proprio Service Access Point (SAP).
- Le operazioni specifiche di un livello sono realizzate mediante un insieme di protocolli

OSI Reference Model (ii)

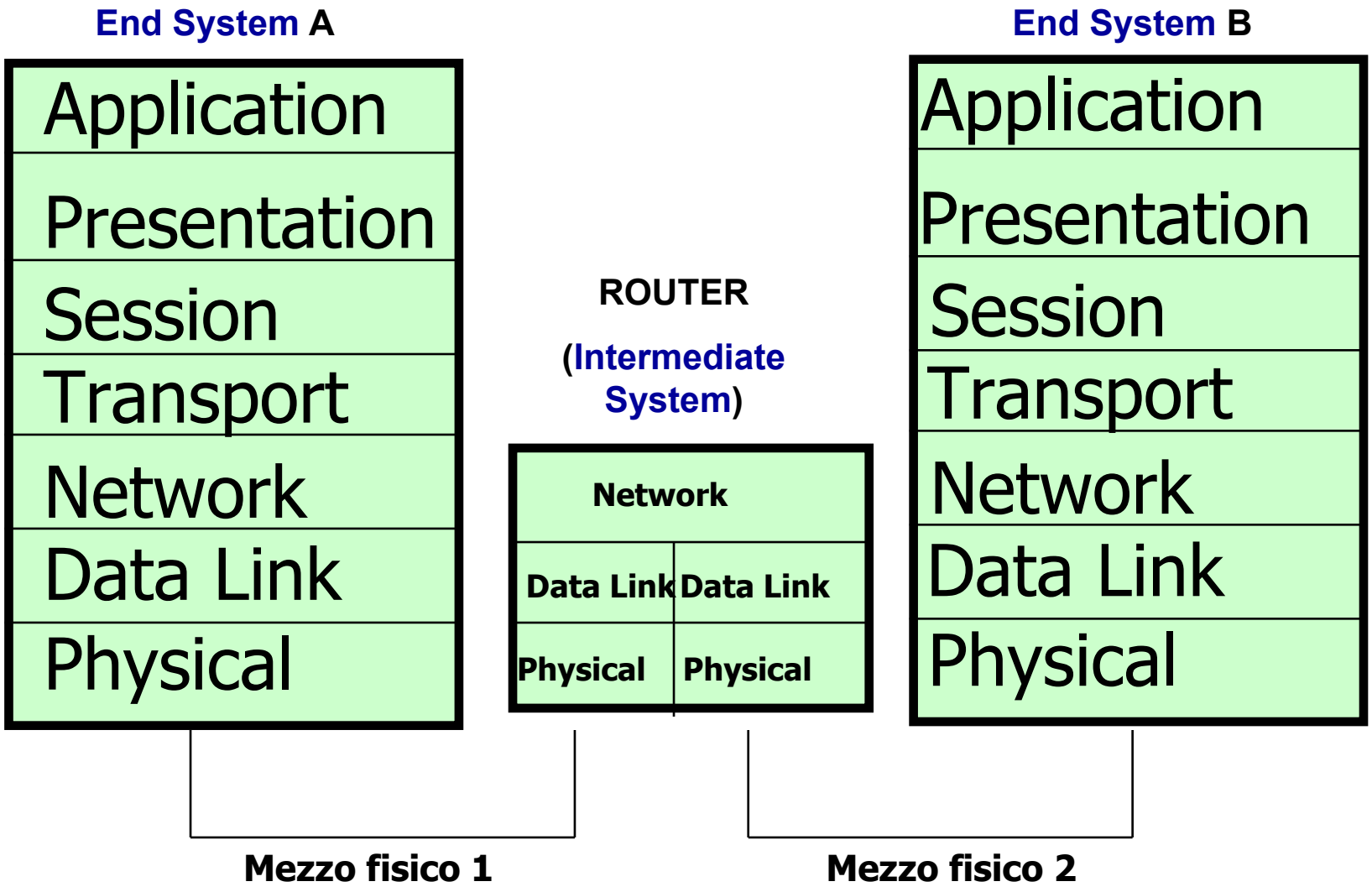


Servizi erogati

Servizi fruiti

Protocollo di livello N-1

Intermediate Systems (IS)



Physical layer

- Al livello più basso, il livello fisico, è un insieme di di regole che specificano le connessioni elettriche e fisiche tra i dispositivi fisici.
- Questo livello specifica le connessioni dei cavi e il tipo di segnale elettrico associato ai vari pin di connessione delle interfacce utilizzate per trasferire dati tra i diversi dispositivi di rete.
- Il *physical link* corrisponde agli standard di interfaccia dei vari dispositivi. Ad esempio appartengono a tale livello le interfacce:
  - ✓ RS232
  - ✓ V.24
  - ✓ V.35
  - ✓ SONET/SDH
- Le regole definiscono la trasmissione dati per i terminali, i modem, le schede di rete, etc.

Data link layer (NIC, hub, bridge, switch)

- Il secondo livello descrive come un dispositivo guadagna l'accesso al mezzo specificato nel physical layer e come realizza la comunicazione con un nodo adiacente.
- Definisce il formato dei dati, la frammentazione dei dati in un messaggio trasmesso, le procedure di controllo dell'errore, etc
- Appartengono a questo livello le schede di rete (NIC), gli hub, i bridge e dispositivi di switching che operano una divisione del dominio di collisione Ethernet (suddividendo, come vedremo, il traffico in base al MAC address)
- è il livello responsabile di un invio affidabile delle informazioni ad un altro nodo della rete.
- Appartengono a questo livello i *data link control protocol* (DLCP), come il Binary Synchronous Communications (BSC) e High Level Data Link Control (HDLC) utilizzati per la trasmissione su linee CDN.
- Appartengono a questo livello anche i sottolivelli LLC e MAC (il quale scende fino a livello 1) di Ethernet

Network layer (router, switch liv.3)

- è responsabile della realizzazione di una connessione tra due nodi della rete: il nodo sorgente e quello destinatario, inclusa la scelta e la gestione del routing (cioè le regole che permettono l'istra-damento delle informazioni in base all'indirizzo della rete di destinazione) e lo scambio di informazioni tra i due nodi
- Appartengono a questo livello i router e gli apparati di commutazione (switch) abilitati a funzioni di routing.
- I servizi di questo livello sono associati al movimento dei dati nella rete, inclusi l'indirizzamento, il routing e le procedure di controllo dei flussi.
- Appartiene a questo livello il protocollo IP.

Transport layer (switch liv.4)

- E' il livello che garantisce che il trasferimento delle informazioni avvenga correttamente
- Analizza la comunicazione tra due *nodi*, basandosi sul fatto che il *network layer* è in grado di stabilire il cammino ottimale tra i due nodi
- Appartengono a questo livello i dispositivi di commutazione che operano a livello 4, quali ad esempio i proxies

- Si occupa principalmente di:
  - controllare l'errore
  - verificare la sequenza delle informazioni
  - analizzare i fattori di affidabilità dello scambio di dati tra i due nodi
- E' il primo livello *end-to-end*
- Appartengono a questo livello i protocolli TCP e UDP

Session layer

- Fornisce le regole per attivare e terminare flussi di dati tra nodi della rete
- E’ responsabile dell’organizzazione del dialogo tra programmi applicativi e del relativo scambio di dati
- Consente di aggiungere a sessioni end-to-end servizi più avanzati

- I servizi che questo livello può fornire sono:
  - attivazione e terminazione della connessione tra due nodi
  - controllo del flusso di messaggi tra i nodi
  - controllo del dialogo
  - controllo dei dati da ambo i nodi

Presentation layer

- I servizi di questo livello sono relativi alla trasformazione dei dati, alla loro formattazione ed alla sintassi (sono previste una rappresentazione astratta, una locale e una per il trasferimento).
- Una delle funzioni è quella di convertire i dati ricevuti in modo da essere rappresentati opportunamente nel dispositivo di ricezione
- Esempi di trasformazioni che possono essere gestiti da questo livello sono
  - crittografazione/ decrittografazione dei dati
  - compressione/ decompressione dei dati

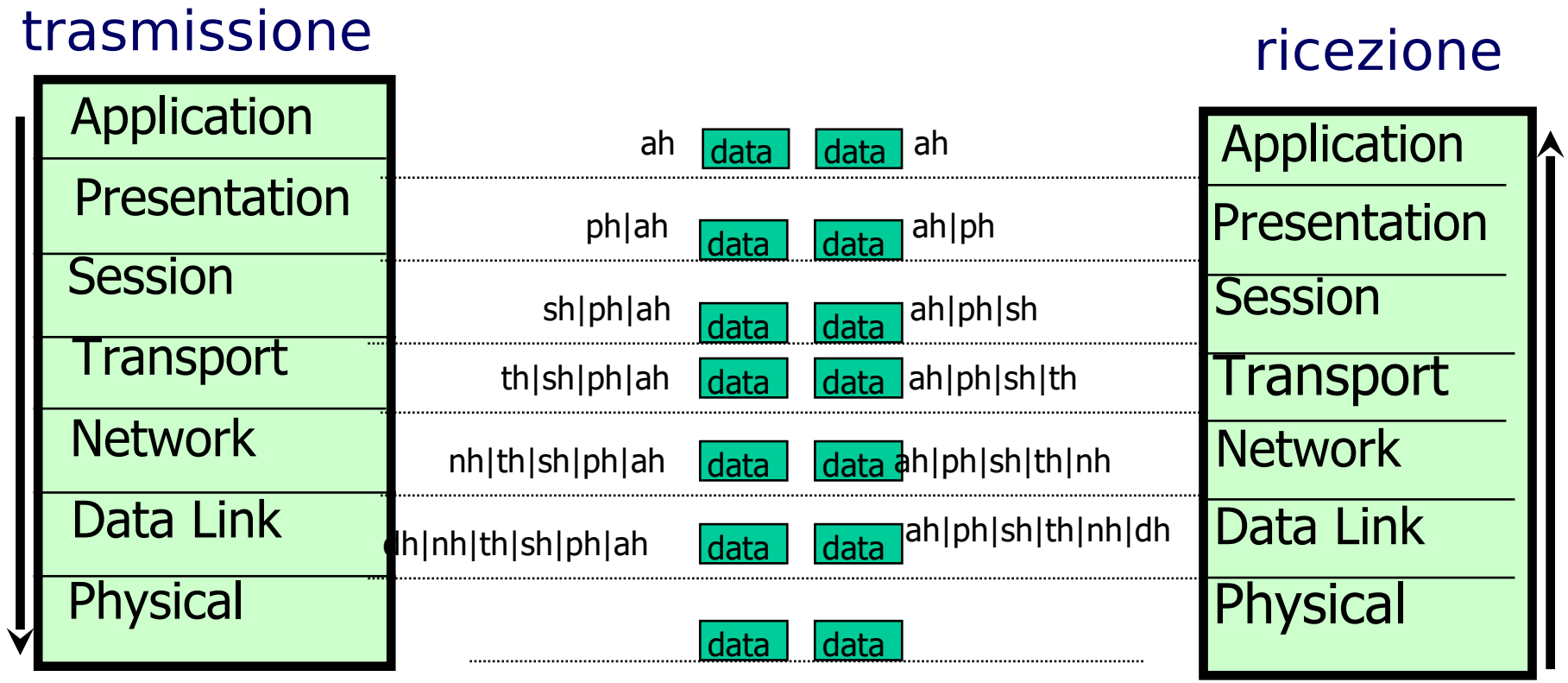
Application layer (switch liv.7)

- Questo livello comprende tutti i programmi applicativi (di sistema o scritti dall'utente) che consentono l'uso della rete.
- L'ultimo livello si comporta come una finestra attraverso la quale l'applicazione accede a tutti i servizi messi a disposizione dal modello.
- Appartengono a questo livello i dispositivi di commutazione che operano a livello 7 (accesso selettivo ad applicazioni in base alla disponibilità o meno di abilitazioni o in base alla tipologia del client)
- Esempi di funzioni svolte da questo livello:
  - Terminale virtuale (VT)
  - file transfer access management (FTAM)
  - Posta elettronica, X.400
  - condivisione di risorse
  - accesso a database (X.500, servizio di Directory)
- Gli ultimi tre livelli possono differire molto a seconda del tipo di rete nella quale vengono istallati e del protocollo di rete utilizzato

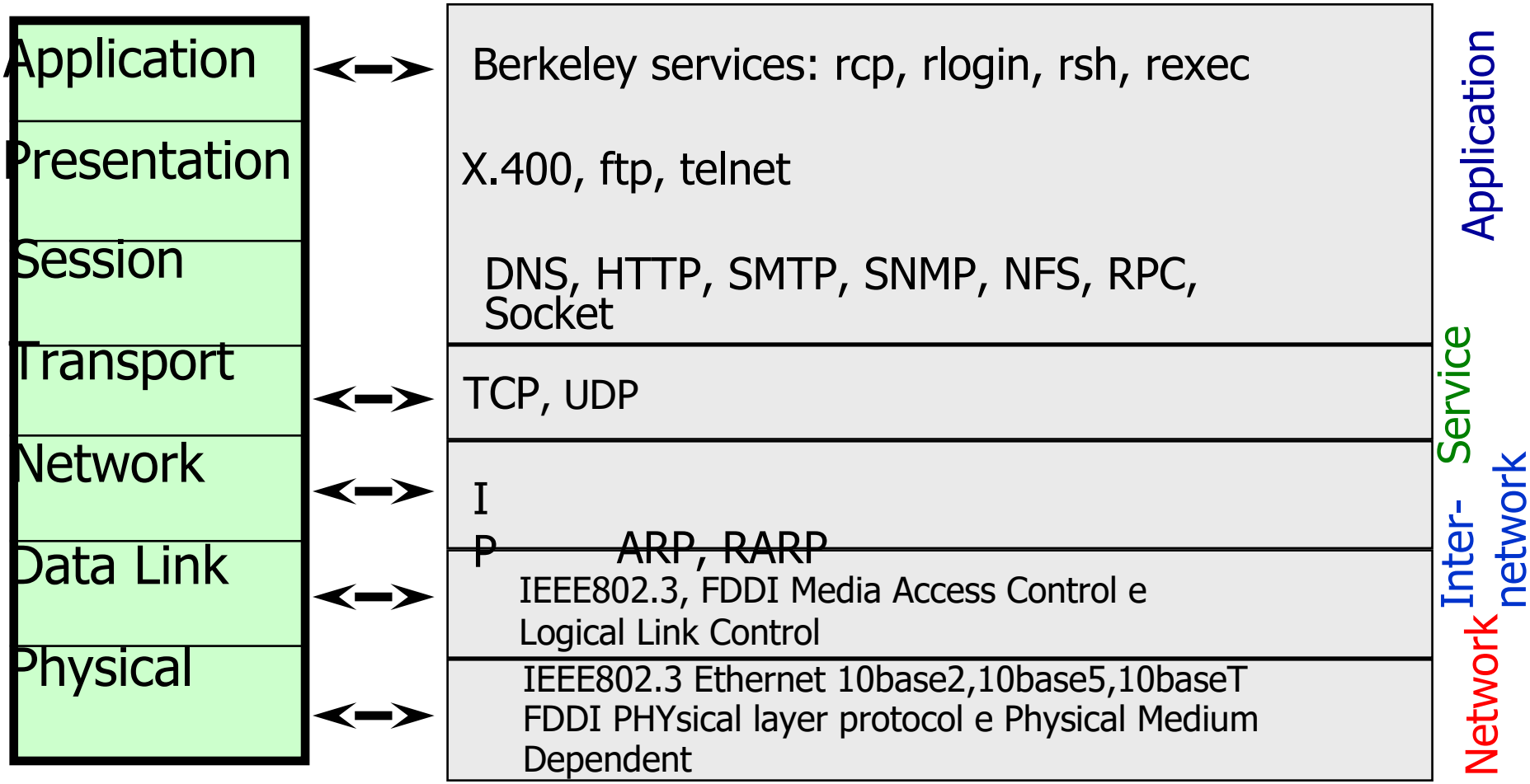
OSI Reference Model: conclusioni

- Analizzando il flusso di dati dal lato del nodo mittente occorre specificare che il livello superiore appende all'informazione una intestazione che contiene le informazioni specifiche di quel livello. Ciò avviene per ogni livello, tranne il Physical Level.
- Per quanto concerne il flusso di dati dal lato del nodo ricevente, ogni livello, tranne il Physical Level, effettuerà il procedimento inverso, rimuovendo l'intestazione dopo averla interpretata, in modo da riavere l'informazione integra.
- Al fluire dei dati in un network ISO, il livello *n* interagisce con il livello *n-1*
- Il punto di comunicazione tra livelli adiacenti è il Neutral Acces Point (NAP)

OSI : headers per comunicazione tra due nodi

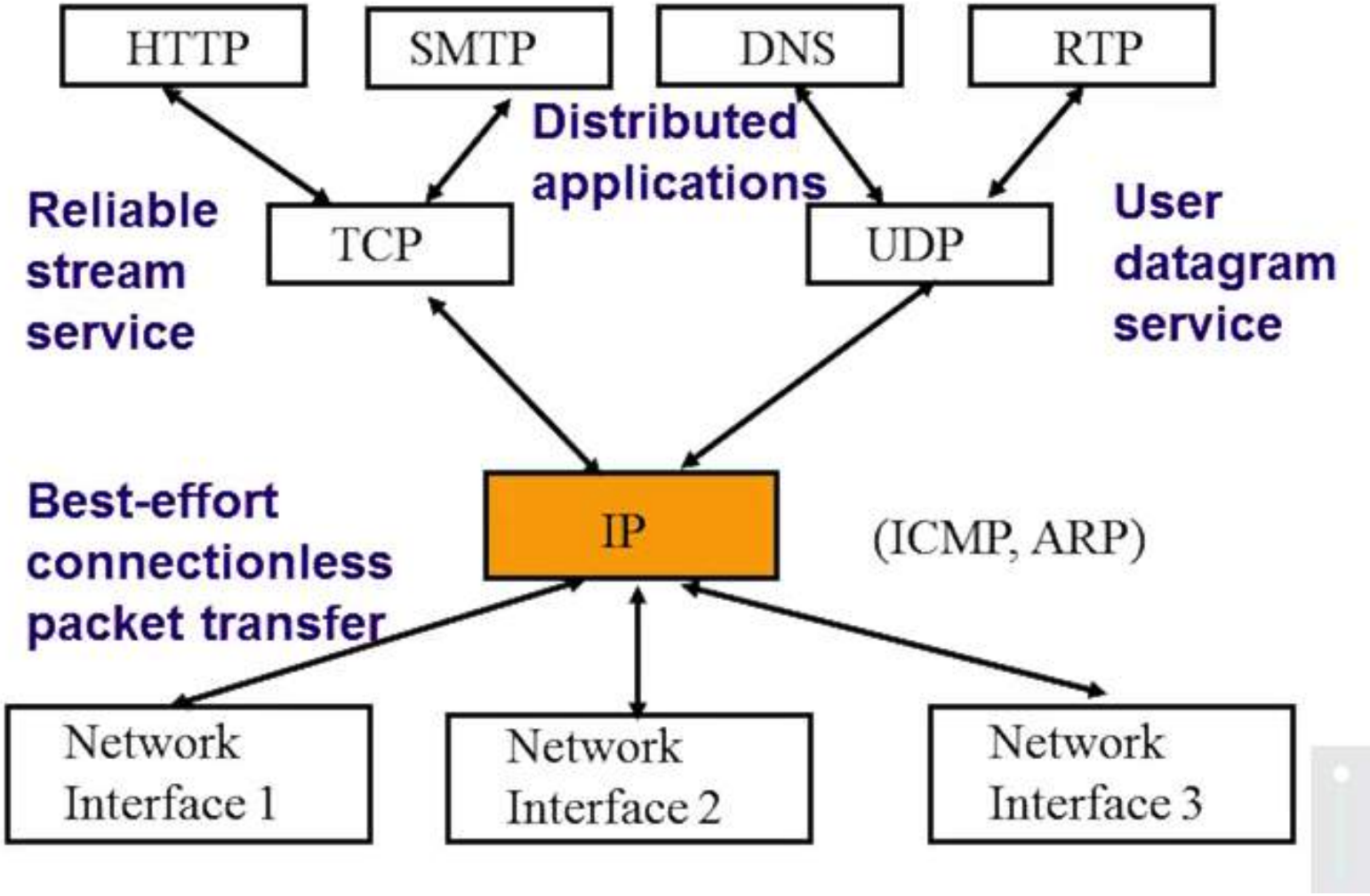


Il modello OSI e la comunicazione in ambiente UNIX e TCP/IP



Famiglia di protocolli TCP/IP

Famiglia di protocolli TCP/IP



Internet Protocol, IP

- L'utente considera un'internet come una singola rete virtuale che interconnette tutti gli host e attraverso cui è possibile comunicare
- Il software dell'internet è progettato intorno a tre servizi di rete disposti su scala gerarchica:
  - ✓ ***Servizio di consegna del pacchetto senza connessione***
  - ✓ ***Servizio di trasporto inaffidabile***
  - ✓ ***Servizi di applicazione***
- **Consegna senza connessione***:* ogni pacchetto è consegnato indipendentemente dagli altri
- **Servizio inaffidabile**: i pacchetti possono andar persi o fuori sequenza
- **Consegna best-effort***:* si fa di tutto per consegnare i pacchetti: l'inaffidabilità si verifica solo per malfunzionamenti hardware. E' compito dei servizi di più alto livello provvedere a garantire l'affidabilità della trasmissione reinviando i pacchetti persi e ristabilendo la giusta sequenza tra i pacchetti.

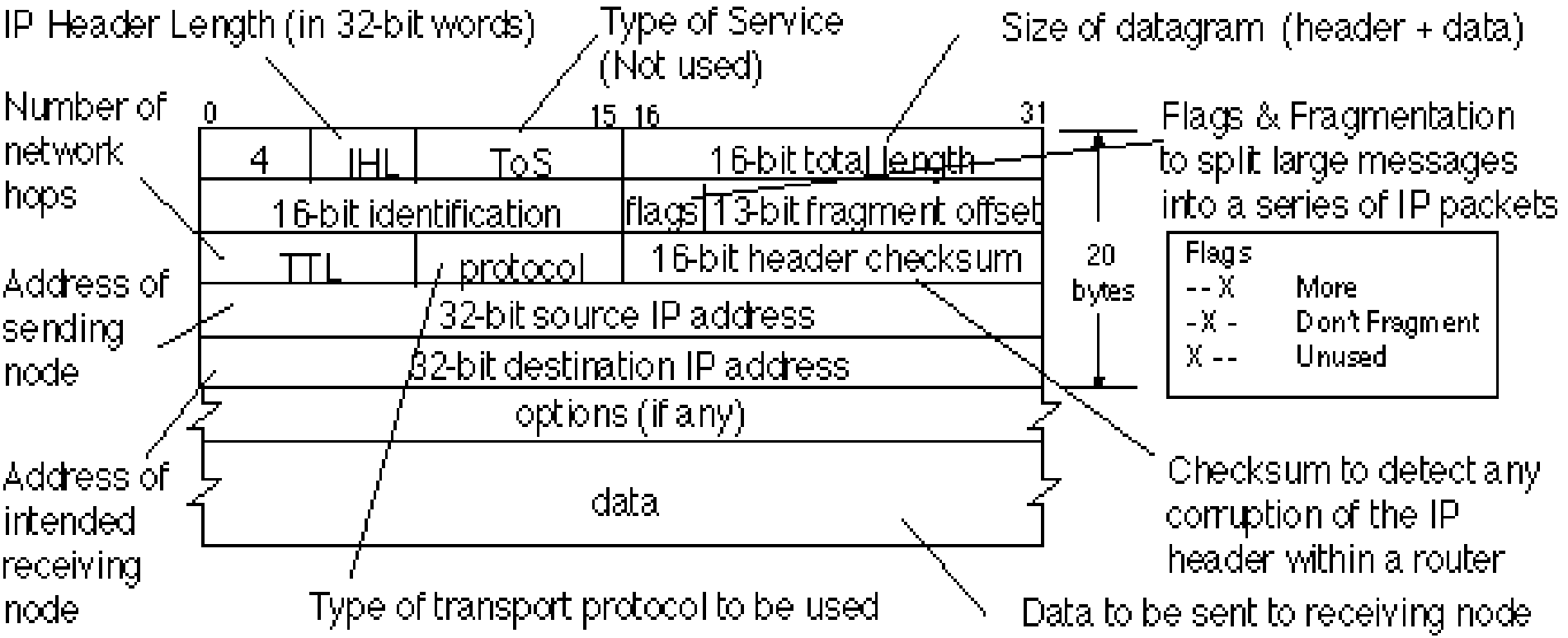
Internet Protocol, IP (II)

- L'IP definisce l'esatto formati dei dati, mentre attraversano l'internet TCP/IP
- L'IP svolge la funzione di **routing** scegliendo il percorso che dovranno seguire i dati
- Definisce un insieme di regole che inglobano i concetti di
  - consegna non affidabile dei pacchetti
  - elaborazione dei pacchetti da parte di host e gateway
  - generazione dei messaggi di errore (ICMP)
  - determinazione delle condizioni in cui occorre scartare i pacchetti

Internet Protocol, IP (III)

- L'unità fondamentale di trasferimento è detta **datagram IP**, il quale è diviso in area di intestazione e campo di controllo dell'header, ed il blocco dei dati.

IP v4 Header



Formato dell'header del datagram

- Nell'header del datagram IP sono presenti i seguenti campi:
  - VERS un campo di 4 bit che indica laversione IP del datagram. La versione attualmente in uso è la 4 (IPv4), si sta introducendo la 6 (IPv6) che potenzia l'indirizzo IP a 64 bit e ne potenzia i servizi e le potenzialità
  - HLEN un campo si 4 bit che indica la lunghezza dell'header del datagram in parole da 32 bit.
  - LUNGHEZZA TOTALE campo lungo 16 bit che indica la lunghezza totale del datagram in ottetti, compresa l'area dati. La massima dimensione possibile per un datagram è **2^{16}=65535 ottetti**
  - TIPO DI SERVIZIO un campo di 8 bit che indica come deve essere gestito il datagram. E' diviso in 5 sottocampi: 3 bit di PRECEDENZA che consentono al trasmettitore di specificare l'importanza del datagram (valori da 0 a 7). Il software dell'host e dei gateway ignora questo tipo di informazione, altrimenti sarebbe possibile implementare algoritmi di controllo della congestione. Se fosse gestito questo campo sarebbe anche possibile attivare servizi basati sul Quality of Service (QoS). Questa anomalia è risolta con IPv6.

Formato dell’header di un datagram

3 bit suddivisi in campi D T e R specifica il tipo di trasporto desiderato per il datagram. Se attivi, il bit D chiede un basso ritardo, il bit T richiede un alto throughput, il bit R alta affidabilità. Naturalmente una internet non garantisce il trasporto richiesto. Quindi questo campo va interpretato come una indicazione agli algoritmi di routing.

- IDENTIFICAZIONE, FLAG e OFFSET DEL FRAMMENTO: sono campi che controllano la frammentazione e il riassemblaggio dei datagram a seguito dell’incapsulamento dei datagram nelle trame a livello fisico. Frammentazione e riassembleggio dei datagram sono funzioni svolte dai protocolli a livello fisico della rete in cui si opera.
- TTL: indica la durata in secondi concessa al datagram per restare nel sistema internet.
- PROTOCOL: indica quale protocollo di più alto livello ha generato la porzione DATI trasportata dal datagram (es: 1=ICMP, 2=IGMP, 16=TCP, 17=UDP)

Formato dell'header di un datagram

- CHECKSUM: garantisce il controllo dell'integrità dell'header del datagram, mediante calcolo di un algoritmo Cyclic Redoundancy Check (CRC) sui bit dell'header
- IP ADDRESS DI PROVENIENZA: indirizzo IP a 32 bit dell'host che ha generato l'informazione contenuta nel datagram
- IP ADDRESS DI DESTINAZIONE: indirizzo IP a 32 bit dell'host al quale è destinata l'informazione contenuta nel datagram. Anche se il datagram è istradato attraverso diversi gateway questi campi non cambiano mai.
- DATI: contiene i dati trasportati dal datagram
- OPZIONI IP: un campo opzionale usato per funzioni di test e debugging della rete.
- RIEMPIMENTO: un'area che viene riempita di bit a 0 per garantire che la lunghezza del datagram sia multipla di 32 bit.

Elaborazione dell'Header IP

- Calcolo del checksum e verifica della sua validità, verifica che I campi dell'header contengano valori validi
- Analisi della routing table per calcolare il next hop
- Modifica dei campi che richiedono aggiornamento (TTL, header checksum).

Indirizzo IPv4

- Un indirizzo IP su 32 bit (4 byte) permette di identificare univocamente una rete ed uno specifico host appartenente alla rete:

  x.y.z.w (Es: `141.250.1.7`)

- L'indirizzo si divide in due parti:
  - rete
  - host
- Esistono 5 tipi di classi di indirizzi IP.

Classi di indirizzi IP

126 reti da 16 milioni di host

subnet mask associata:

- **Classe A: con x < 128** — **rete host** — 255.0.0.0

16382 reti da 64000 host

- **Classe B: con 128 <= x <= 191** — 255.255.0.0

2 milioni di reti da 254 host

- **Classe C: con 192<= x <= 223** — 255.255.255.0

- **Classe D: con x > 223** — **multicast addresses**

- **Classe E con x > 240** — **(riservata)**

x.y.z.w

Connessione alla rete

- Dato che le tre classi primarie (A, B, C) sono identificabili in base ai primi due bit, è molto agevole per i router estrarre la parte *rete* e la parte *host* di un indirizzo IP.
- L'indirizzo IP identifica la connessione di un host alla rete (non l'host in sé)
- Macchine (quali i router) con più connessioni alla rete hanno più indirizzi IP*:* uno per ogni connessione alla rete

Indirizzi di rete e broadcast

- Gli indirizzi IP possono far riferimento a *reti* oppure a *host*
- Per convenzione l'hostid 0 non è mai assegnato ad un singolo host: un indirizzo IP ove i bit che indicano la parte host siano pari a 0 *denota la rete stessa* ed è chiamato *indirizzo di rete*
- Gli indirizzi IP possono essere usati per specificare *indirizzi broadcast* (riservati a tutti gli host della rete) ponendo i bit della parte host dell'indirizzo IP a 1

Indirizzi speciali

- Indirizzi speciali:
  - 0.0.0.0 (default route)
  - 127.0.0.1 (loopback address)
- Indirizzi di rete e indirizzi broadcast:
  - 255.255.255.255 broadcast locale
  - x.0.0.0 e x.255.255.255 “ per una rete di classe A
  - x.y.0.0 e x.y.255.255 “ per una rete di classe B
  - x.y.z.0 e x.y.z.255 “ per una rete di classe C

Indirizzi privati

- I seguenti indirizzi identificano reti private (RFC 1918), non istradabili dai router (tali indirizzi sono gestiti e amministrati dai NAT server che gestiscono la conversione indirizzo pubblico-privato):

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

Indirizzi link local

- I seguenti indirizzi sono definiti dall'RFC 3927 come Link Local. Essi sono validi solo in una rete locale e non vengono istradati dai router:

169.254.0.0/16

Tali indirizzi vengono assegnati ad un'interfaccia dal sistema operativo quando ci sono problemi con l'assegnazione di indirizzi da parte di un server DHCP.

Configurazione IP

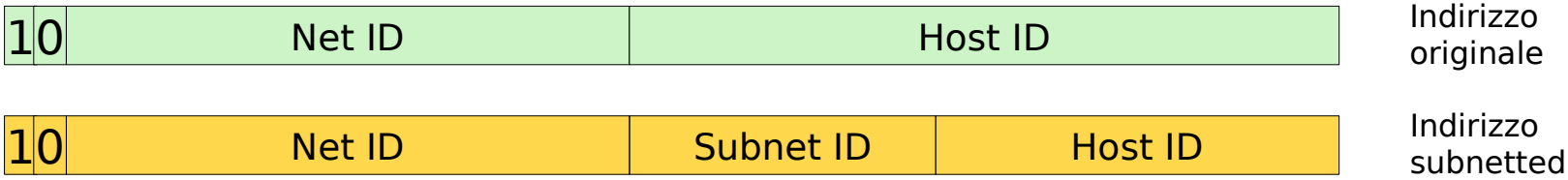
- Per configurare un host IP occorre specificare le seguenti entità:
  - Indirizzo IP
  - Subnet mask
  - Default gateway
  - Indirizzo IP del nameserver
- La possibilità alternativa è quella di utilizzare il protocollo DHCP e lasciare gestire la definizione di queste informazioni a tale protocollo
  - Questa soluzione, oltre a semplificare la fase di configurazione permette di gestire facilmente la gestione della rete (posso cambiare gli indirizzi IP e/o i parametri di configurazione senza intervenire sui client, cosa molto importante nel caso di grandi organizzazioni)

Configurazione IP

- Un errore in fase di configurazione dei parametri IP genera malfunzionamenti:
  - Se si sbaglia la definizione del default gateway le applicazioni locali funzionano, mentre quelle che richiedono connessioni all'esterno della rete locale no, poiché non si è in grado di raggiungere il giusto gateway.
  - Un errore nella subnet mask può generare problemi di connettività. E' possibile, anche se altamente sconsigliabile, che la definizione della subnet mask differisca tra gli host della rete. L'effetto risultante può essere quello di comportamenti non predicibili.

Indirizzamento con Subnet

- L’indirizzamento con Subnet introduce un nuovo livello gerarchico negli indirizzi IP
- E’ una tecnica trasparente per le reti ed i router remoti
- Semplifica la gestione delle varie LAN di un’organizzazione
- Viene definita la subnet mask per trovare il numero associato alla rete



Schema per subnetting

- Consideriamo l'indirizzo di classe B di cui dispone la nostra Università: 141.250.0.0
- Nello schema generale di subnet che viene utilizzato oggi, in genere ad ogni struttura dell'Università viene assegnato un indirizzo equivalente ad una classe C, usando una subnet mask di 255.255.255 (o /24). Vediamo come si calcola l'indirizzo della subnet per l'indirizzo: 141.250.5.25

IP:	**141**	**250**	**5**	**25**
	10001101	11111010	00000101	00011001
Mask:	**255**	**255**	**255**	**0**
	11111111	11111111	11111111	00000000
AND:				
	10001101	11111010	00000101	00000000

Bitwise AND operation

Subnet: 141.250.5.0

Schema per subnetting (i)

- Se volessimo subnet più piccole (con circa 100 host) dovremmo adottare una subnet mask più restrittiva, 255.255.255.128 o /25. Avremmo due reti: 141.250.5.0 e 141.250.5.128
- L'intervallo degli indirizzi host in questo secondo caso andrebbe da

141	250	5	129
10001101	11111010	00000101	10000001

141	250	5	254
10001101	11111010	00000101	11111110

La submet mask sarebbe 255.255.255.128, il primo indirizzo è 141.250.5.129, l'ultimo 141.250.5.254. L'indirizzo broadcast è 141.250.5.255

Subnetting

- Un indirizzo IP di una rete può essere gestito come un insieme di sottoreti introducendo una *subnet mask più restrittiva* che assegni i bit più significativi della parte host alla parte di network, ottenendo da un indirizzo di una certa classe, un insieme di sottoreti di classe inferiore e conseguentemente di dimensioni inferiori.

Es: **Rete di classe C 194.143.128**

n. bit	rete	ind. Rete	num. Host
25	194.143.128	**.{0, 128}**	**128**
26	194.143.128	**.{0,64,128,192}**	**64**
27	194.143.128	**.{0,32,64,96,128,160,192,224}**	**32**
28	194.143.128	**.{0,16,32,48,64,80,96,112,128,144,160,176,192,208,224,240}**	**16**
29	194.143.128	**.{0,8,16,24,32,40,48,56,64,72,80,86,96,104,112,120,128,136,144,150,160,168,176,184,192,200,208,216,224,232,240,248}**	**8**

Subnet mask

- La subnet mask deve avere per la parte rete tutti i bit a 1 (senza 0 nella sequenza della parte di rete)
- Questo implica che i possibili indirizzi di una rete di classe C, ad esempio 194.143.128.0, sono

0 11111111111111111111111 (/24)

0, 128 11111111111111111111111 (/25)

0,64,128, 192 11111111111111111111111 (/26)

0,32,64,96,128,160,192,224 11111111111111111111111 (/27)

0,16,32,48,64,80,96,112,128,144,160,176,
192,208, 224,240 11111111111111111111111 (/28)

0,8,16,24,32,40,48,56,64,72,80,88,96,104,112, 120,128,136,144,152,160,168,176,184,192,
200,208,216,224,232,240,248 11111111111111111111111 (/29)

0,4,8,12,16,20,24,28,32,36,40,44,48,52,56,60,64,68,72,76,80,84,88,92,96,100,104,108,112, 116,
120,124,128,132,136,140,144,148,152,156,160,164,168,172,176,180,184,188,192,196,200,204,208,212,216,
220,224,228,232,236,240,244,248,252 11111111111111111111111 (/30)

0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,32,34,36,36,38,40,42,44,46,48,50,52,54,56,58,60,62,64,66,68,70,72,74,76,78,80,82,84,86,88,90
,92,94,96,98,100,102,104,106,108,110,112,114,116,118,120,122,124,126,128,130,132,134,136,138,140,142,144,
146,148,150,152,154,156,158,160,162,164,166,168,170,172,174,176,178,180,182,184,186,188,190,192,194,196,198,200,202,
204,206,208,210,212,214,216,218,220,222,224,226,228,230,232,234,236,238,240,242,244,246,248,250,252

11111111111111111111111 (/31)

Esempio: 194.143.128.0/26

- 11111111 11111111 11111111 11 (Subnet mask:255.255.255.192)
- 11000010 10001111 10000000 00 0 (Rete 194.143.128.0)

000000 0 ind. rete 1

111111 63 ind. broadcast 1

- 11000010 10001111 10000000 01 64 (Rete 194.143.128.64)

000000 64 ind. rete 2

111111 127 ind. broadcast 2

- 11000010 10001111 10000000 10 128 (Rete194.143.128.128)

000000 128 ind. rete 3

111111 191 ind. broadcast 3

- 11000010 10001111 10000000 11 192 (Rete 194.143.128.192)

000000 192 ind. rete 4

111111 255 ind. broadcast 4

Subnets

- La realizzazione di subnet comporta l'alterazione del comportamento standard della classe primaria IP mediante introduzione di una subnet mask che ne alteri il significato.
- La decisione di creare una sottorete dipende da aspetti topologici ed organizzativi.
  - ragioni topologiche:
    - ✓ **superamento limiti di distanza:** a seconda del tipo di rete considerata occorre considerarne le caratteristiche fisiche e le specifiche di interfaccia. Ad esempio ogni segmento UTP deve essere al massimo lungo 100m. Da notare che la lunghezza dei cavi della rete è data dalla somma di tutti i segmenti, incluse le bretelle di giunzione negli armadi e i segmenti che vanno dalla presa di rete all'interfaccia di rete dei singoli host.
    - ✓ **connessione di reti fisiche diverse:** router IP possono essere usati per collegare reti che hanno una diversa tecnologia o un diverso mezzo trasmissivo (da token ring a ethernet o tra ethernet con diverso mezzo trasmissivo, es: fibra-cavo coassiale).
    - ✓ **filtro del traffico fra reti:** il traffico locale rimane nella sottorete locale, solo il traffico verso altre reti è inviato al gateway.

Subnetting e supernetting

- La realizzazione di subnet comporta l'alterazione del comportamento standard della classe primaria IP mediante introduzione di una subnet mask che va applicata all'indirizzo IP e ne modifica il significato primario
- La subnet mask altera le informazioni standard relative alla rete ed all'host presente nell'indirizzo primario
- Mediante subnetting si suddivide una rete primaria in più sottoreti differenti che diventano entità autonome dal punto di vista del routing e del TCP/IP
- Mediante supernetting si accorpano più reti fisiche primarie diverse in un'unica rete per semplificare le informazioni di routing da trasmettere ai router

Subnetting: perché?

- Ragioni organizzative:
  - ✓ amministrazione: le sottoreti possono essere usate per delegare la gestione degli indirizzi, il controllo e la diagnostica a piccole entità.
  - ✓ visibilità di strutture: singole strutture (es. dipartimenti universitari) necessitano di realizzare la propria autonomia al fine di meglio organizzare i servizi
  - ✓ isolamento del traffico: per motivi di sicurezza è preferibile isolare il traffico locale in modo tale da renderlo inaccessibile all'esterno.
- Ragioni tecniche:
  - ✓ ottimizzazione dell'uso dello spazio di indirizzamento IP
  - ✓ limitazione del dominio di broadcast IP
  - ✓ limitazione degli effetti di eventuali malfunzionamenti

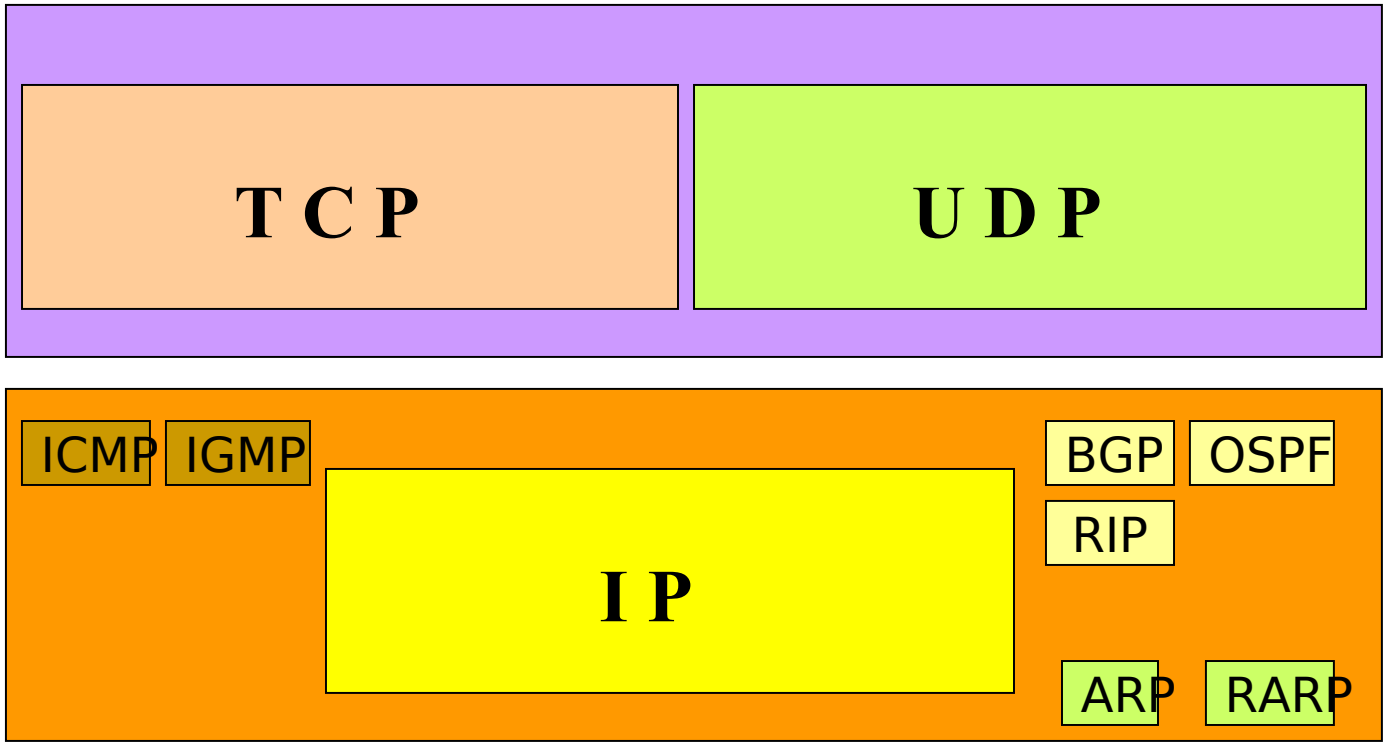
Piano di indirizzamento IP

- E’ il documento che il network administrator deve scrivere e tenere aggiornato per descrivere l’utilizzo del proprio spazio di indirizzamento IP. Es:

194.143.128.0 /26	255.255.255.192	rete interna1
194.143.128.64 /26	255.255.255.192	rete interna2
194.143.128.128/25	255.255.255.128	rete interna3
194.143.129.0 /30	255.255.255.252	punto-punto1
194.143.129.4 /30	255.255.255.252	punto-punto2
194.143.129.8 /29	255.255.255.248	rete lab1
194.143.129.16 /28	255.255.255.240	rete lab2
194.143.129.32 /27	255.255.255.224	rete lab3
194.143.129.64 /26	255.255.255.192	rete lab3
194.143.129.128/25	255.255.255.128	rete amm1

Famiglia di Protocolli TCP/IP

Famiglia di Protocolli TCP/IP



Address Resolution Protocol (ARP)

- Considerando il Modello di Riferimento ISO/OSI, quando un pacchetto di livello 3 (Network) deve essere incapsulato nel protocollo di livello 2 (Data Link, in genere Ethernet) deve inserire nell'header del pacchetto l'indirizzo Data Link.
- Ne consegue che un host Internet può comunicare con un altro host solo se ne conosce l'indirizzo fisico del protocollo di rete locale (es: l'indirizzo ethernet).
- In particolare occorre conoscere l'indirizzo fisico dell'host di destinazione se questi appartiene alla stessa rete del mittente, oppure quello del gateway, se l'host destinatario appartiene ad altra rete.
- Gli indirizzi fisici (Ethernet) non possono essere desunti, in quanto tali indirizzi vengono preassegnati ai produttori hardware e sono specifici della scheda di rete (tale indirizzo può comunque facilmente essere alterato da persone esperte).

Address Resolution Protocol (ARP)

- I programmi applicativi in genere conoscono solo il ***nome*** dell'host o il suo indirizzo IP
- L'ARP fornisce il servizio di risolvere la corrispondenza Indirizzo IP-Indirizzo fisico.
- L'host A che ha bisogno di conoscere l'indirizzo fisico dell'host B, invia un pacchetto broadcast chiedendo all'host il cui indirizzo IP è specificato nel pacchetto broadcast, di rispondere fornendo il proprio indirizzo fisico.
- Esiste in ciascuna macchina una ***cache*** che memorizza gli indirizzi risolti via protocollo ARP per le consultazioni successive.
- La cache ARP fornisce un esempio di *soft state*, una tecnica usata nei protocolli di rete ove le informazioni possono diventare obsolete senza preavviso. Il problema viene gestito mediante dei timer che fanno comunque scadere la validità dell'informazione.

ARP

- L'host che effettua la richiesta ARP via broadcast include il proprio indirizzo fisico nel pacchetto broadcast, cosicché tutti gli host possono aggiornare l'informazione nella propria cache.
- Il protocollo è composto funzionalmente dai processi di:
  - determinazione degli indirizzi fisici quando si trasmette un pacchetto da un host ad un altro
  - risposta a richieste ARP di altre macchine
- Occorre considerare che il meccanismo di richiesta via broadcast può generare problemi (metodo best-effort di ethernet, errori hardware, etc)
  - L'aggiornamento dei dati in cache allo scadere del timer può portare ritardi (jitter): si effettua la rivalidazione anticipata
  - Impatto sull'operatività degli altri protocolli in presenza di richieste ARP pendenti

Reverse Address Resolution Protocol (RARP)

- Le workstation diskless hanno bisogno di caricare il sistema operativo e la configurazione da uno o più server mediante effettuazione di una richiesta broadcast che utilizza il protocollo denominato RARP
  - l'host spedisce la richiesta RARP ad un *server* mediante un pacchetto broadcast nel quale è evidenziato il MAC address dell'host mittente ed attende dallo stesso una risposta (che include l'IP address a partire dall'indirizzo fisico trasmesso in fase di richiesta RARP)
  - Se la richiesta è ripetuta, rispondono anche i server secondari
- L'identificatore unico è l'indirizzo fisico della macchina
- Richiesta e risposta ARP differiscono per il campo *tipo* della frame
- Il server nel rispondere scambia gli indirizzi mittente-destinatario, cambia il contenuto del campo tipo e trasmette l'indirizzo IP

Il protocollo ICMP (1)

- Il protocollo Internet Control Message Protocol (ICMP) è stato progettato per riportare anomalie che accadono nel routing dei pacchetti IP e per verificare lo stato della rete.
- I vari tipi di messaggi ICMP sono:

Codice	Messaggio	Codice	Messaggio
0	Echo Reply ✥	13	Timestamp Request
3	Destination Unreachable ▯	14	Timestamp Replay
4	Source Quence	15	Information Request
5	Redirect	16	Information Replay
8	Echo Request ✥	17	Address Mask Request
11	Time Exceeded for a Datagram ▯	18	Address Mask Replay
12	Parameter Problem on a Datagram ▯		

▯ messaggi che riportano anomalie

✥ messaggi di verifica della raggiungibilità di un nodo

Il protocollo ICMP (2)

- Il messaggio Redirect indica una condizione di stimolo per un instradamento migliore dei pacchetti, in quanto un router è stato attraversato inutilmente (ha dovuto ritrasmettere il messaggio sulla stessa rete da cui lo ha ricevuto). Quando un host riceve un pacchetto di routing redirect associa un router diverso da quello di default a quella destinazione.
- I messaggi Mask Request e Address Mask Reply sono stati introdotti per permettere ad una interfaccia di scoprire automaticamente la netmask usata in quella rete

IP multicasting

- IP multicasting è definito come la trasmissione di un datagram ad un gruppo di host: un insieme di host identificato da un indirizzo IP di destinazione
- Un datagram multicast è inviato a tutti i membri del suo gruppo di host di destinazione con la stessa affidabilità *best effort* di un datagram unicast: il datagram non è garantito che arrivi a tutti i membri del gruppo di destinazione o nello stesso ordine rispetto ad altri datagram.
- Gli appartenenti al gruppo possono cambiare dinamicamente: gli host possono aggiungersi o uscire dal gruppo senza limitazioni, anche se è possibile definire una chiave di accesso che renda l'ingresso nel gruppo selettivo.

IP multicasting

- Un gruppo di host può essere permanente (in questo caso ha un indirizzo IP ben noto ed assegnato amministrativamente) o transitorio.
- La creazione di gruppi transitori ed il mantenimento delle informazioni relative alla composizione dei gruppi è responsabilità dei multicast agents, che sono entità che girano sui routers o su host speciali.
- I multicast agents sono responsabili anche dell'invio in Internet dei datagram multicast. Se un host di destinazione è in una rete diversa rispetto a quella degli altri host, il multicast agent diventa esso stesso destinatario del datagram e lo consegna ad altri agenti fino alla consegna all'host destinatario

Internet Group Management Protocol (IGMP)

- IGMP è il protocollo che supporta le funzioni di IP multicasting, consentendo ad un host di creare, unirsi ad un gruppo multicast o di abbandonarlo.
- IGMP provvede anche all'invio di datagram IP ad un gruppo di host
- Esso richiede l'implementazione di IGMP e l'estensione di servizi IP e della rete locale al fine di gestire IP multicast.
- E' definito negli RFC966, RFC1112, RFC1122, RFC1812, RFC2236, RFC2715, RFC2933, RFC3228

User Datagram Protocol (UDP)

- UDP è un protocollo di trasporto molto semplice, di trasmissione e ricezione di datagram, che offre due servizi all'IP:
  - Multiplexing: permette la condivisione su un host dei datagram IP che provengono da diversi host
  - Controllo dell'errore sui dati
- UDP conosce il metodo per distingere tra le diverse applicazioni che vengono eseguite sull'host.
- UDP è un protocollo connectionless: non c'è handshaking e non c'è connessione.
- Ha un basso overhead per la gestione dell'header, ed i datagram possono essere persi o essere fuori controllo
- Non c'e controllo di flusso, non c'e' controllo della congestione

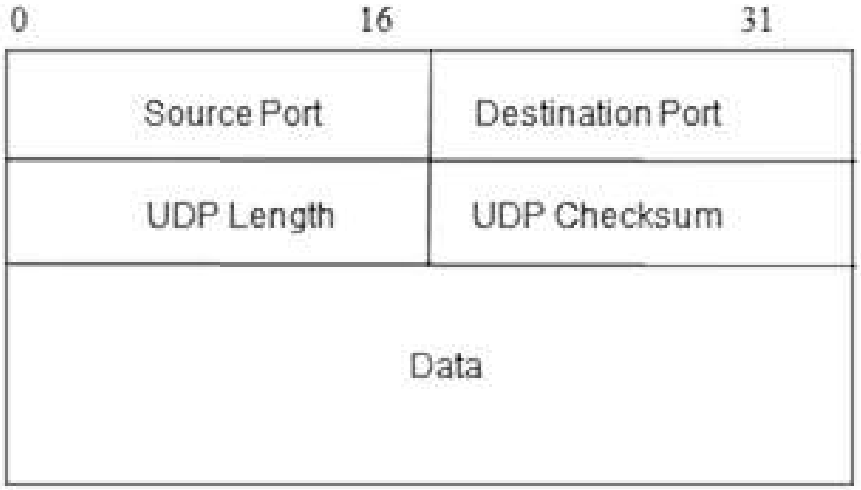
User Datagram Protocol (UDP)

- Per consentire la identificazione del processo al quale destinare il datagram viene introdotto il concetto di *portnumber*: un numero intero positivo che rappresenta diversi punti di destinazione astratti che vengono indirizzati dagli host internet per implementare i diversi servizi ed accedere alle diverse applicazioni. Il sistema operativo degli host si fa carico di fornire dei meccanismi di interfaccia che i processi utilizzeranno per specificare una porta o per accedervi.
- Per comunicare con una porta esterna l'host che trasmette deve conoscere l'indirizzo IP del destinatario e il numero di porta del protocollo della destinazione all'interno di tale host.
- Applicazioni più diffuse:
  - Multimedia (RTP, Real Time Protocol)
  - Servizi di rete (DNS, RIP, SNMP, etc)

UDP

- UDP fornisce un servizio di consegna non affidabile e senza connessione, utilizzando l'IP per trasportare i messaggi tra le macchine. Esso offre la capacità di distinguere tra più destinazioni all'interno di un certo host, tramite il portnumber.
- Un protocollo applicativo che impieghi l'UDP accetta l'intera responsabilità di gestire il problema dell'*affidabilità*, che comprende la perdita di messaggi, la loro duplicazione, il ritardo, la consegna fuori ordine e la perdita di connettività.
- UDP è un protocollo a livello di *trasporto* responsabile *della differenziazione tra le varie provenienze e destinazioni all'interno di un singolo host*, ed è posto sopra al livello IP (responsabile della consegna delle informazioni tra una coppia di host in internet) e sotto ai protocolli applicativi
- Applicazioni che usano UDP funzionano bene in ambito locale e falliscono quando utilizzati attraverso un'internet di dimensioni maggiori

UDP datagram

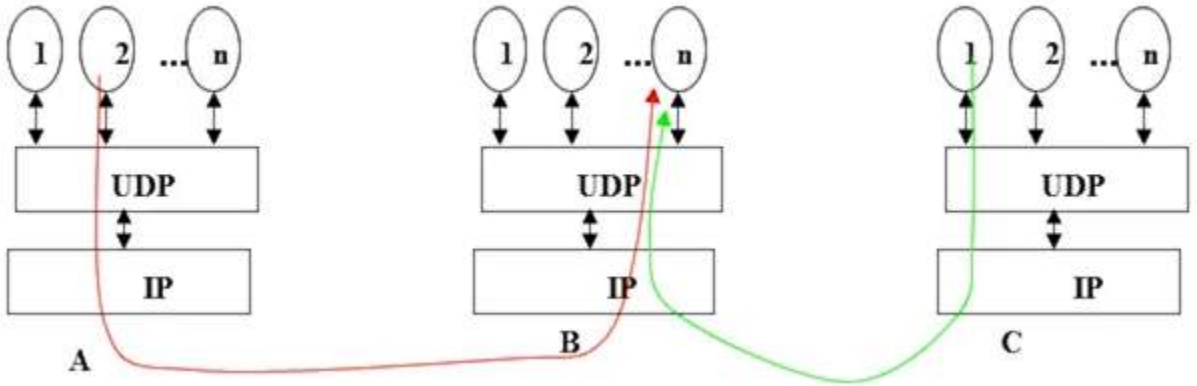


0-255: Well-known ports
256-1023: Less well-known ports
1024-65535: ephemeral client ports

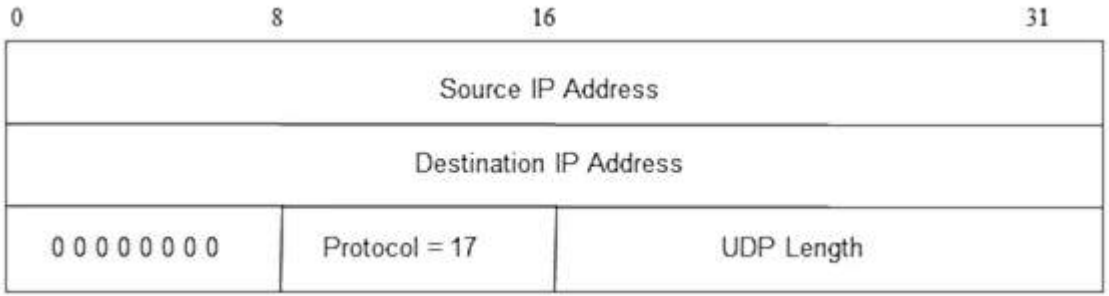
- **UDP length**: lunghezza del Datagram incluso header e dati
- **UDP checksum**: controllo dell'errore nel datagram UDP (opzionale)

UDP De-multiplexing

- Tutti datagram che arrivano all'host B con portnumber n sono passati allo stesso processo
- Il numero source port non viene utilizzato quando si effettua il de-multiplexing



UDP checksum



UDP pseudo header

- Il checksum UDP permette di individuare errori di comunicazione tra due host
- Include uno pseudo-header seguito dal datagram UDP che contiene l'indirizzo IP del destinatario per intercettare false consegne di pacchetti. L'host ricevente ricalcola il checksum e se il risultato è errato cancella il pacchetto senza segnalare errori.
- L'uso dell'UDP checksum è facoltativo, ma i due host che comunicano devono avere il checksum abilitato

Trasmission Control Protocol (TCP)

- TCP fornisce un servizio di **consegna affidabile delle informazioni con connessione.**
- TCP è un singolo protocollo di applicabilità generale che contribuisce ad isolare i programmi applicativi dai dettagli del networking e rende possibile la definizione di un'interfaccia uniforme per il servizio di trasferimento di stream.
- L'interfaccia tra i programmi applicativi e il servizio di consegna affidabile del TCP/IP può essere descritta da
  - *Orientamento dello stream*: quando due programmi applicativi trasferiscono dati, questi vengono immagazzinati come sequenze di bit (stream) suddivisi in byte. Il servizio di consegna dello stream passa dal mittente al destinatario esattamente la stessa sequenza di ottetti.
  - *Connessione di circuito virtuale*: il trasferimento di stream è analogo ad una chiamata telefonica: solo quando mittente e destinatario hanno verificato la sussistenza delle condizioni necessarie ha inizio il trasferimento

TCP

- *Trasferimento bufferizzato*: anche se il programma applicativo genera le informazioni un ottetto alla volta, il trasferimento accorpa un insieme di ottetti, in modo da otttimizzare la trasmissione. Se il programma genera invece grandi blocchi di dati, il trasferimento potrebbe avvenire a blocchi più piccoli per ottimizzare la trasmissione stessa.
- *Stream non strutturata*: il servizio di stream del TCP non rispetta eventuali strutture presenti in dati strutturati. Sono i programmi che usano il servizio di trasferimento di stream che devono comprendere la struttura dei dati trasmessi
- *Connessione full-duplex*: Le connessioni fornite dal servizio di stream consentono il trasferimento simultaneo in entrambe le direzioni

- Il TCP garantisce l'affidabilità mediante una tecnica chiamata *riscontro positivo con ritrasmissione*
- Per ottimizzare la trasmissione il TCP usa la tecnica della *finestra scorrevole*: si continua a trasmettere stream senza verificarne il riscontro sino a che ci si muove all'interno di una finestra predefinita di stream

TCP

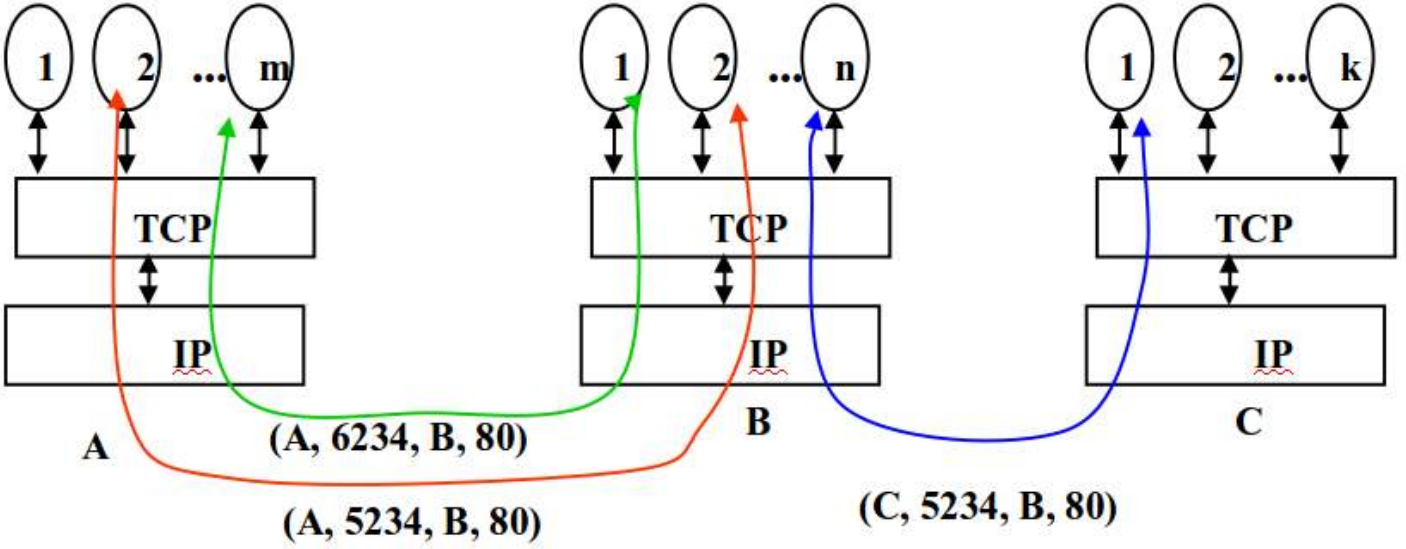
- Anche il TCP usa i portnumber per identificare il flusso di dati tra le varie applicazioni di un host.
- Nel caso del TCP il meccanismo di comunicazione è però molto più complesso che nel caso dell'UDP, essendo stato definito un concetto di *astrazione di connessione*: gli oggetti da identificare sono connessioni virtuali di circuiti, non singole porte.
- Il TCP usa una coppia di valori per identificare una connessione: l'indirizzo IP dell'host e la porta dell'applicazione.
- L'insieme *indirizzo IP - portnumber* è chiamato **socket**
- Questo approccio fa sì che un certo portnumber possa essere condiviso contemporaneamente da più host, aumentando molto l'efficienza di Internet

TCP

- Servizio byte stream affidabile
- Complesso meccanismo di trasmissione tra ricevente e trasmettitore:
  - Connection oriented, full-duplex. Connessione unicast tra server e client
  - Sono necessarie attivazione della connessione, verifica dello stato della connessione e chiusura della la connessione
  - l'overhead per la gestione dell'header è maggiore, ma molti protocolli usano TCP per la sua affidabilità
  - Controllo dell'errore, controllo del flusso, controllo della congestione
  - Il ritardo è maggiore rispetto all'UDP
- Molte applicazioni utilizzano il TCP per la sua affidabilità
  - HTTP, SMTP, SSH, POP, IMAP ...

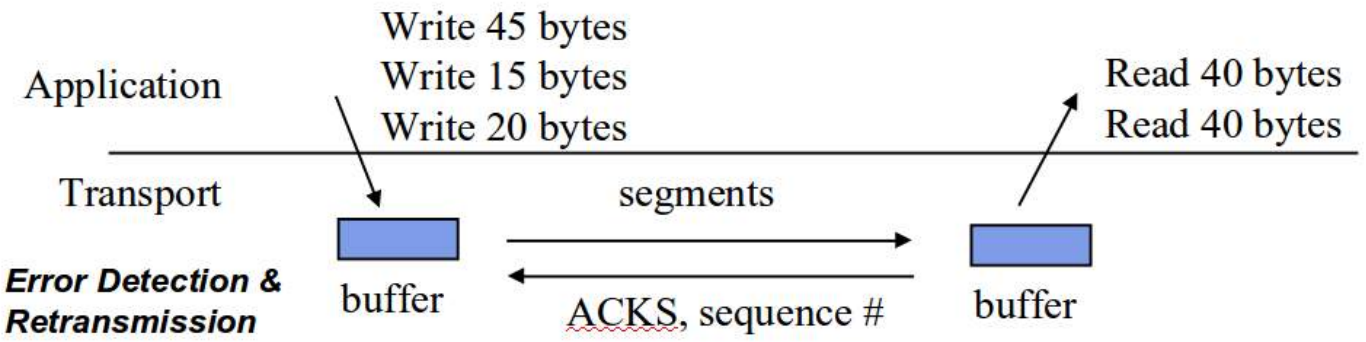
TCP multiplexing

- La connessione TCP è specificata da una 4-tupla:
  - Indirizzo mittente, porta mittente, indirizzo destinatario, porta destinatario
- TCP consente il multiplexing di connessioni multiple tra sistemi per consentire nello stesso tempo l'uso ottimale delle varie risorse.



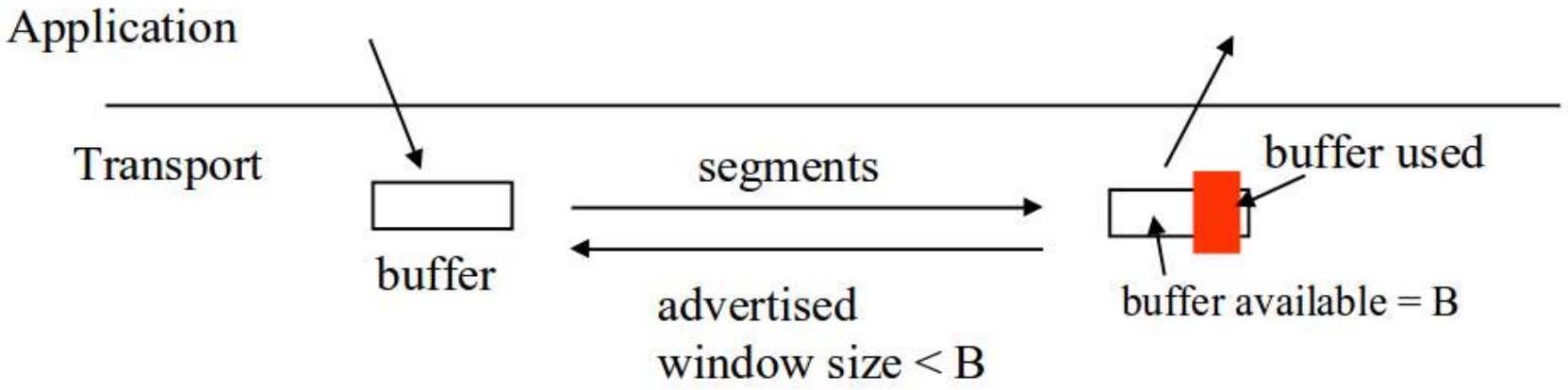
Servizio affidabile di trasporto di un flusso di byte

- Trasferimento di flussi di dati
  - Trasferisce un flusso continuo di byte attraverso la rete
  - Raggruppa i byte in segmenti
  - Trasmette i segmenti nel modo opportuno
- Affidabilità: controllo degli errori per far fronte a problemi di trasferimento IP



Controllo di flusso

- Le limitazioni dei buffer e il disallineamento delle velocità trasmissive possono generare perdite di dati
- Il ricevente controlla la velocità con la quale il mittente trasmette per prevenire il buffer overflow del ricevente



TCP Header

- Window size
  - 16 bit per annunciare le dimensioni della finestra
  - Usata per controllare il flusso
  - Il mittente accetterà bytes da ACK a ACK+window
  - Dimensioni massime della window 64K
- TCP checksum

TCP Header

0								1								2								3							
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source port																Destination port															
Sequence number																															
Acknowledgment number (if ACK set)																															
Data offset			Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
Checksum																Urgent pointer (if URG set)															
Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

TCP: gestione della connessione

- Può accadere che pacchetti relativi a comunicazioni precedenti arrivino in ritardo complicando il calcolo dei pacchetti duplicati.
- TCP risolve questo problema tramite un Initial Sequence Number (ISN), un campo di 32 bit scelto casualmente.
- TCP esegue un periodo di timeout alla fine della connessione, chiamato maximum segment lifetime (MSL), in genere 2 minuti.
- ISN viene stabilito durante il setup della connessione (il bit SYN è posto a 1)
- Il ricevente risponde con un Acknowledgment number che indica il Sequence Number del prossimo byte che deve ricevere il destinatario. Il flag ACK deve essere impostato.

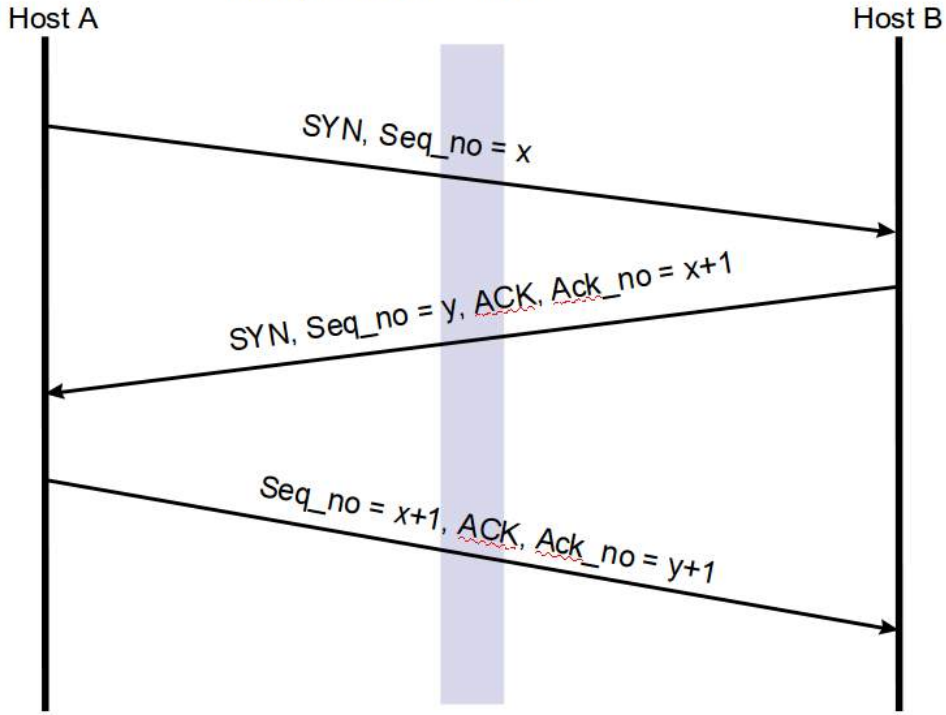
TCP: bit di controllo

- 6 bit flags:
  - URG: urgent pointer flag
  - ACK: acknowledgemnt of the communicaion
  - PSH: override TCP Buffering
  - RST: reset connection
  - SYN: establish connection
  - FIN: close connection

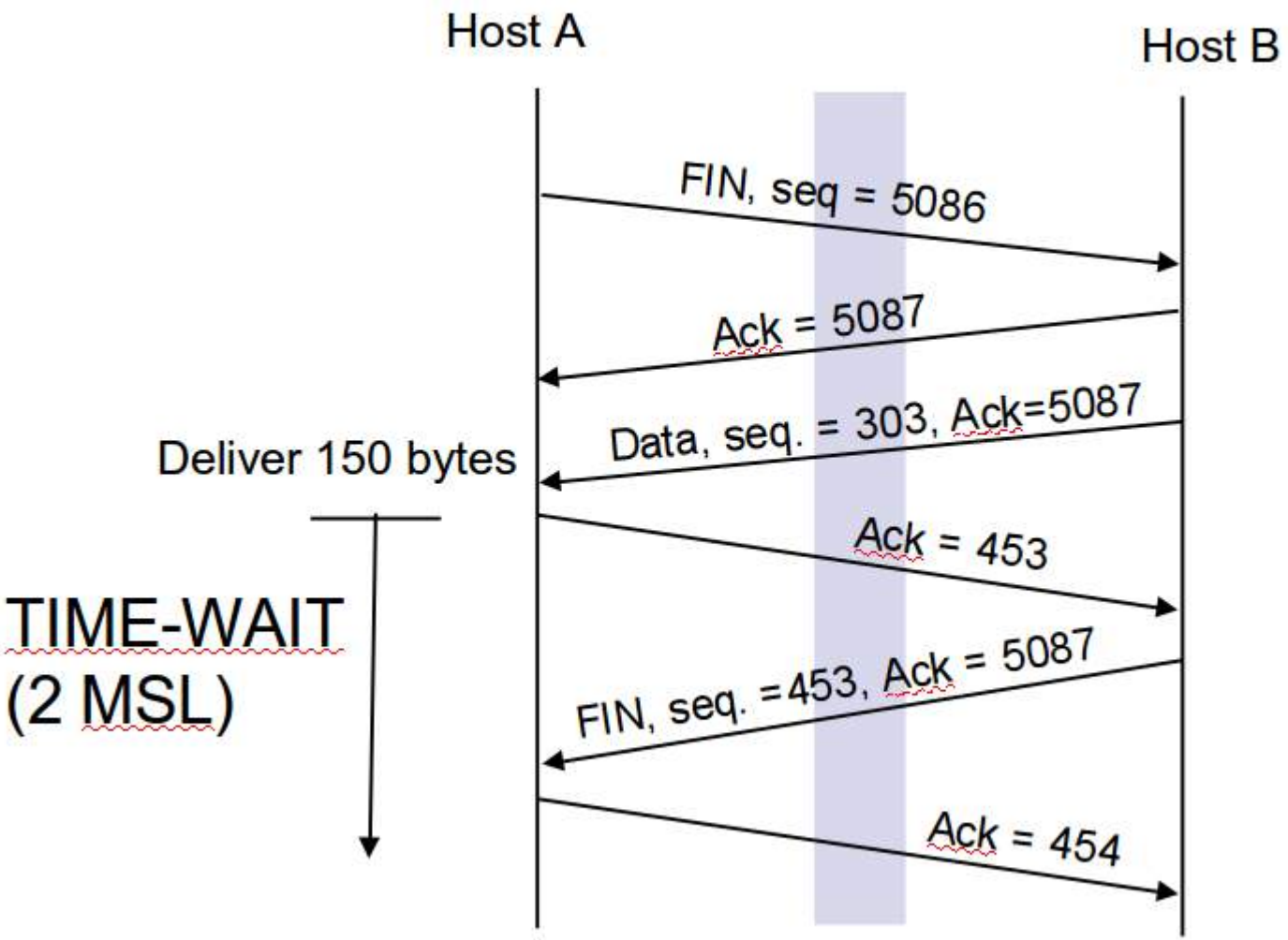
TCP 3ways handshake

EVENT
Host A **sends** a TCP **SYN**chronize packet to Host B
Host B receives A's **SYN**
Host B **sends** a **SYN**chronize-**ACK**nowledgement
Host A receives B's **SYN-ACK**
Host A **sends** **ACK**nowledge
Host B receives **ACK**.
TCP socket connection is ESTABLISHED.

- "Three-way Handshake"
- ISN's protect against segments from prior connections



"Graceful Close"



TCP/IP Routing

Routing

- Il routing è l'azione di scambiare informazioni in una rete da una sorgente ad una destinazione, incontrando almeno un nodo intermedio
- Il routing coinvolge due attività di base:
  - determinare il percorso ottimale di routing
  - trasportare gruppi di informazioni (chiamati pacchetti) attraverso una rete
- La prima attività può risultare molto complessa
- Il routing riguarda il livello 3 del modello di riferimento ISO/OSI

Routing

- Si introduce il concetto di metric per indicare una modalità standard di misura, come la lunghezza di un percorso in termini di gateway attraversati, per stabilire il percorso ottimale da calcolare da parte di un protocollo di routing
- Un router considera l'associazione destination/next_hop per calcolare quale sistema intermedio rappresenta il miglior percorso
- Ricevuto un pacchetto il router calcola in base alle sue informazioni il next hop

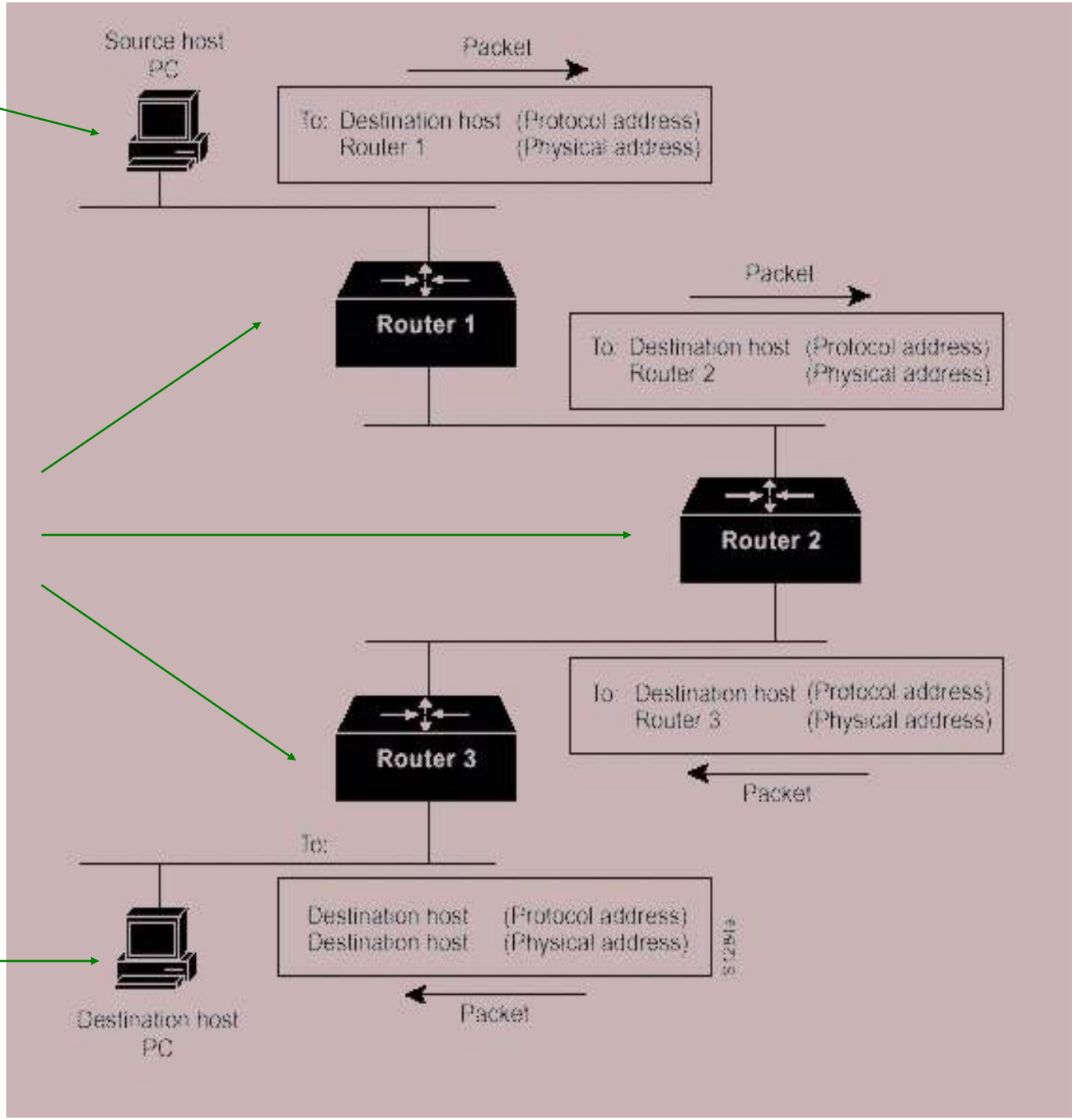
Routing

- I router comunicano tra loro e mantengono aggiornate le *routing tables* mediante la trasmissione di vari messaggi
- Il messaggio *routing update* è uno di questi e consiste in un messaggio contenente tutta o parte di una routing table. Analizzando i routing update un router è in grado di costruire un disegno dettagliato della topologia della rete
- Il messaggio *link-state advertisement* è un altro esempio di messaggio tra router e serve ad informare i router che usano il protocollo OSPF dello stato del link del mittente, oltre che a consentire agli stessi il calcolo del miglior percorso da seguire per una determinata destinazione

End System (ES)

Intermediate Systems (IS)

End System (ES)



Routing algorithms

- Gli algoritmi di routing devono possedere uno o più dei requisiti seguenti:
  - ottimali deve scegliere la migliore strada
  - semplici e con basso overhead deve farlo consumando meno risorse possibile
  - robusti e stabili devono comportarsi correttamente in condizioni inusuali e mai viste prima.
  - rapidi nella convergenza la scelta del percorso ottimale deve avvenire subito e con il minor sforzo possibile.
  - Flessibili devono adattarsi facilmente a diverse condizioni.

Routing algorithms

- Gli algoritmi di routing vengono classificati in base al comportamento rispetto alle classi seguenti:
  - statici vs. dinamici
  - single-path vs. multi-path
  - piatti vs. gerarchici
  - Host-intelligent vs. router-intelligent
  - Intradomain vs. interdomain
  - Link state vs. distance vector

Routing metrics

- Gli algoritmi di routing usano una o diverse delle seguenti caratteristiche per determinare il percorso ottimale:
  - *Path Length*
  - *Reliability*
  - *Delay*
  - *Bandwidth*
  - *Load*
  - *Communication Cost*

Routing table

- I gateway instradano i dati tra diverse reti
- Gli host prendono decisioni di instradamento nel modo seguente:
  - Se l'host di destinazione è sulla rete locale, i dati vengono spediti all'host di destinazione;
  - Se l'host di destinazione è su una rete remota, i dati vengono mandati al gateway locale.
- Il protocollo IP basa le sue decisioni di instradamento sulla parte rete dell'indirizzo IP

Routing table

- Analisi dell'indirizzo IP fatta dall'host:
  - determina il tipo di classe dell'indirizzo IP (bit più significativi)
  - controllo rete di destinazione, se è locale (sottorete) applica all'indirizzo di destinazione la subnet mask
  - cerca la rete di destinazione nella routing table
  - instrada i pacchetti di dati seguendo il percorso indicato nella tabella di routing (interfaccia).
- In ambiente Unix il comando per visualizzare la tabella di routing è:

```
netstat -nr
```

Routing table (host Unix)

Destination	Gateway	Flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	UH	1	298	lo0
default	128.66.12.1	UG	2	50360	en0
128.66.12.0	128.66.12.2	U	40	98379	en0
128.66.2.0	128.66.12.3	UG	4	1179	en0
128.66.1.0	128.66.12.3	UG	10	1113	en0
128.66.3.0	128.66.12.3	UG	2	1379	en0
128.66.4.0	128.66.12.3	UG	4	1119	en0

dove: **Destination** = rete o host di destinazione
Gateway = gateway da usare per la specifica destinazione
Flags = U : route in linea e attiva
H : route per host spec. (non per una rete)
G : route che usa un gateway
D : route aggiunta da una ICMP redirect
Refcnt = n.ro di volte che la route è stata usata
Use = n.ro pacchetti trasmessi su quella route
Interface = nome dell'interf. di rete usata per la route

Routing table

- Esistono tre tipi di definizione di routing:
  - minimale: le operazioni minime di aggiornamento della tabella di routing che vengono effettuate al momento della definizione di una interfaccia
  - statico: L'instradamento viene gestito mediante informazioni di routing predefinite e costanti. Può essere sufficiente in configurazioni ove la topologia è molto semplice (rete connessa in un solo modo al backbone)
  - dinamico: L'instradamento viene gestito via software da protocolli di routing che si adattano le informazioni di routing a tutti i cambiamenti della rete. I protocolli di routing utilizzano dei pacchetti per lo scambio delle informazioni necessarie all'aggiornamento delle informazioni in tabella.

Routing table

- Ovviamente in un dato istante di tempo e a seconda della complessità della configurazione, le informazioni attuali potranno provenire da tutti e tre i tipi di definizione
- Le informazioni assunte mediante protocolli di routing dinamici prendono il sopravvento su quelle statiche, qualora tra queste informazioni esistano contraddizioni
- In un router possono essere eseguiti contemporaneamente diversi protocolli di routing
- In alcuni casi (cfr CISCO) è possibile *iniettare* delle informazioni da un protocollo di routing dinamico all'altro, in modo da controllare la *distribuzione delle informazioni di routing*

Comandi per routing statiche

- Cisco:

  per inserire una route statica:

  `ip route network subnet gateway distance`

  `ip route 141.250.4.0 255.255.255.0 141.250.9.3 2`

  per visualizzare la routing table:

  `sh ip route [network]`

- Linux:

  per inserire una route statica:

  `route add network subnet gateway`

  `route add 141.250.4.0 255.255.255.0 141.250.9.3`

  per visualizzare la routing table:

  `netstat -nr`

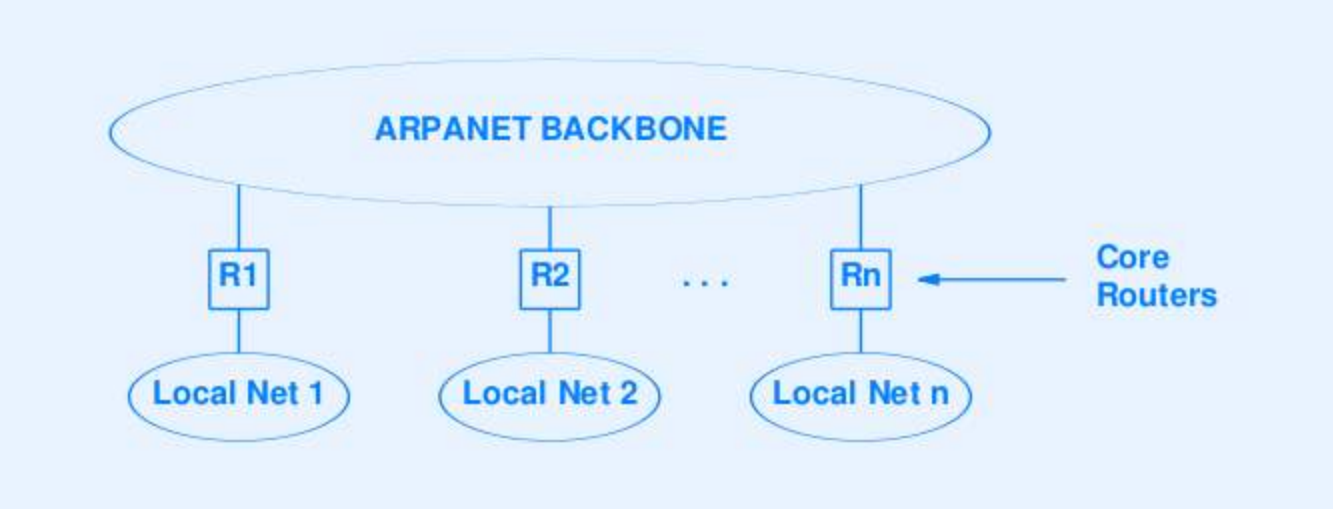
Routing table

- La routing table permette ad un router di operare le corrette scelte per indirizzare I pacchetti
- La routing table riceve informazioni da due sorgenti:
  - Dal file di configurazione creato dall'amministratore di rete e salvato sul disco del dispositivo e interpretato in fase di inizializzazione dell'hardware
  - Da protocolli dinamici di aggiornamento (protocolli di routing)
- Gli host tendono a mantenere congelata la tabella di routing (non eseguono protocolli di routing dinamici)
- I router eseguono protocolli di routing dinamici per ricevere gli aggiornamenti sulle destinazioni delle varie reti e calcolare I corretti percorsi di routing dinamicamente

Routing con informazioni parziali

- Nel caso di router interni ad un AS (Interior Gateway protocols, IGP) le informazioni che un singolo router possiede sono assolutamente **parziali**: infatti il router conosce esplicitamente soltanto i percorsi per raggiungere le reti ad esso collegate e le routing statiche, che indirizzano reti collegate a dei gateway.
- Il router in questione si affida al *default router* per istradare correttamente i pacchetti che sono destinati a reti che lui non conosce.
- Il routing con informazioni parziali permette localmente a dei router di modificare autonomamente alcune istruzioni di routing, introducendo il rischio di inconsistenze che possano rendere inaccessibili certe reti.

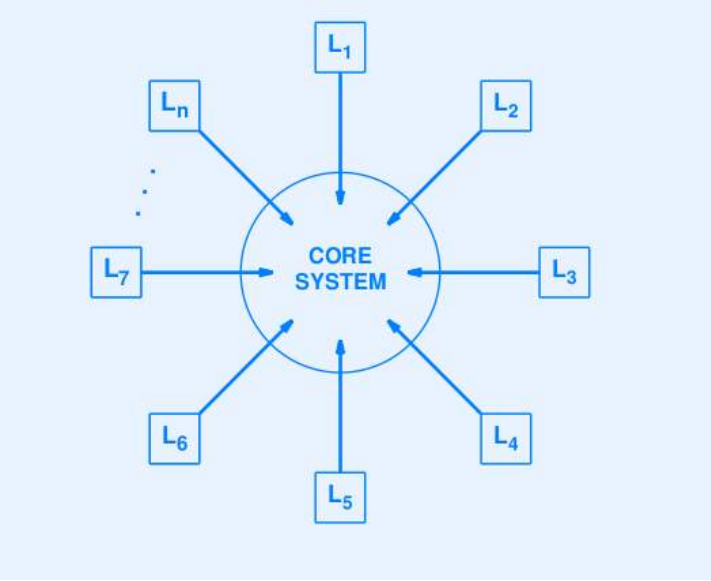
Routing dell'Internet originale



- Costituita da un backbone centrale e da una serie di router, ciascuno che connette una propria rete
- Se ogni router è oggetto di una default route può accadere nel peggiore dei casi che pacchetti destinati a reti inesistenti girino nella rete fino allo scadere del TTL associato al pacchetto

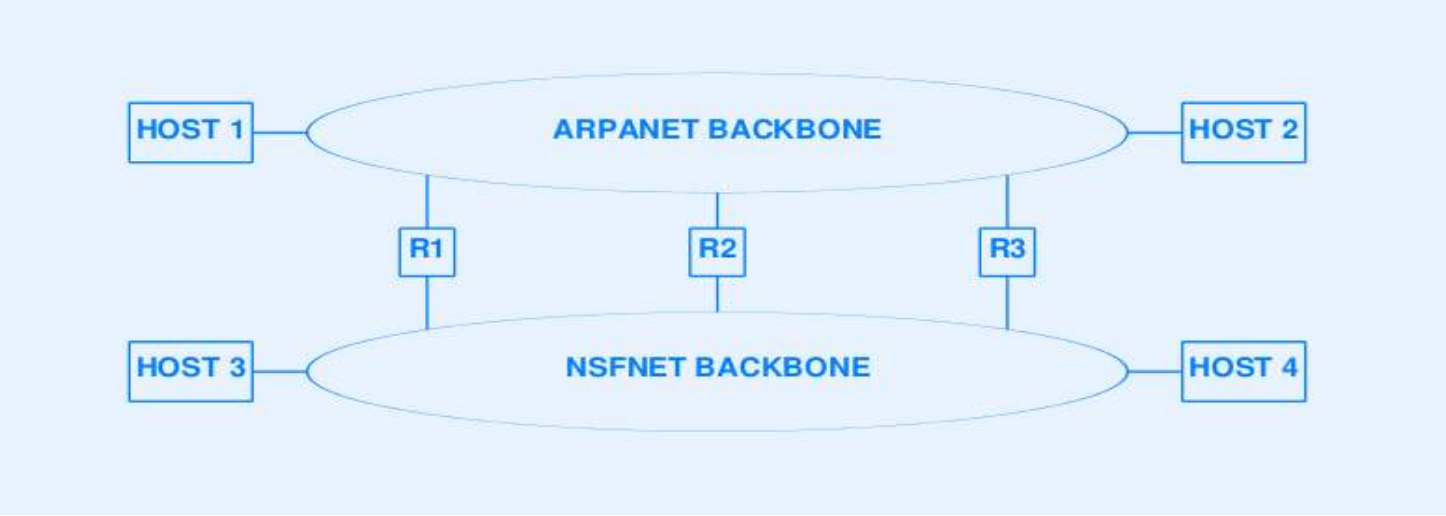
Architettura originale

- L'architettura dell'Internet iniziale prevedeva un insieme di router centrali (core routers) che conoscevano completamente le destinazioni di tutte le reti
- Gli altri router conoscevano le informazioni locali e utilizzavano i core router come router centrali.
- Controindicazioni:
  - Collo di bottiglia rappresentato dai router del Core System
  - Non sono possibili scorciatoie
  - Non scala con l'aumentare del traffico



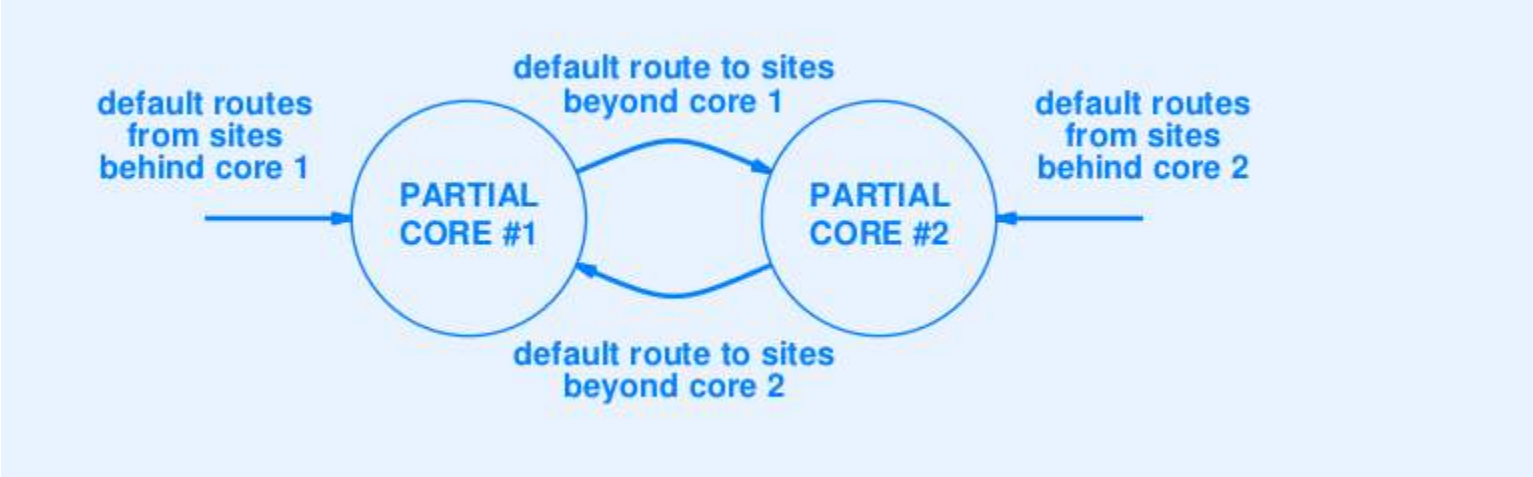
Oltre il Core System

- Un unico Core System diventa insufficiente al crescere degli ISP con proprie reti di dorsale.
- Due dorsali sono apparse quando NSF e ARPA crearono le proprie infrastrutture di rete.
- Sono diventate note come *peer backbones*.



Partial Core

- Nel nuovo schema non veniva supportato il “Partial Core”:



- Pacchetti destinati a reti inesistenti rimangono intrappolati fino a che non scade il TTL

L'architettura del Core routing

- L'architettura del Core routing assume un insieme di router centralizzati che contengono le informazioni su tutte le possibili destinazioni di Internet.
- I sistemi di Core funzionano bene per delle Internet che abbiano un singolo backbone amministrato centralmente.
- Se la topologia della rete viene estesa a più backbone il routing diventa complesso
- Se si tenta di dividere l'architettura in modo tale che tutti i router usino una default route si introducono potenziali routing loop.

Il Core routing

- La soluzione adottata è proprio quella del Core Routing, dove i router del Core System conoscono le destinazioni di tutte le reti.
- Un meccanismo consente ai router di contattare i Core router per conoscere le informazioni di routing
- Analogamente viene implementato un meccanismo che consente ai router di apprendere gli aggiornamenti in modo automatico.
- Due sono gli algoritmi utilizzati per distribuire gli aggiornamenti di routing:
  - Distance-vector
  - Link-state

Algoritmo Distance-vector

- Viene inizializzata la routing table con una riga per ogni rete direttamente connessa.
- Con cadenza periodica viene eseguito un algoritmo distance-vector per scambiare le informazioni con I router raggiungibili attraverso le reti connesse.
- Un router invia le sue istruzioni di routing ad un altro. La lista contiene 2ple inerenti l'indirizzo di rete di destinazione e la distanza.
- Il ricevente rimpiazza le istruzioni che presentano una soluzione più ottimale rispetto a quella in suo possesso.
- Le nuove istruzioni verranno propagate dal router al prossimo aggiornamento trasmesso.

Esempio di distance-vector update

Destination	Distance	Route
Net 1	0	direct
Net 2	0	direct
Net 4	8	Router L
Net 17	5	Router M
Net 24	6	Router J
Net 30	2	Router Q
Net 42	2	Router J

(a)

Destination	Distance
Net 1	2
→ Net 4	3
Net 17	6
→ Net 21	4
Net 24	5
Net 30	10
→ Net 42	3

(b)

(a) Tabella di routing esistente

(b) Aggiornamenti in arrivo

Link-state update

- Alternativo al distance-vector
- Calcolo distribuito:
  - Informazioni via broadcast
  - Permette a ciascun router di calcolare il cammino ottimale
- Evita i problemi che si hanno quando un router trasmette informazioni errate
- I router imparano la topologia della rete
- I router sono nodi di un grafo interconnessi da reti
- Periodicamente le coppie di router connessi:
  - Verificano l'esistenza del link attivo tra loro
  - Propagano lo stato dei link
- Tutti i router:
  - Ricevono i routing updates
  - Ricalcolano i percorsi ottimali sulla base delle loro informazioni

Autonomous System

- Le reti e gli Intermediate System (IS) si suddividono in
  - interni ad un *dominio di routing*
  - esterni ad un *dominio di routing*
- Per dominio di routing si intende l'insieme delle reti che sono soggette all'amministrazione ed al controllo di una stessa organizzazione
- Il dominio di routing prende il nome di **Autonomous System** o AS ed identifica la politica di routing adottata.
- L'AS condiziona il routing, consentendo ad un'organizzazione di attivare diverse politiche.

Autonomous System

- L'**RFC 1930** definisce le modalità con le quali diverse organizzazioni possono effettuare routing BGP usando degli AS privati attraverso ad unico ISP che connette queste organizzazioni ad Internet.
- Anche se ci possono essere diversi AS gestiti da un ISP, la sua politica di routing viene identificata da un Autonomous System Number (ASN) ufficialmente registrato.
- Un ASN viene assegnato a ciascun AS per poter effettuare routing BGP.
- Gli ASN identificano univocamente le reti ai fini del routing.

ASN

- Fino al 2007 gli ASN erano indicati da un numero intero a 16 bit (0-65536), denominati *asplain*
- **RFC 4893** definisce una nuova sintassi per la numerazione degli AS, che prende il nome di *asdot*, nella forma *x.y*, con *x* e *y* numeri interi di 16 bit.
- I numeri 0.y coincidono con gli asplain.
- L'ASN 23456 è stato assegnato da IANA come variabile metasintattica per valori di ASN a 32 bit nel caso in cui router BGP in grado di gestire la nuova sintassi comunicassero con router BGP di vecchia generazione non in grado di comprendere ASN a 32 bit.
- Gli ASN 0 e 65535, e l'ultimo ASN della numerazione a 32 bit: 4.294.967.295 sono riservati e non possono essere usati dagli operatori
- Gli ASN 64.512–65.534 e 4.200.000.000-4.294.967.294 sono riservati per uso privato dall'RFC 6996.

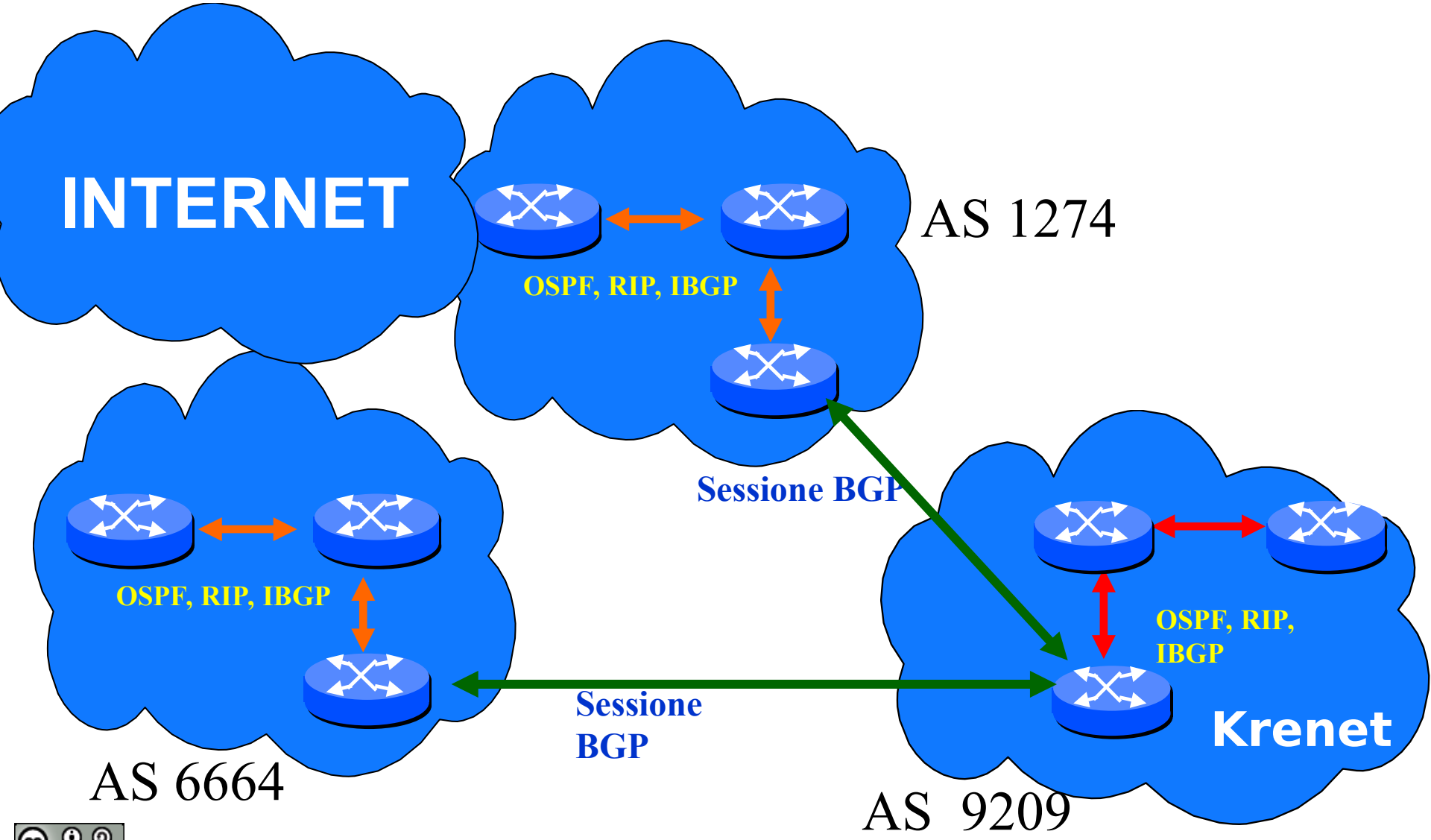
ASN

- Gli ASN vengono assegnati da ICANN (in passato da IANA) ai Regional Internet Registries (RIRs).
- Gli AS si suddividono in:
  - **multihomed autonomous system:** è un AS che mantiene connessioni con più di un AS. Ciò consente all'As di rimanere connesso alla rete Internet anche in presenza di un malfunzionamento di una delle connessioni. Questo AS non consente di effettuare il pass-through con un altro AS.
  - **stub autonomous system:** si riferisce ad un AS connesso solamente con altro AS. Questo sembra un controsenso e uno spreco di ASN. Questo AS consente forme di peering privato con altri AS che non viene riflesso nelle politiche generali di routing.
  - **transit autonomous system:** è un AS che fornisce attraverso di sé connessioni con altre reti. La rete A può usare la rete B, appartenente ad un transit AS, per connettersi alla rete C. Se un AS è un ISP per un altro AS, allora questi è un transit AS.

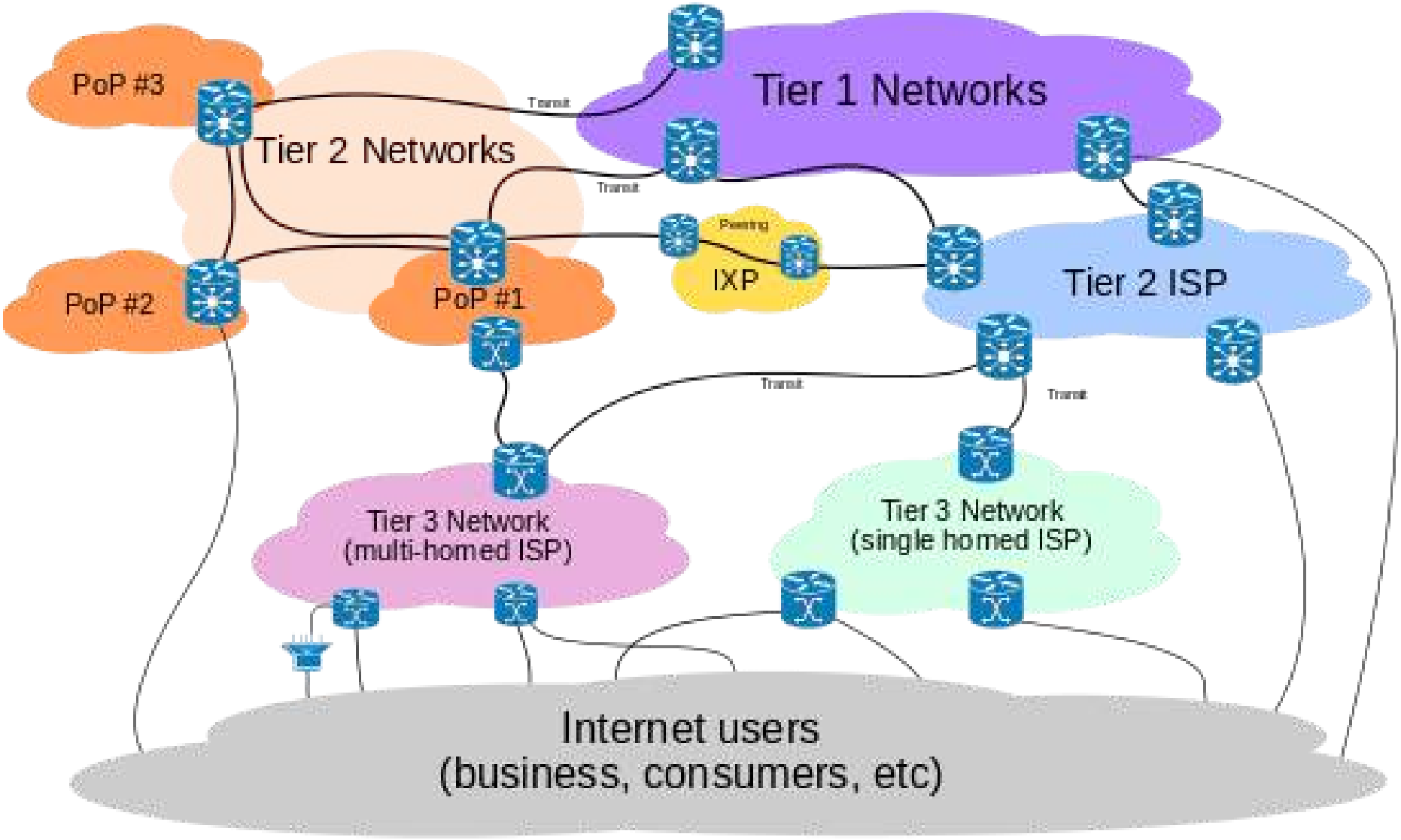
ASN

- Condizione necessaria per ottenere il rilascio di un ASN è quella di possedere due distinte connessioni ad Internet, attraverso diversi provider (ISP).
- In ISP ha più ASN assegnati per poter gestire situazioni differenti.
- I router che instradano messaggi all'interno dello stesso AS sono detti Interior Router, mentre quelli che instradano messaggi anche tra AS diversi sono detti Exterior Router.
  - Gli Interior Router eseguono un Interior Gateway Protocol (IGP) per determinare il percorso ottimale
  - Gli Exterior Router eseguono un Exterior Gateway Protocol (EGP)

Esempio di connessione miltihomed, considerando degli asplain



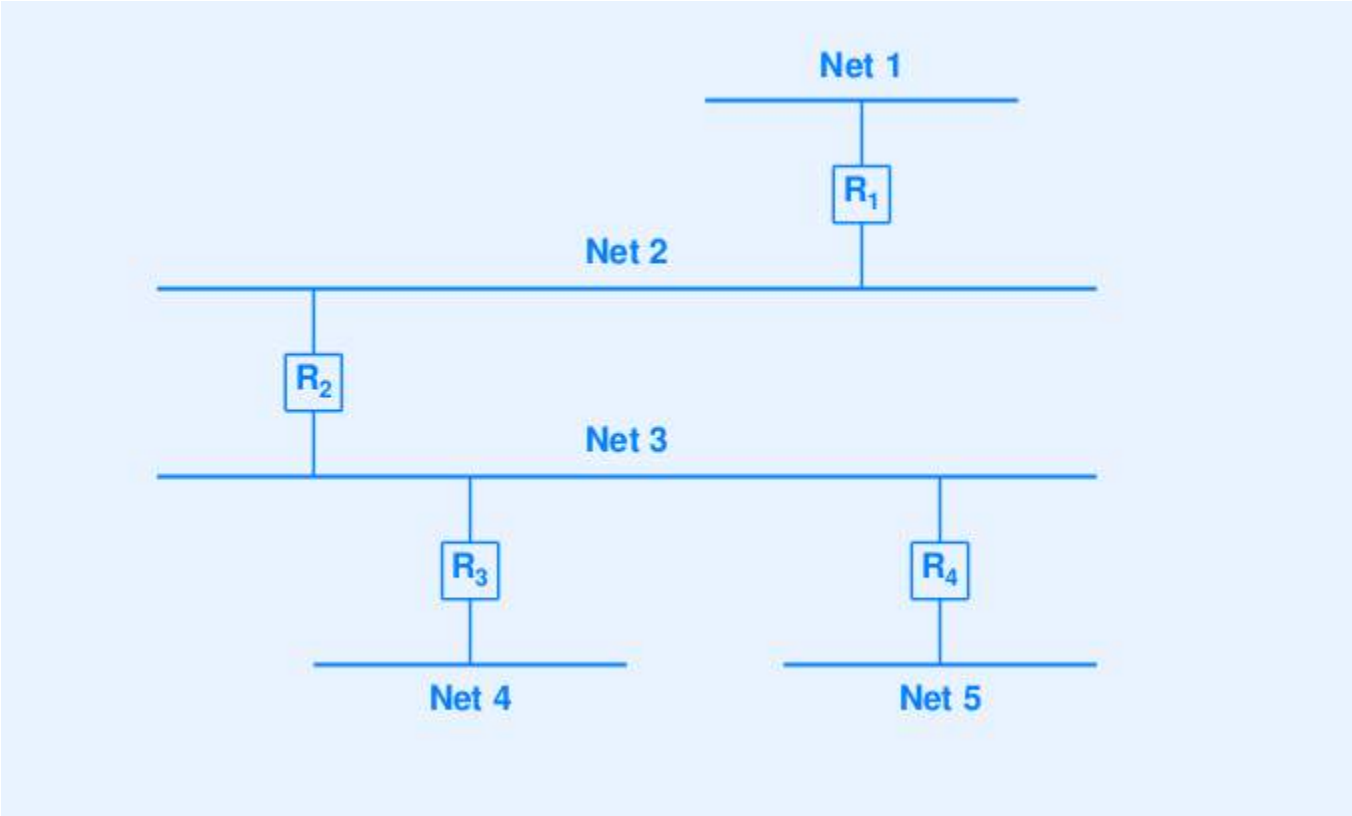
Architecture of the Internet infrastructure



Routing statico e routing dinamico

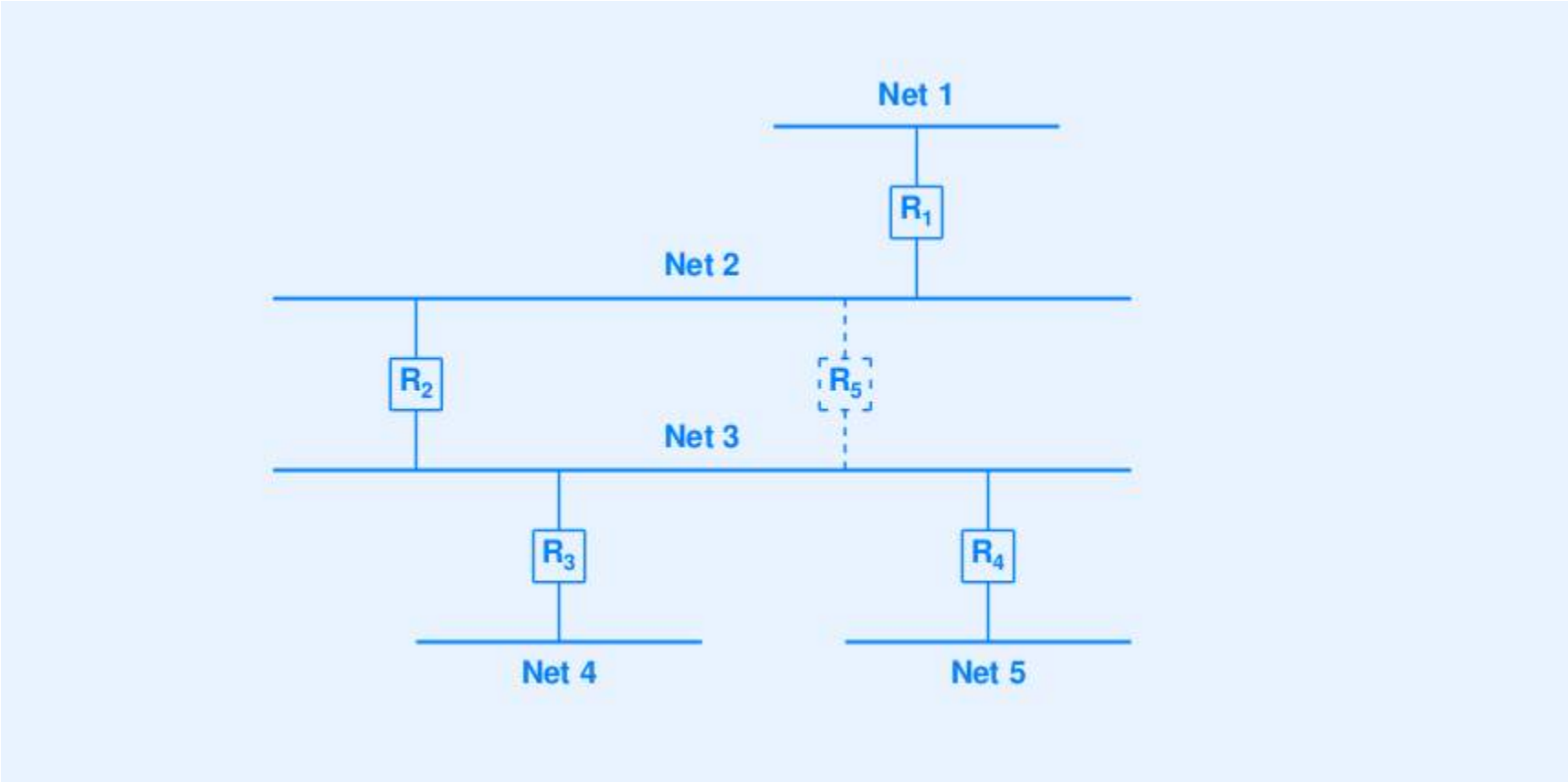
- Route statiche:
  - Sono inizializzate allo start-up
  - Non cambiano mai
  - Sono tipiche degli host
  - Usate qualche volta nei router
- Route dinamiche:
  - Sono inizializzate allo start-up
  - Aggiornate mediante dei protocolli di propagazione dei router
  - Sono tipiche dei router
  - Usate qualche volta negli host

Esempio di routing statico ottimale



Ogni rete ha soltanto una possibile route

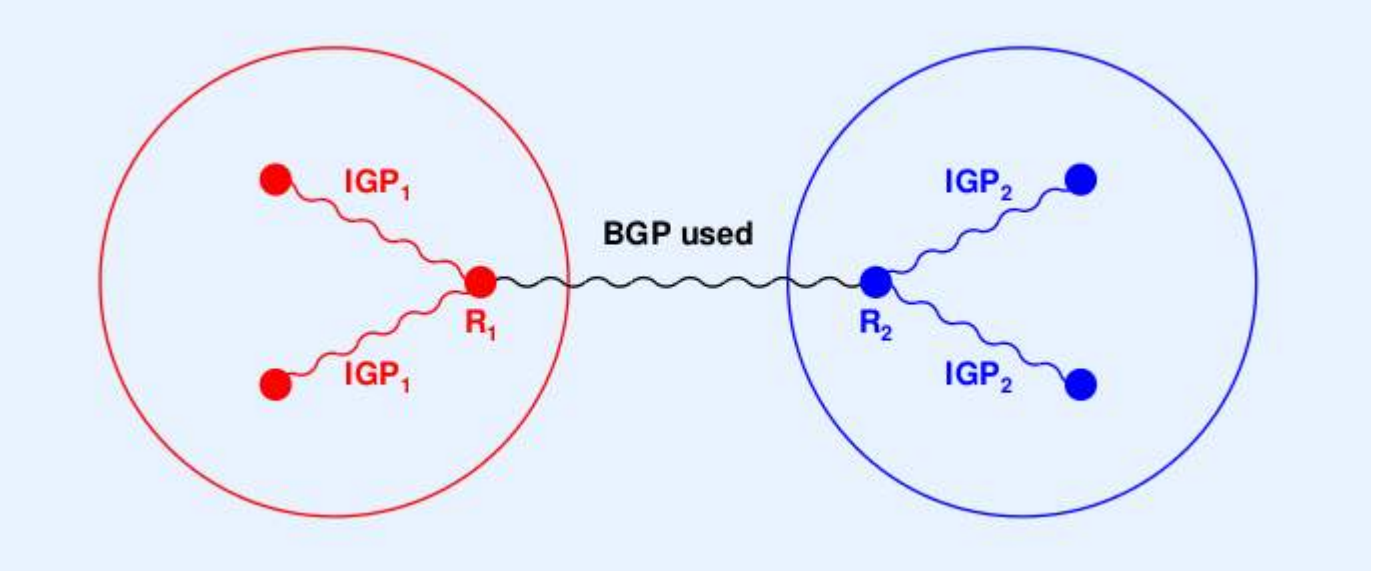
Esempio nel quale è necessario il routing dinamico



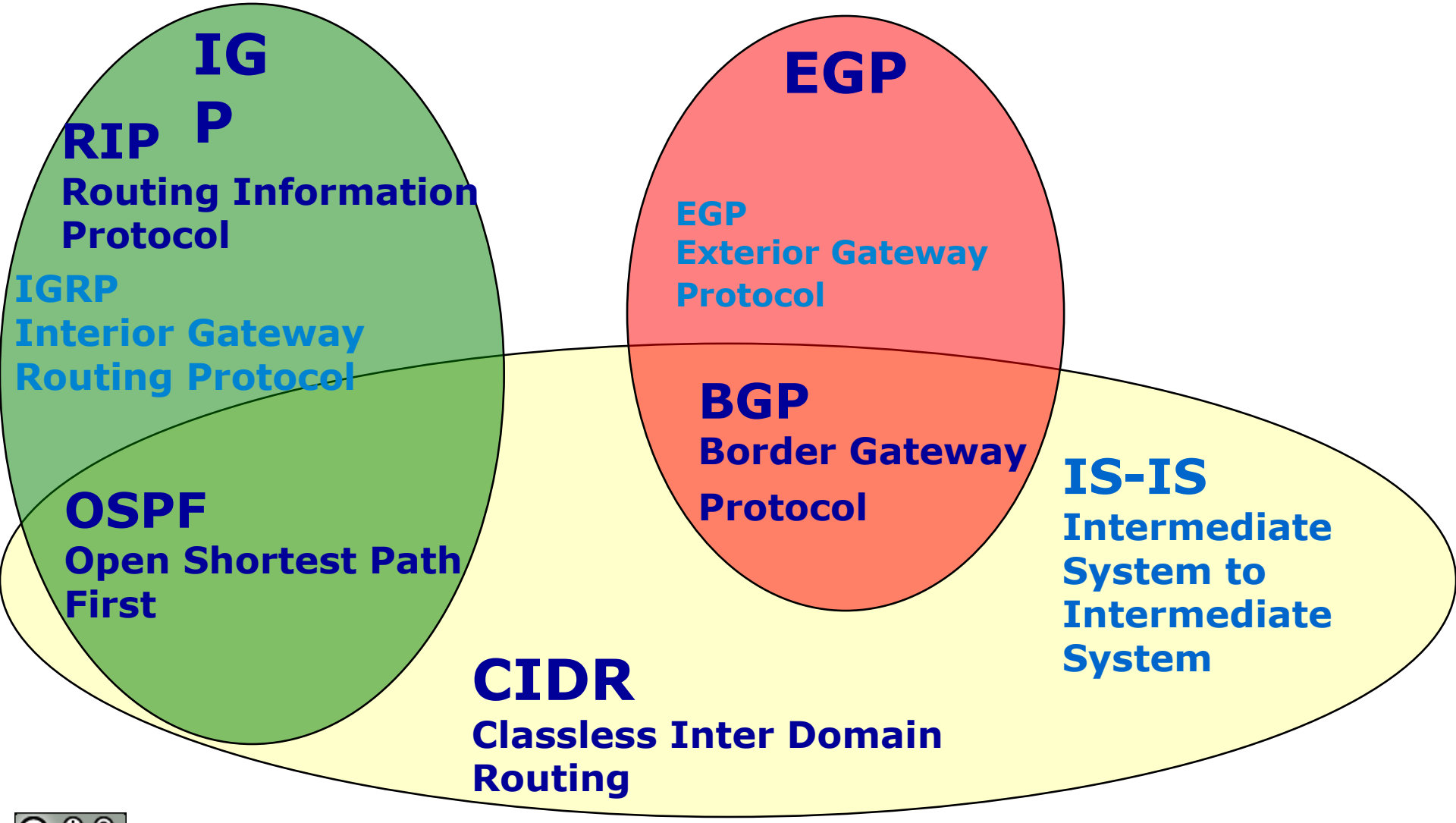
Ci sono più percorsi possibili per raggiungere una rete

Scambio di informazioni di routing all'interno ad un AS

- Meccanismo denominato Interior Gateway Protocols, IGPs
- Le scelte di tipo IGP sono effettuate dall'AS
- NB: se un AS si connette al resto del mondo, un router nell'AS deve usare un protocollo EGP per annunciare la raggiungibilità della rete ad altri AS



Protocolli di routing



Open Shortest Path First (OSPF)

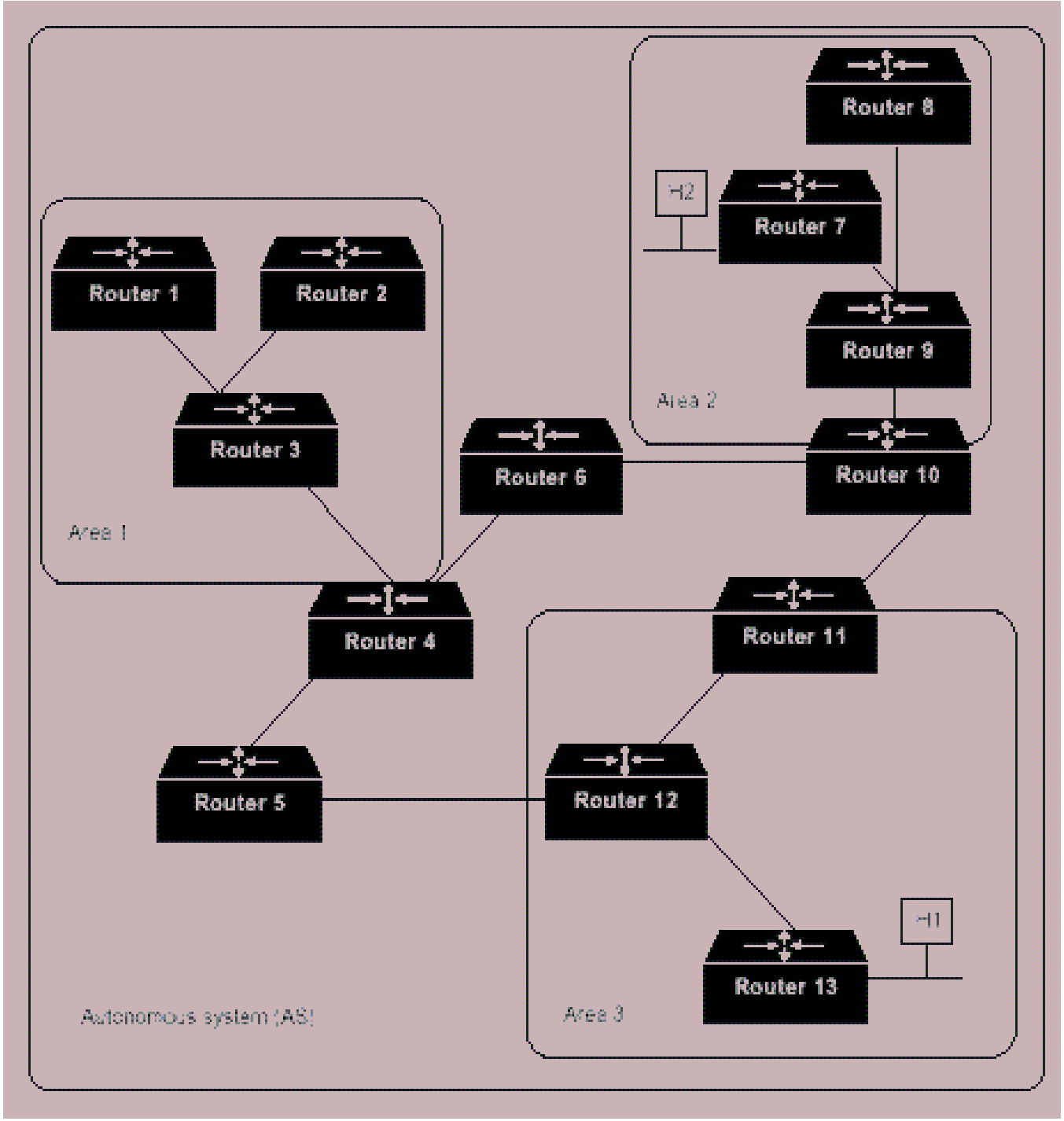
- Sviluppato nel 1988 dall'IGP working group di IETF, standard nel 1990 (RFC1247) per routing all'interno di un AS
- Una risposta di tipo Open Source ai protocolli proprietari, di straordinaria efficienza, molto complesso da configurare e gestire.
- OSPF:
  - **è aperto**
  - **è basato sull'algoritmo Shortest Path First (***Dijkstra algorithm***)**
  - **supporta subnet variabili**
  - **implementa routing dinamico**
  - **supporta routing in base al tipo di servizio**
  - **esegue il bilanciamento del carico**
  - **supporta l'autenticazione dei messaggi**
  - **supporta sistemi gerarchici (aree)**

OSPF

- E’ un link-state routing protocol così chiamato perché invia *link-state advertisements* (LSA) a **tutti i router di una stessa area gerarchica**
- Nell’ LSA invia informazioni relative alle interfaccie attive, alle metriche usate, ed altre variabili
- Un router OSPF accumula LSA e calcola il percorso ottimale mediante l’algoritmo SPF
- E’ computazionalmente relativamente pesante

OSPF

- I router di una stessa area condividono lo stesso *topological database*
- La suddivisione in aree riduce il traffico di routing nell'AS
- L'introduzione delle aree genera due tipi di traffico di routing
  - *Inter-area routing*
  - *Intra-area routing*
- L'OSPF backbone è responsabile di distribuire informazioni di routing tra aree


Router 8
H2
Router 7
Router 1
Router 2
Router 9
Area 2
Router 3
Router 6
Router 10
Area 1
Router 4
Router 11
Router 5
Router 12
H1
Router 13
Autonomous system (AS)
Area 3

OSPF

- Le aree possono essere definite in modo tale che il backbone non sia continuo: in tal caso la continuità può essere realizzata mediante *virtual-links*
- Questo permette ai gestori della rete di definire una topologia *logica* differente da quella fisica.
- I virtual-links vengono definiti tra i backbone router che condividono link con aree non-backbone e funzionano come se fossero link diretti
- OSPF può apprendere informazioni da altri exterior gateway protocol, interior gateway protocol, o mediante istruzioni di configurazione

OSPF

- OSPF può operare all'interno di una gerarchia
- la maggiore entità gerarchica è l'AS
- OSPF è un intra-AS (IGP) routing protocol, anche se può inviare e ricevere route verso o da altri AS
- Un AS può essere diviso in diverse aree, che è bene riguardino host in gruppi di reti contigue per semplificare la routing table.
- Router con diverse interfacce possono appartenere a più aree e prendono il nome di **Area Border Router** (**ABR**). Essi mantengono diversi *topological database* per ogni area

OSPF

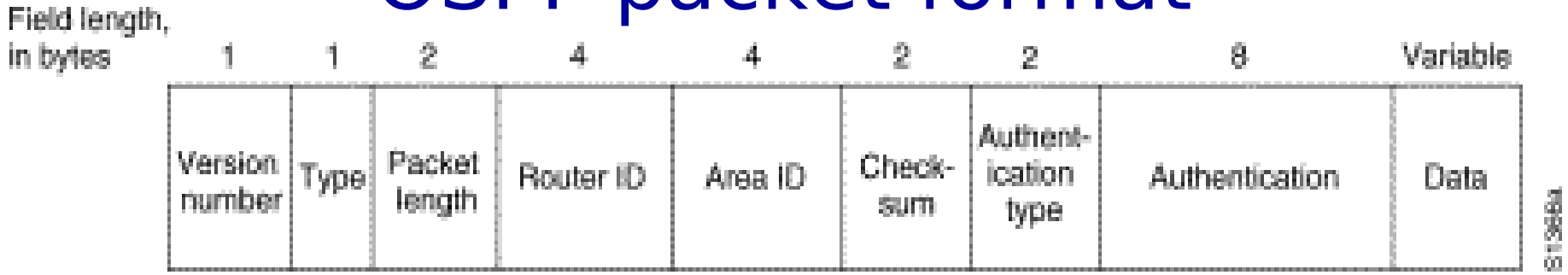
- OSPF distingue 4 tipi di router:
  - **Internal router**: interni ad un'area
  - **Area Border router**: che connettono 2 o più aree
  - **Backbone router**: che appartengono alla dorsale (area 0)
  - **Border AS router**: router di confine tra AS
- Quando un router viene avviato mediante messaggi di tipo *HELLO* inviati su tutte le interfaccie, si costruisce la mappa topologica ed in particolare definisce:
  - i **router adiacenti**
  - il **designed router** (**DR**)
  - il **backup designed router** (**BDR**)

OSPF packets

- Router che non sono adiacenti non scambiano tra loro informazioni
- I pacchetti OSPF sono:

Hello	**usato per scoprire i neighbors**
Link state update	**fornisce i propri criteri per la selezione del costo del link**
Link state ack	**conferma un LS update**
Database description	**comunica gli aggiornamenti che conosce**
Link state request	**richiesta di informazioni di stato ai neighbor routers**

OSPF packet format



Header fisso di 24 Bytes

Version number: identifica la versione del software OSPF usato

Type:identifica il tipo di pacchetto OSPF tra i seguenti possibili:

Hello:stabilisce e mantiene le relazioni con i *neighbor routers*

Database Description: descrive i contenuto del topological database*, che varia con lo stabilirsi di* adjacencies con altri routers.

Link-State-Request: Richiede porzioni del *topological database* dai *neighbor routers*

Link-State-Update: risponde a pacchetti Link-State-Request

Link-State-Acknowledgment: risposta di conferma a pacchetti Link-State-Update

Packet length:specifica la lunghezza del pacchetto, inclso l'header, in bytes

Router ID: identifica la sorgente del pacchetto

AreaID: identifica l'area a cui appartiene il pacchetto

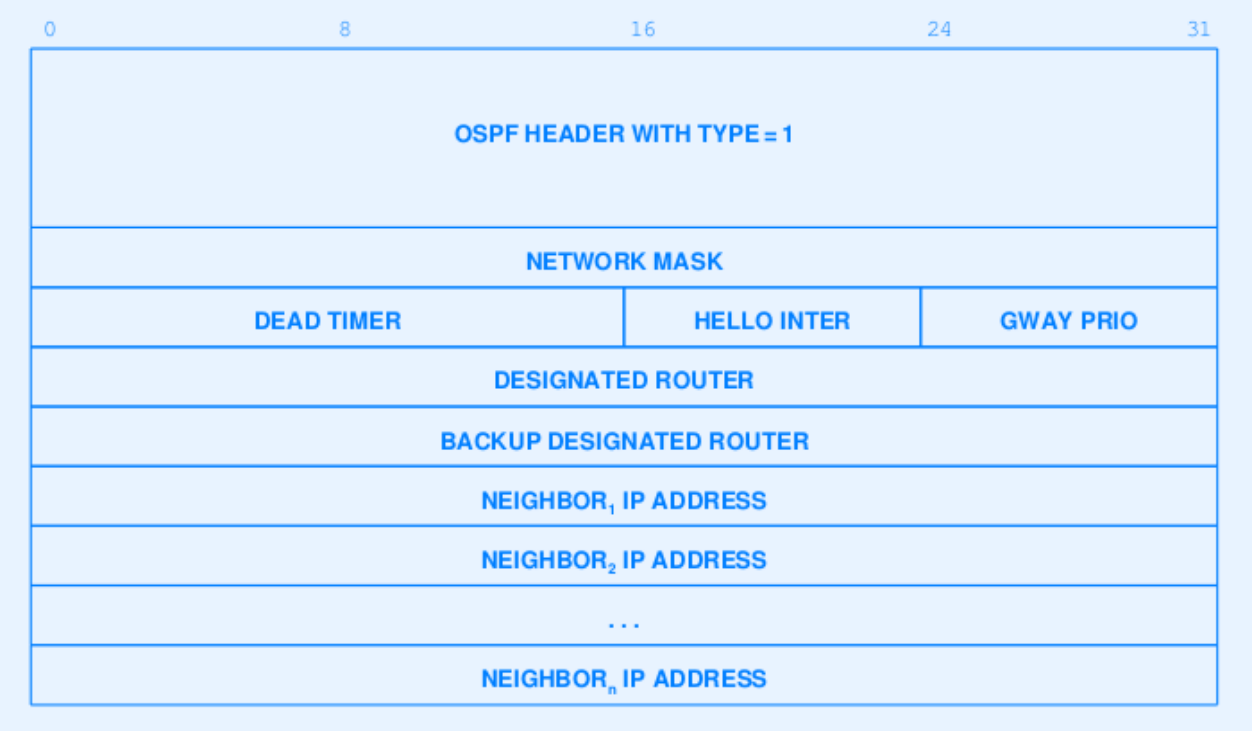
Checksum: verifica l'integrità dell'intero pacchetto dopo la trasmissione

Authentication type: contiene il tipo di autenticazione. Lo scambio di dati in OSPF tra i vari protocolli è sempre autenticato in base all'area

Authentication: contiene le informazioni per l'autenticazione

Data: contiene informazioni relative a protocolli di più alto livello incapsulati

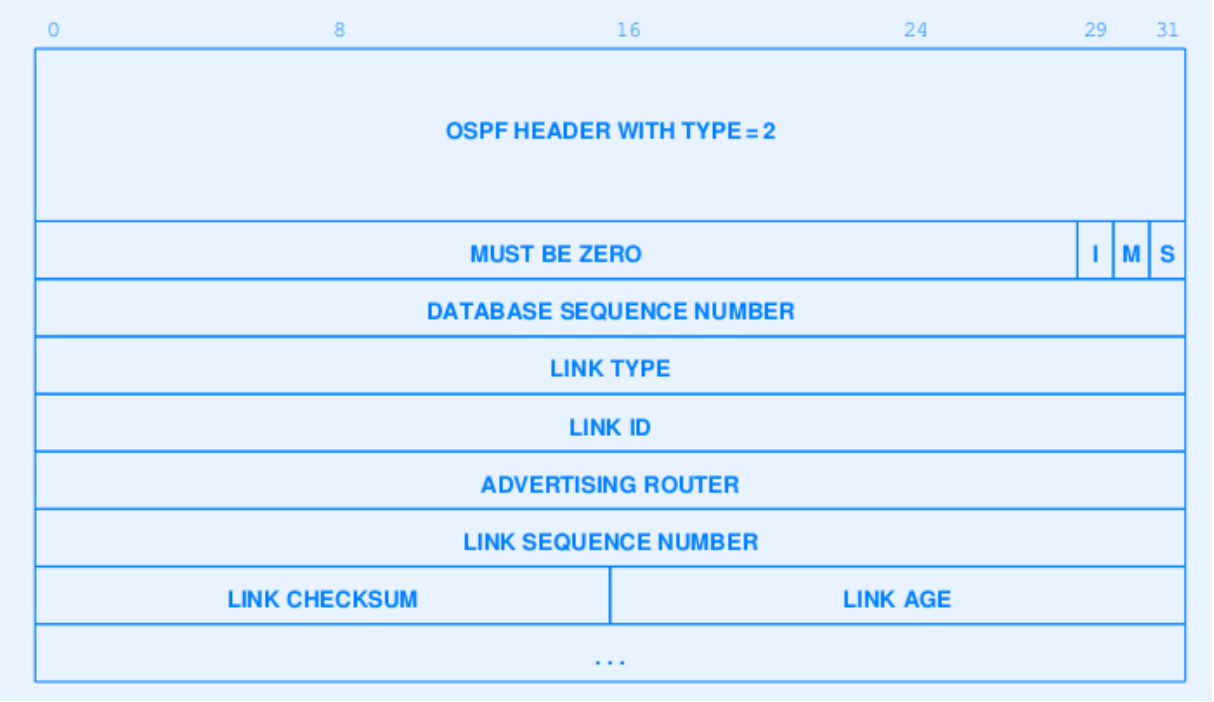
OSPF Hello packet



- Due router OSPF vicini si scambiano periodicamente questo pacchetto per verificare la reciproca raggiungibilità
- ROUTER DEAD INTERVAL indica il tempo trascorso il quale se il router vicino non risponde, è considerato inattivo
- HELLO INTERVAL è il tempo che intercorre tra messaggi HELLO
- GWAY PRIO indica la priorità del router e serve per identificare il Backup Designed Router (BDR)

Formato dei messaggi di descrizione del database OSPF

- Per inizializzare il loro topological database i router si scambiano dei messaggi di descrizione del database OSPF
- Nello scambio uno funge da router principale (master), l'altro secondario (slave) e conferma la ricezione di ogni messaggio con una risposta.



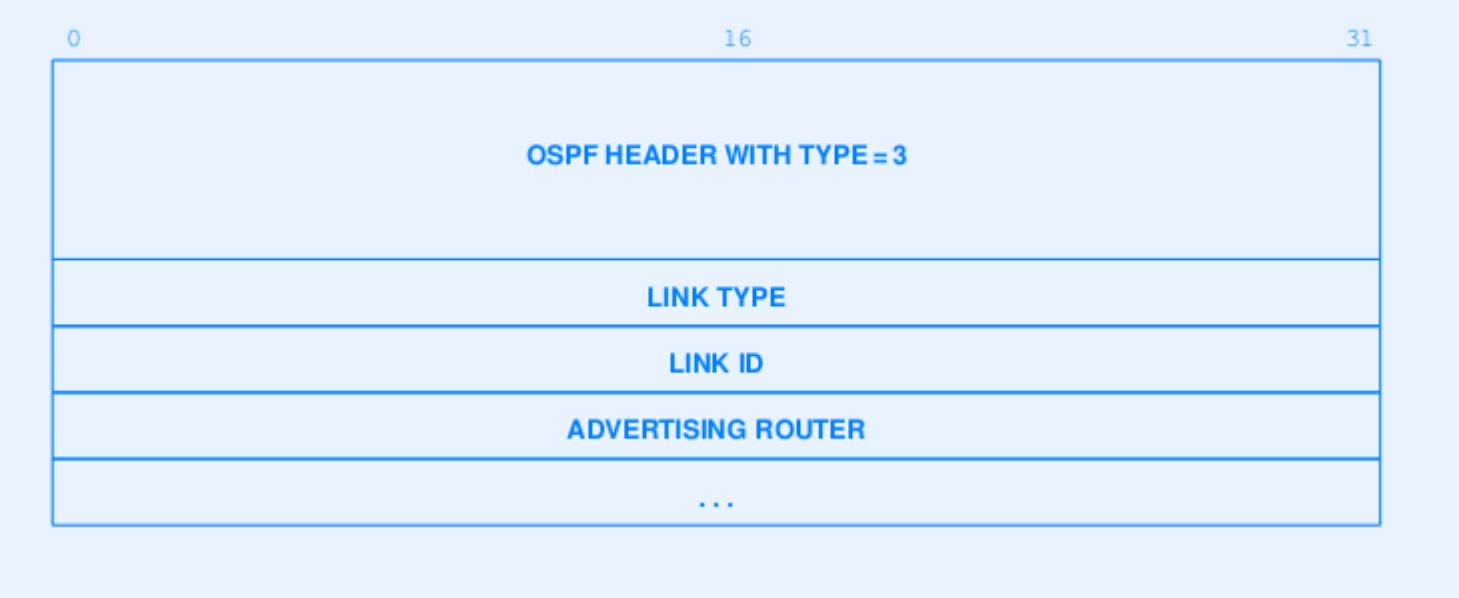
Formato dei messaggi di descrizione del database OSPF

- Poiché il messaggio può essere molto esteso, vengono utilizzati i bit *I* (impostato a 1 nel messaggio iniziale) e *M* (impostato a 1 nei messaggi che seguono)
- Il bit *S* indica se il messaggio è stato inviato ad un master (1) o a uno slave (0).
- DATABASE SEQUENCE NUMBER numera in sequenza i messaggi, in modo che il ricevente possa identificare eventuali messaggi persi. Il primo contiene un numero R casuale, i successivi interi sequenziali a partire da R.
- I campi da Link AGE a Link LENGTH descrivono un collegamento di rete. Link TYPE indica il tipo di collegamento:

1. collegamento del router
2. collegamento di rete
3. Collegamento di riepilogo (rete IP)
4. Collegamento di riepilogo (collegamento al router di confine)
5. Collegamento esterno (collegamento ad un altro sito)

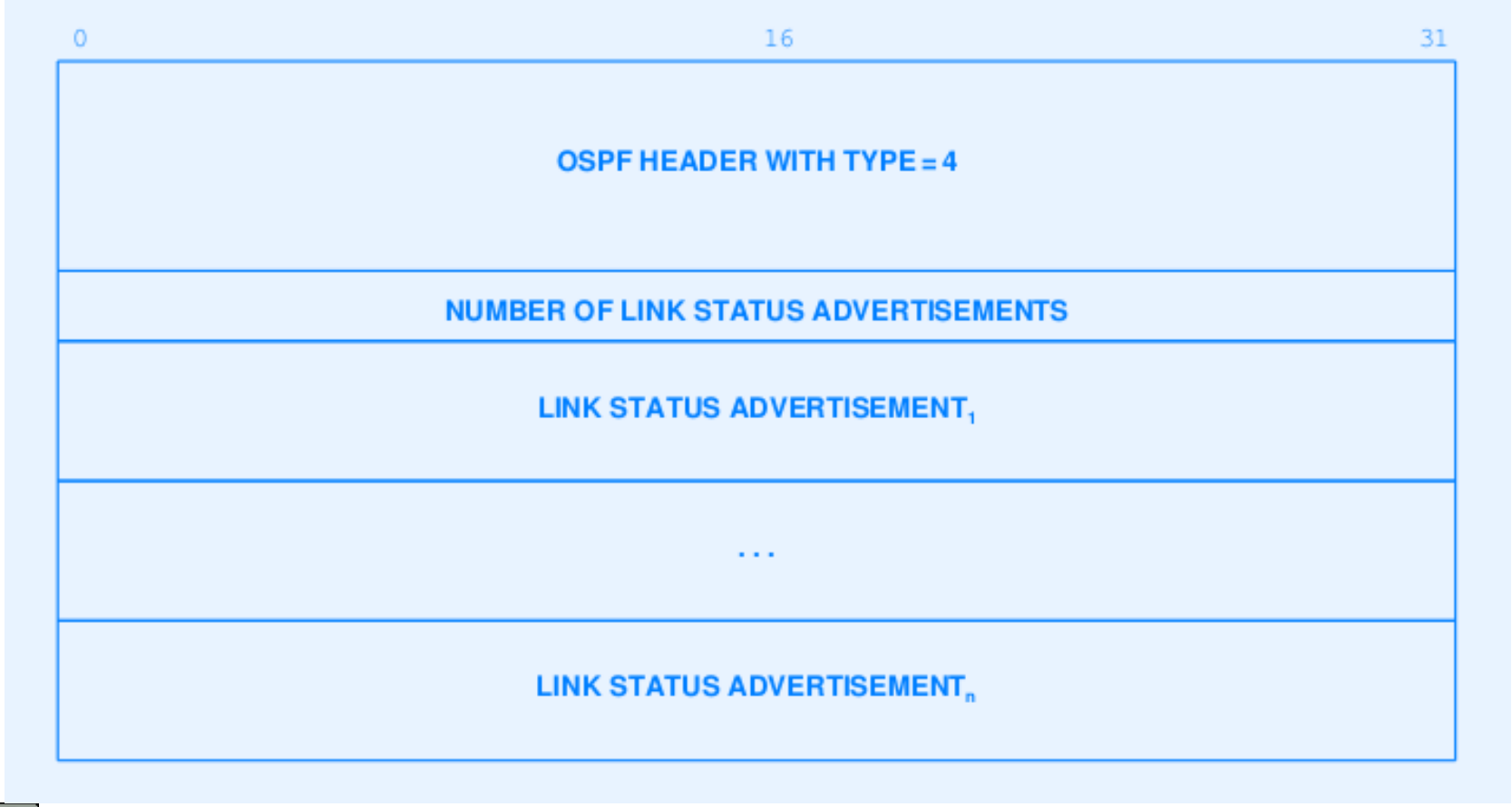
Formato dei messaggi di richiesta dello stato dei collegamenti OSPF

- Dopo aver scambiato messaggi di descrizione del database con un vicino, un router può scoprire parti obsolete del suo database
- Affinché il vicino gli risponda con gli aggiornamenti, il router invia un messaggio di richiesta dello stato dei collegamenti
- Il vicino risponde con le informazioni aggiornate che ha.



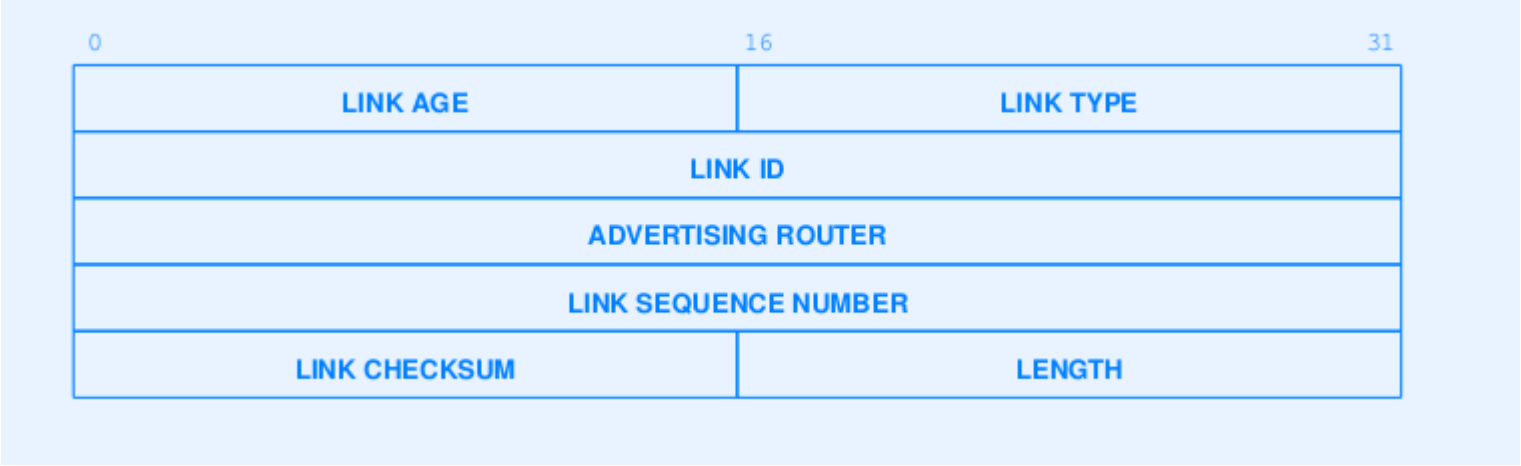
Formato dei messaggi di aggiornamento dello stato dei collegamenti OSPF

- I router trasmettono in broadcast lo stato dei collegamenti con un messaggio di aggiornamento dello stato dei collegamenti.

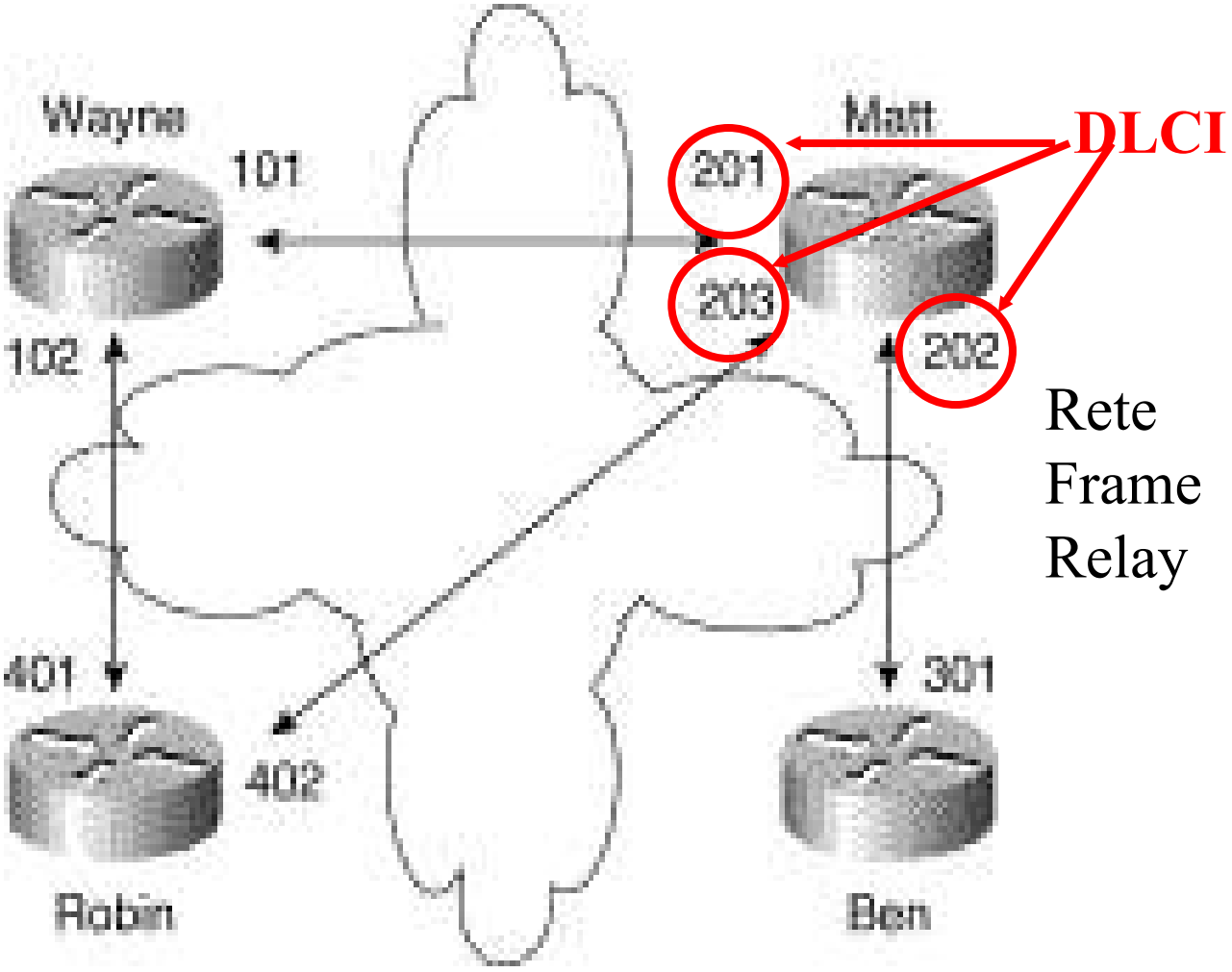


Formato dell'intestazione usata nei messagg sullo stato dei collegamenti OSPF

- L'intestazione dello stato dei collegamenti usa uno dei quattro possibili formati per descrivere i collegamenti del router ad una certa area, a una rete specifica, alle reti fisiche di una rete IP suddivisa in sottoreti ed infine a reti di altri siti.



OSPF: esempio



OSPF: esempio

```
hostname Matt
!
interface serial 1
ip address 10.0.0.2 255.0.0.0
ip ospf network point-to-multipoint
encapsulation frame-relay
frame-relay map ip 10.0.0.1 201 broadcast
frame-relay map ip 10.0.0.3 202 broadcast
frame-relay map ip 10.0.0.4 203 broadcast
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

OSPF: esempio

```
hostname Wayne
!
interface serial 0
ip address 10.0.0.1 255.0.0.0
ip ospf network point-to-multipoint
encapsulation frame-relay
frame-relay map ip 10.0.0.2 101 broadcast
frame-relay map ip 10.0.0.4 102 broadcast
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

OSPF: esempio

```
hostname Robin
!
interface serial 3
ip address 10.0.0.4 255.0.0.0
ip ospf network point-to-multipoint
encapsulation frame-relay
clockrate 1000000
frame-relay map ip 10.0.0.1 401 broadcast
frame-relay map ip 10.0.0.2 402 broadcast
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

OSPF: esempio

```
hostname Ben
!
interface serial 2
ip address 10.0.0.3 255.0.0.0
ip ospf network point-to-multipoint
encapsulation frame-relay
clockrate 2000000
frame-relay map ip 10.0.0.2 301 broadcast
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

RIP

- RIP è un popolare algoritmo di routing, definito negli RFC 1058 e 1023.
- E' implementato dal programma *routed*
- Si basa sull'algoritmo di *Bellman-Ford*, detto anche *vettore-distanza*
- RIP ha il limite di 15 hops: reti più distanti sono considerate irraggiungibili
- RIP v1 non supporta subnet variabili
- Un router che implementa RIP invia **tutta la routing table** o una porzione di essa **ai router vicini** (neighbor) (distanti 1 hop) ad intervalli di tempo regolari

Due forme di RIP

- Attiva
  - Forma usata dai router
  - Invia in broadcast periodicamente aggiornamenti di routing
  - Usa I messaggi in arrivo per aggiornare la routing table
- Passiva
  - Forma usata dagli host
  - Usa I messaggi in arrivo per aggiornare la routing table
  - Non invia aggiornamenti
- Ogni router invia update ogni 30 secondi
- Gli aggiornamenti contengono coppie di valori del tipo: (destination address, distance)
- La distanza di 16 è infinita (non viene fatto routing)

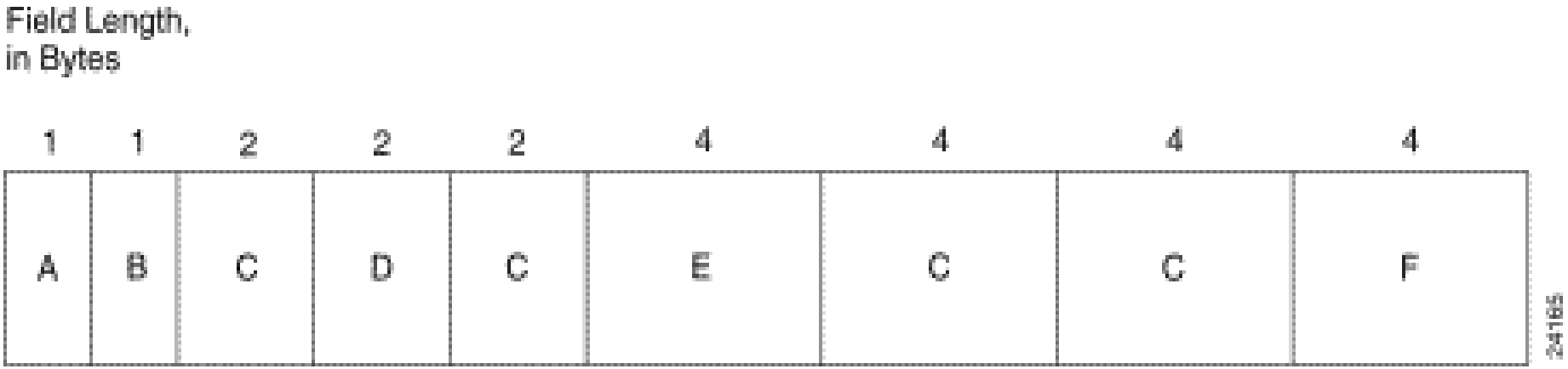
RIP

- RIP converge meno rapidamente di OSPF: ciò lo rende più fragile per quanto attiene la possibilità di generare *routing loops*
- RIP ha bisogno di meno risorse di OSPF, in quanto l'algoritmo è più leggero
- RIP è disponibile per default sui sistemi Unix/Linux (daemon **`routed`**)
- E' più semplice da implementare e gestire rispetto a OSPF
- RIP distingue i router tra *attivi* (coloro che trasmettono le istruzioni di routing) e *passivi* (ricevono i messaggi e aggiornano la loro routing table): solo un router può essere attivo (un host è passivo)

RIP

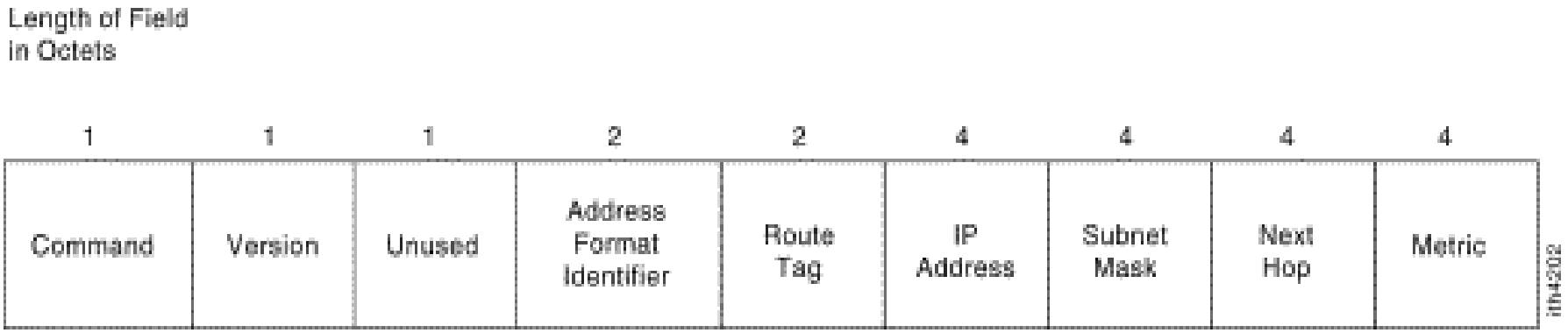
- **Routing updates**: RIP invia questi messaggi a intervalli regolari o quando cambia la topologia della rete ai router confinanti.
- **RIP timers**: RIP mantiene i timer *routing-update timer*(30 sec, in genere), *route timeout*, *route-flush timer*
- RIP mantiene solo le informazioni relative a *best routes*
- RIP usa il protocollo UDP e la porta 520

RIP packet format



A = Command
B = Version Number
C = Zero
D = Address Family Identifier
E = Address
F = Metric

RIP 2 packet format



Command: indica se il pacchetto è un comando oppure una risposta
Version number: identifica la versione del software RIP usato
Unused: valore posto a zero
Address-Family-Identifier: identifica la famiglia di protocolli utilizzata. RIP è concepito per trasportare informazioni relative a diversi protocolli. La famiglia di indirizzi per l'IP è 2.
Route tag: fornisce un metodo per distinguere fra routing interno ed esterno (appreso da alti protocolli)
IP Address: specifica l'IP address relativa all'informazione di routing
Subnet-Mask: specifica la subnet mask relativa all'informazione di routing
Next-Hop: Specifica il next-hop al quale deve essere indirizzata l'informazione di routing
metric: indica quanti router intermedi devono essere attraversati fino alla rete di destinazione. Questo valore va da 1 a 15. Un valore uguale o maggiore di 16 indica *network unreachable.*

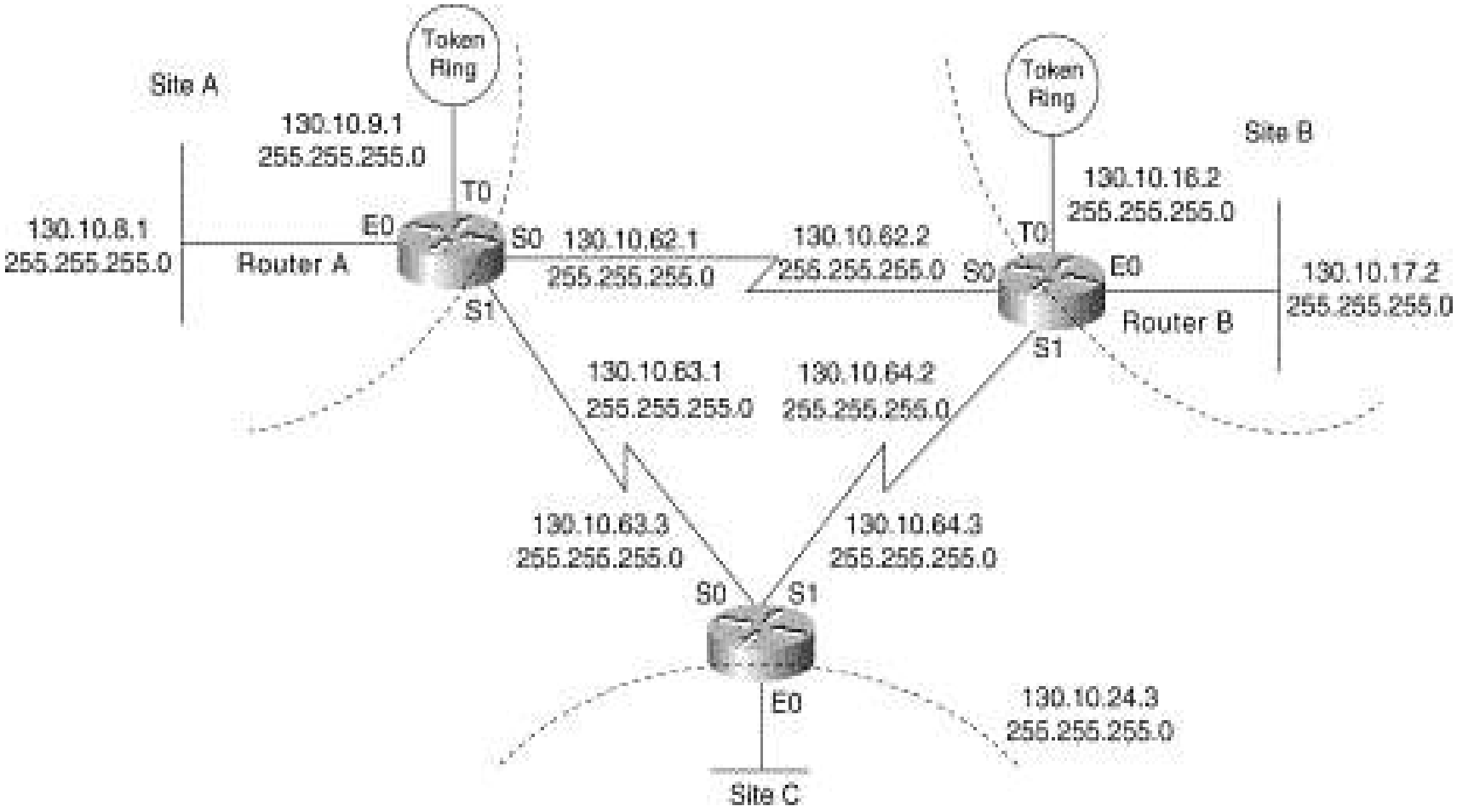
RIP

- Per evitare oscillazioni tra percorsi di costo uguale, RIP specifica che gli istradamenti esistenti dovrebbero essere mantenuti sino a che uno nuovo non abbia un costo rigorosamente più basso (applica l'isteresi, cioè un meccanismo che reagisce in ritardo alle sollecitazioni e dove lo stato attuale dipende anche dallo stato precedente)
- Quando un router si guasta gli altri router annulleranno le informazioni di routing relative allo scadere dei timer associati all'istruzione di route
- RIP deve gestire tre errori causati dall'algoritmo sottostante. In primo luogo poiché non rileva i routing loop. Inoltre per evitare instabilità deve usare un numero basso (16 in genere) come distanza massima presa in esame in termini di routers. Inoltre l'algoritmo genera problemi di convergenza lenta.

RIP

- Per evitare I problemi di convergenza lenta I router adottano la tecnica dello *split horizon update*: il router non propaga informazioni su una route al router che ha generato tale aggiornamento.
- Un'altra tecnica è l'*hold down*, che costringe un router a ignorare aggiornamenti inerenti una rete per un certo tempo (60 sec in genere), una volta che ha ricevuto un messaggio di rete irrangiugibile.
- Altra tecnica è il *poison reverse*: quando un collegamento scompare, il router che effettuava l'annuncio continua ad annunciarlo ancora per un certo tempo assegnandogli una distanza infinita.
- Questo va accompagnato al *triggered update*, che obbliga i router ad annunciare la scomparsa di route immediatamente senza attendere che i timer si azzerino.

RIP: esempio


Token Ring
Site A
130.10.9.1
255.255.255.0
T0
130.10.8.1
255.255.255.0
E0
Router A
S0
130.10.62.1
255.255.255.0
S1
130.10.62.2
255.255.255.0
Token Ring
Site B
130.10.16.2
255.255.255.0
T0
S0
E0
Router B
S1
130.10.17.2
255.255.255.0
130.10.63.1
255.255.255.0
130.10.64.2
255.255.255.0
130.10.63.3
255.255.255.0
130.10.64.3
255.255.255.0
S0
S1
E0
130.10.24.3
255.255.255.0
Site C

RIP: schema di indirizzamento

Network Number	Subnets	Subnet Masks
130.10.0.0	Site A: 8 through 15	255.255.255.0
130.10.0.0	Site B: 16 through 23	255.255.255.0
130.10.0.0	Site C: 24 through 31	255.255.255.0
130.10.0.0	Serial Backbone: 62->64	255.255.255.0

RIP: esempio di configurazione

Router A:

```
interface serial 0
ip address 130.10.62.1 255.255.255.0
interface serial 1
ip address 130.10.63.1 255.255.255.0
interface ethernet 0
ip address 130.10.8.1 255.255.255.0
interface tokenring 0
ip address 130.10.9.1 255.255.255.0
router rip
network 130.0.0.0
```

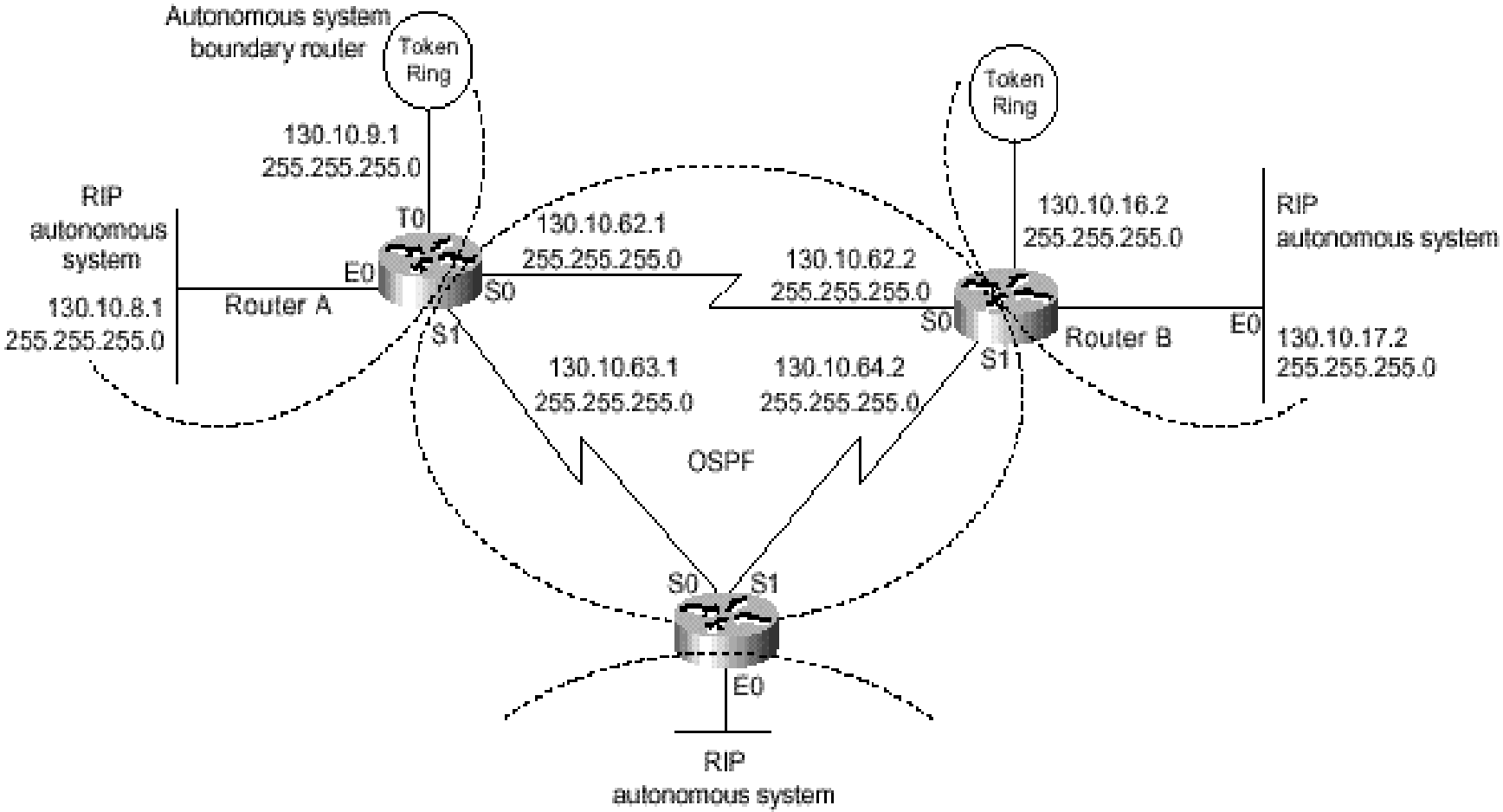
Router B:

```
interface serial 0
ip address 130.10.62.2 255.255.255.0
interface serial 1
ip address 130.10.63.2 255.255.255.0
interface ethernet 0
ip address 130.10.17.2 255.255.255.0
interface tokenring 0
ip address 130.10.16.2 255.255.255.0
router rip
network 130.0.0.0
```

Router C:

```
interface serial 0
ip address 130.10.63.3 255.255.255.0
interface serial 1
ip address 130.10.64.3 255.255.255.0
interface ethernet 0
ip address 130.10.24.3 255.255.255.0
router rip
network 130.0.0.0
```

Inserimento di una dorsale OSPF in RIP



Esempio di configurazione

- **Router A:**

```
router rip
passive-interface serial 0
passive-interface serial 1
```

- **ridistribuzione:**

```
router ospf 109
redistribute rip subnets

router rip
redistribute ospf 109 match internal external 1 external 2
default-metric 10
```

- **alternativa:**

```
router ospf 109
redistribute rip subnet
distribute-list 11 out rip
access-list 11 permit 130.10.8.0 0.0.7.255
access-list 11 deny 0.0.0.0 255.255.255.255
```

Alle informazioni

OSPF propagate via RIP viene assegnata la metric 10

Unicast updates

- E’ possibile in RIP 2 ridurre le informazioni di routing mediante invio di routing update a selezionati router (neighbor) invece che in modalità broadcast:

```
router rip
network 10.109.0.0
passive-interface ethernet 1
neighbor 10.109.20.4
```

Modifica delle informazioni di routing

- E’ possibile alterare localmente le informazioni di routing apprese tramite RIP o da propagare all’esterno, in modo da alterarne volutamente l’effetto:

`offset-list` *[acl_num|name]* *{***`in`**|**`out`***}* *offset [type_number]*

timers

`timers basic` *update invalid holddown flush*

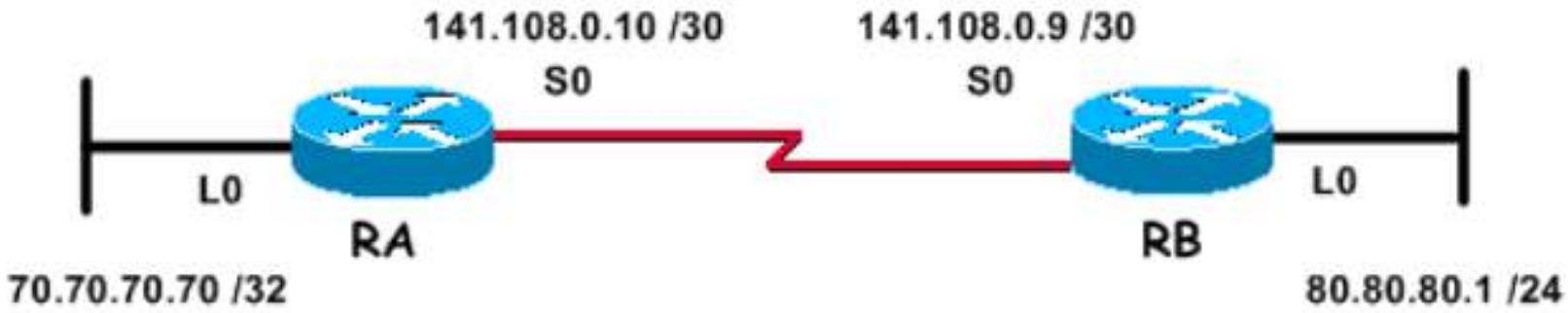
Intervallo di aggiornamento in sec (30)

Intervallo in sec oltre il quale la route è dichiarata non valida. Deve essere almeno il triplo di update (180)

Intervallo in sec, in cui viene soppresso l'aggiornamento riguardo il 'better path' . Una route entra in questo stato quando il router riceve un pacchetto che informa che la route non è più raggiungibile. La route viene etichettata come inaccessibile ed annunciata come irraggiungibile. Deve essere almeno il triplo di update (180)

Lasso di tempo in sec trascorso dall'ultimo aggiornamento oltre il quale la route è cancellata dalla routing table. L'intervallo deve essere maggiore della somma di *holddown* e *update* (240)

Autenticazione (RIP 2)



router RA

```
key chain ka1
key 1
key-string 234
interface loopback0
ip address 70.70.70.70 255.255.255.255
interface serial0
  ip address 141.108.0.10 255.255.255.252
ip rip authentication mode md5
ip rip authentication key-chain ka1

router rip
  version 2
  network 141.108.0.0
  network 70.0.0.0
```

router RB

```
key chain ka1
key 1
key-string 234
interface loopback0
ip address 80.80.80.1 255.255.255.0
interface serial0
  ip address 141.108.0.9 255.255.255.252
ip rip authentication mode md5
ip rip authentication key-chain ka1

router rip
  version 2
  network 141.108.0.0
  network 80.0.0.0
```

EGP dynamic routing protocol

Border Gateway Protocol
(BGP)

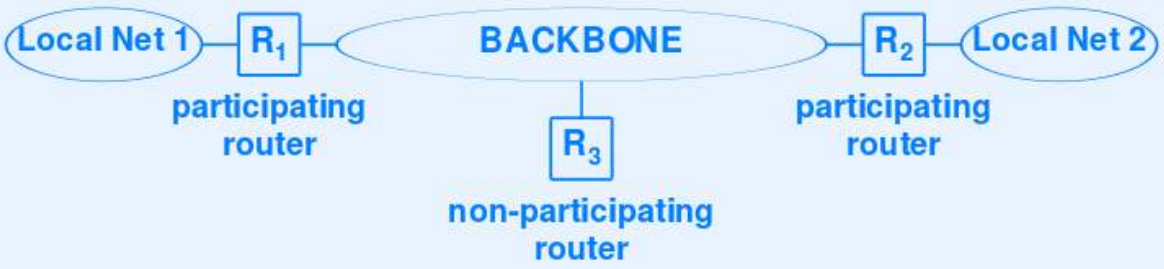
Border gateway Protocol (BGP)

- I router di Internet devono essere divisi in gruppi per 3 motivi:
  - Se ogni organizzazione fosse costituita da una singola rete, non esisterebbe un protocollo di routing in grado di scambiare informazioni di routing in modo efficiente: se il numro di router è grande il traffico diventa insostenibile.
  - Poiché non condividono una rete comune, i router di Internet non possono comunicare direttamente
  - In una grande rete Internet, le reti e i router non possono essere gestiti tutti da una singola entità e non sono sempre scelti I percorsi più brevi. Poiché le reti sono possedute e gestite da organizzazioni commerciali indipendenti, queste devono poter scegliere politiche differenti.

Border gateway Protocol (BGP)

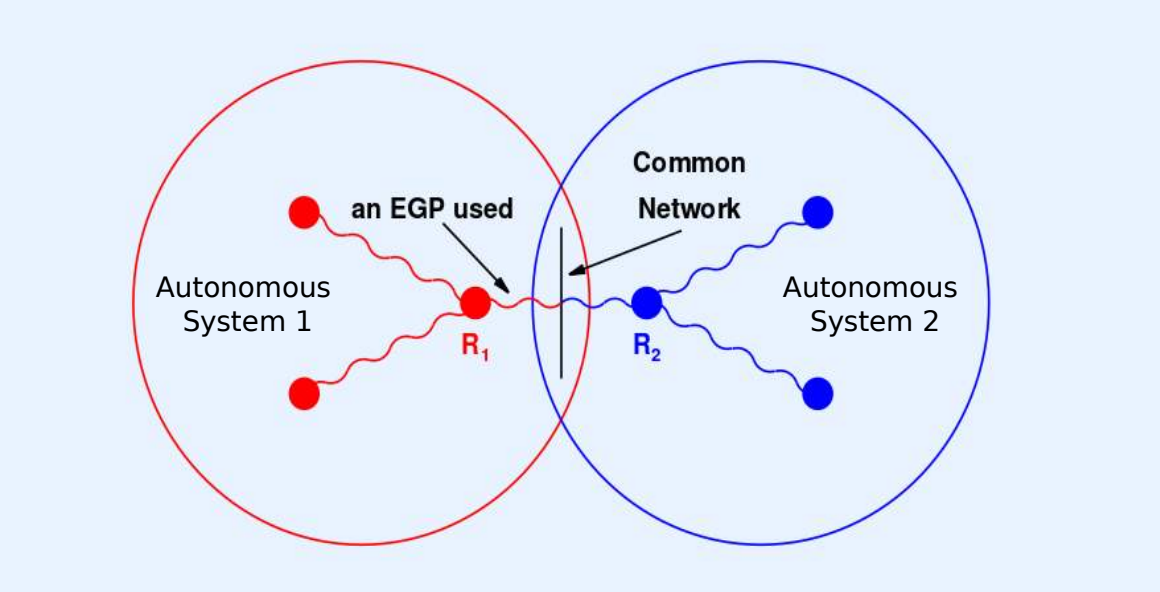
- Un'architettura d'instradamento deve fornire un modo perché ciascun gruppo controlli indipendentemente l'istradamento e l'accesso
- Due sono i problemi che impattano sulla capacità dei router di scambiarsi efficientemente le informazioni di routing:
  - Il ritardo: il tempo che occorre affinché le informazioni aggiornate si propaghino dipende dal numero di router coinvolti, N. Per questo N deve essere mantenuto piccolo.
  - L'overhead: poiché ogni router deve inviare messaggi per aggiornare le informazioni, maggiore è il numero di router coinvolti, maggiore è il traffico. Siccome i messaggi contengono l'elenco delle possibili destinazioni, anche le dimensioni aumentano al crescere del numero di router.

Border gateway Protocol (BGP)



- Se un router esterno ad un gruppo (R_3) sceglie un router partecipante ad un gruppo (R_1) come default router si generano inefficienze: R_3 invierà a R_1 anche il traffico destinato alla rete 2 invece che inviare i pacchetti direttamente a R_2 (problema del salto extra).
- ICMP non aiuta perché tali info non possono essere scambiate con i router intermedi, ma solo alla sorgente.

Border gateway Protocol (BGP)



- I router R1 e R2 sono *peer BGP* uno dell'altro e sono detti router di confine dei rispettivi Autonomous System
- I router R1 e R2, attraverso BGP, annunciano la raggiungibilità delle reti dei propri AS all'esterno

Border gateway Protocol (BGP)

- Caratteristiche di BGP:
  - Comunicazione tra AS
  - Coordinamento tra più router BGP (iBGP)
  - Diffusione delle informazioni di raggiungibilità
  - Paradigma del salto successivo
  - Supporto delle politiche di routing
  - Trasporto affidabile
  - Informazioni d'instradamento
  - Aggiornamenti incrementali
  - Supporto per l'indirizzamento senza classi
  - Aggregazione di routes
  - Autenticazione

Border gateway Protocol (BGP)

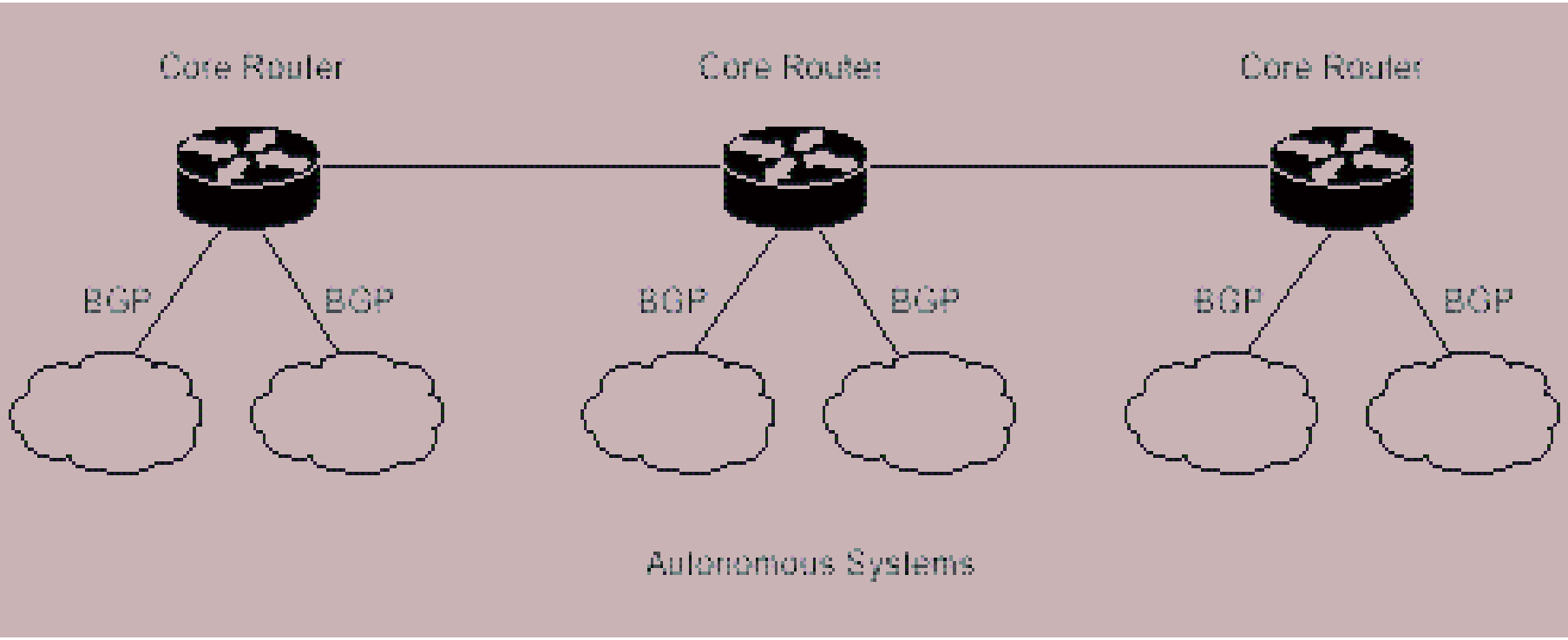
- I peer che eseguono il protocollo BGP eseguono tre funzioni di base:
  - Innanzitutto i peer si autenticano l'un l'altro e si scambiano un insieme di messaggi per stabilire la correttezza delle operazioni e se entrambi sono disponibili a comunicare
  - Successivamente avviene la fase principale del BGP: ciascuno invia all'altro le informazioni relative alle reti raggiungibili, fornendo i dati del salto successivo, o non più raggiungibili.
  - La terza funzione permette di verificare che i peer e la connessione di rete stanno funzionando correttamente.
- Per eseguire queste tre funzioni, il protocollo BGP definisce un insieme di 5 messaggi:
  - Open
  - Update
  - Notification
  - Keepalive
  - Refresh

BGP

- Diversi sono i documenti RFC relativi a BGP, tra i quali:
  - RFC 1771—Descrive BGP4, la versione corrente di BGP
  - RFC 1654—Descrive la prima specifica di BGP4
  - RFC 1105, RFC 1163, e RFC 1267—Descrivono le versioni precedenti di BGP rispetto a BGP4

Border gateway Protocol (BGP)

- BGP effettua **interdomain routing** in reti TCP/IP.
- E’ un Exterior Gateway Protocol (EGP) usato per la comunicazione tra **AS**
- Si basa su un algoritmo vettore-distanza evoluto
- Si occupa del transito di dati di terze parti su una certa rete. Le reti vengono suddivise in:
  - ✓ reti **stub** (unica connessione al grafo BGP)
  - ✓ reti **multiconnesse** (usate per il traffico in transito)
  - ✓ reti di **transito** (sono disponibili al transito di traffico di terze parti, sono spesso reti di tipo backbone)


Core Router
Core Router
Core Router
BGP
BGP
BGP
BGP
BGP
BGP
Autonomous Systems

BGP

BGP effettua

inter-autonomous system routing:

- avviene tra due o più router BGP appartenenti ad AS diversi.
- Router vicini (peers, o *neighbors*) usano BGP per mantenere una vista omogenea della topologia della rete.
- Internet usa questo tipo di routing, essendo costituita da entità che appartengono a diversi AS
- BGP è utilizzato in questi casi per calcolare il percorso che fornisca il routing migliore attraverso Internet

BGP

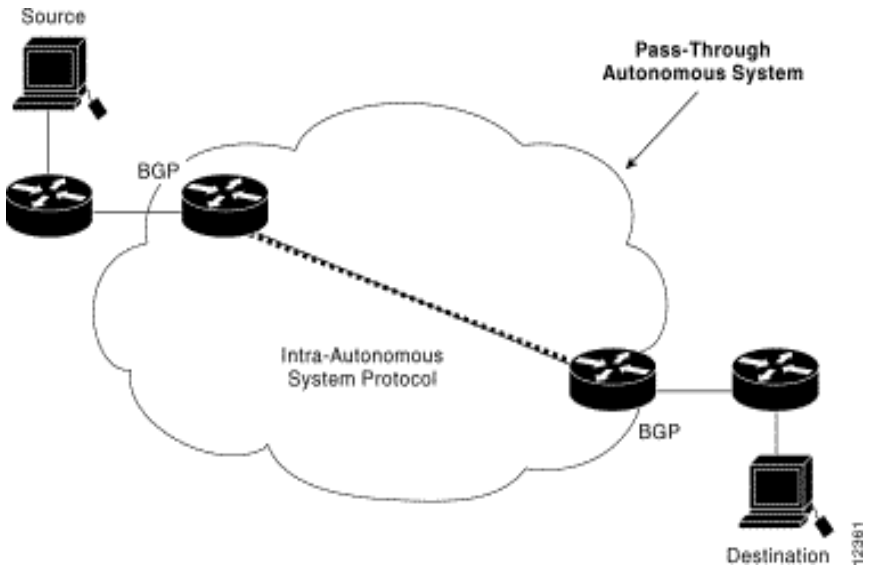
intra-autonomous system routing:

- avviene tra due o più router BGP appartenenti allo stesso AS (iBGP).
- Router vicini usano BGP per mantenere una vista omogenea della topologia del sistema.
- BGP identifica quale router serve da punto di connessione ottimale per l'interconnessione con specifici AS esterni.
- Internet usa questo tipo di routing per consentire ad un'organizzazione di usare BGP per fornire il routing ottimale tra i suoi AS.
- BGP può fornire servizi di routing sia **inter-** che **intra-** autonomous system

BGP

pass-through autonomous system routing:

- avviene tra due o più router BGP che scambiano traffico attraverso un AS che non esegue BGP.
- In un ambiente pass-through il traffico BGP non origina dentro l'AS in questione e non è destinato a nessun nodo interno dell'AS stesso.



BGP

- BGP usa la porta TCP 179
- Due router BGP formano tra loro una connessione TCP (**peer** o **neighbor** routers), si autenticano reciprocamente e scambiano messaggi per aprire e confermare i parametri di connessione.
- I due neighbor all'inizio si scambiano tutta la loro routing table, comunicando per ciascuna rete (in formato Classless Inter Doman Router (CIDR), cioè indirizzo IP/bit subnet mask) il prossimo hop
- Successivamente vengono scambiati messaggi contenenti gli aggiornamenti sui percorsi modificati
- BGP verifica continuamente che i partner e le reti stiano funzionando correttamente.

BGP routing

- BGP mantiene le routing tables, trasmette routing update e basa le decisioni di routing sulla base delle routing metric
- Le funzioni primarie sono lo scambio di informazioni network reachability, inclusa la lista dei percorsi per gli AS con altri sistemi BGP
- Ogni router BGP mantiene una lista di tutti i percorsi fattibili verso una particolare rete. Il router non aggiorna le tabelle fino a che non riceve un aggiornamento incrementale.

BGP routing

- I dispositivi BGP scambiano informazioni di routing sulla base di uno scambio iniziale e successivi aggiornamenti.
- Quando un router si collega per la prima volta riceve l’intera tabella di routing. Similmente quando le informazioni cambiano, vengono spedite in forma di insieme di aggiornamenti periodici.
- L’aggiornamento propaga solo il routing ottimale per una certa rete

BGP routing

- BGP mantiene un numero di versione della routing table che deve essere lo stesso per il rispettivo peer BGP
- Il numero di versione cambia ogni volta che BGP aggiorna la routing table attraverso aggiornamenti
- pacchetti di tipo *keepalive* sono inviati per verificare l'integrità della sessione BGP tra i peers
- pacchetti di tipo *notification* sono inviati in risposta a condizioni di errore o in situazioni speciali

BGP routing

- BGP usa una routing metric singola, che consiste in un numero in unità arbitrarie che specifica il grado di preferenza per quel dato link.
- Viene assegnato dal Network Administrator ad ogni link
- Il numero assegnato può basarsi su ogni tipo di criterio possibile, incluso il numero di AS che devono essere attraversati, la scalabilità, la velocità, il ritardo della comunicazione, il costo.

BGP: tipi di messaggi

- L'RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*, definisce 5 tipi di messaggio:

  open message: apre una sessione BGP tra *peers* ed è il primo messaggio inviato da ciascuna parte dopo l'attivazione della sessione TCP. Questo messaggio è confermato da un messaggio *keep-alive* del peer e deve essere confermato prima che abbia luogo lo scambio di messaggi ordinario.

  update message: è usato per effettuare l'aggiornamento del routing ad ogni sistema BGP, consentendo ai router di effettuare un disegno consistente della topologia di rete. Gli aggiornamenti sono inviati usando TCP per ragioni di affidabilità. Il messaggio di update può cancellare route irrangiungibili dalla routing table

BGP: tipi di messaggi (2)

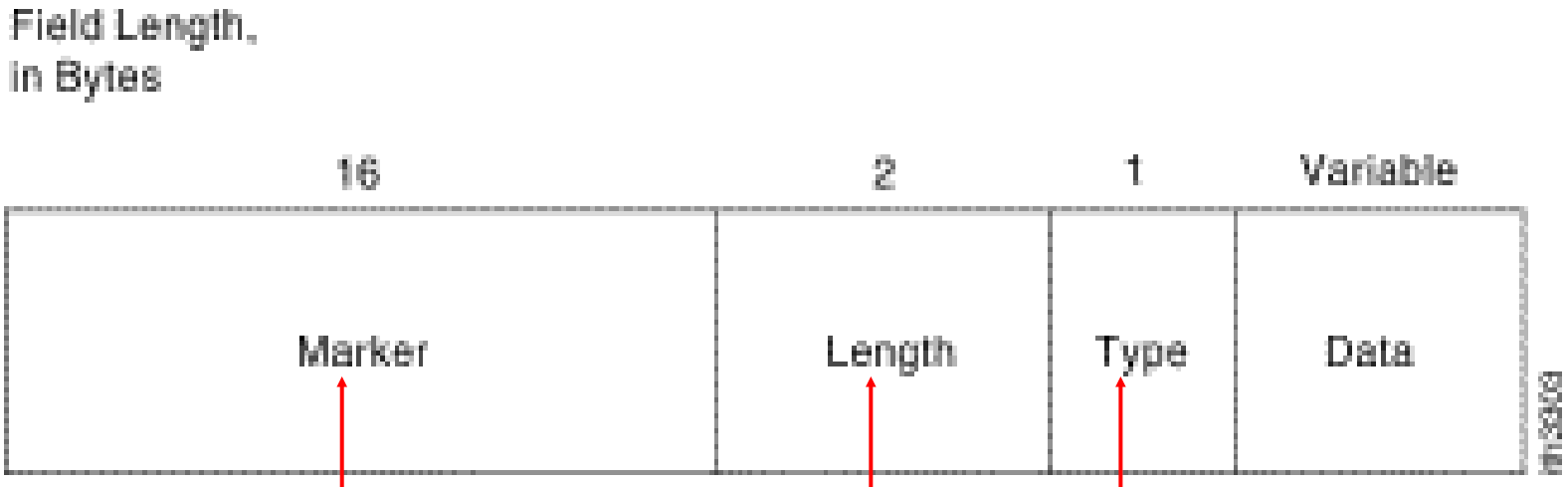
notification message: è inviato quando si evidenzia una condizione di errore. Il messaggio *notification* è utilizzato per chiudere una sessione attiva e per avvisare i router connessi del perché la sessione viene chiusa

keep-alive message: informa ogni sistema peer BGP che un dispositivo è attivo. I messaggi *keep-alive* sono inviati con una frequenza tale da prevenire che la sessione BGP si esaurisca.

refresh message: richiede il reinvio delle informazioni di routing per una rete da parte di un peer

BGP: formato dei pacchetti - Header

Ciascun pacchetto BGP contiene un header la cui funzione principale è quella di identificare lo scopo del pacchetto in questione.



Contiene un valore riconosciuto da entrambi i peers per contrassegnare l'inizio del messaggio. Importante per la sincronizzazione e l'autenticazione, ...

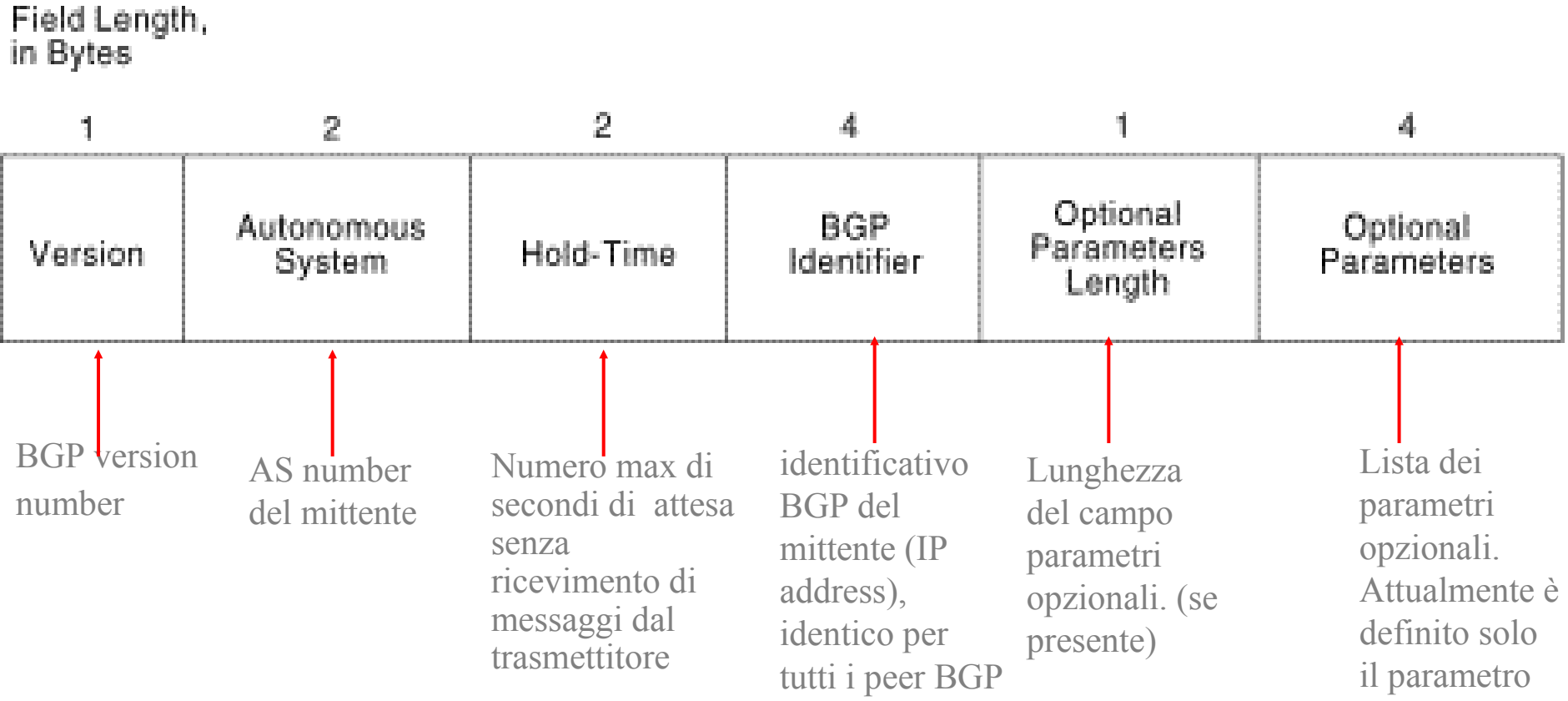
Contiene la lunghezza del messaggio in bytes (min 19B, max 4096B)

Open
Update
Refresh
Data

Notification
Keep-alive

BGP: Open message

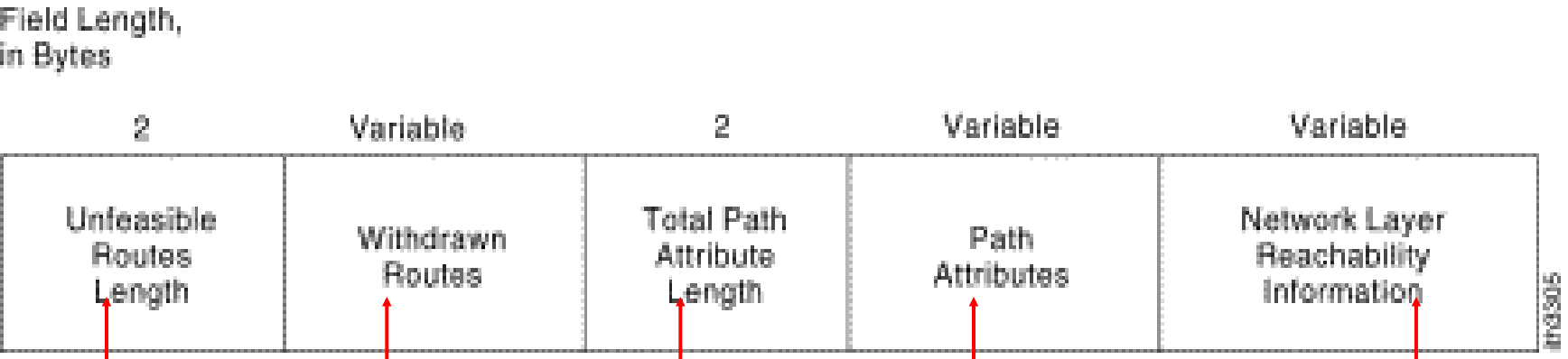
Un *open message BGP* è costituita da un header e da:



Un messaggio OPEN è confermato dal ricevimento di un messaggio KEEPALIVE

BGP: Update message

Un *update message BGP* è costituita da un header e da:



Indica la lunghezza del campo withdrawn routes

Lista di IP riferiti a route irrangiungibili

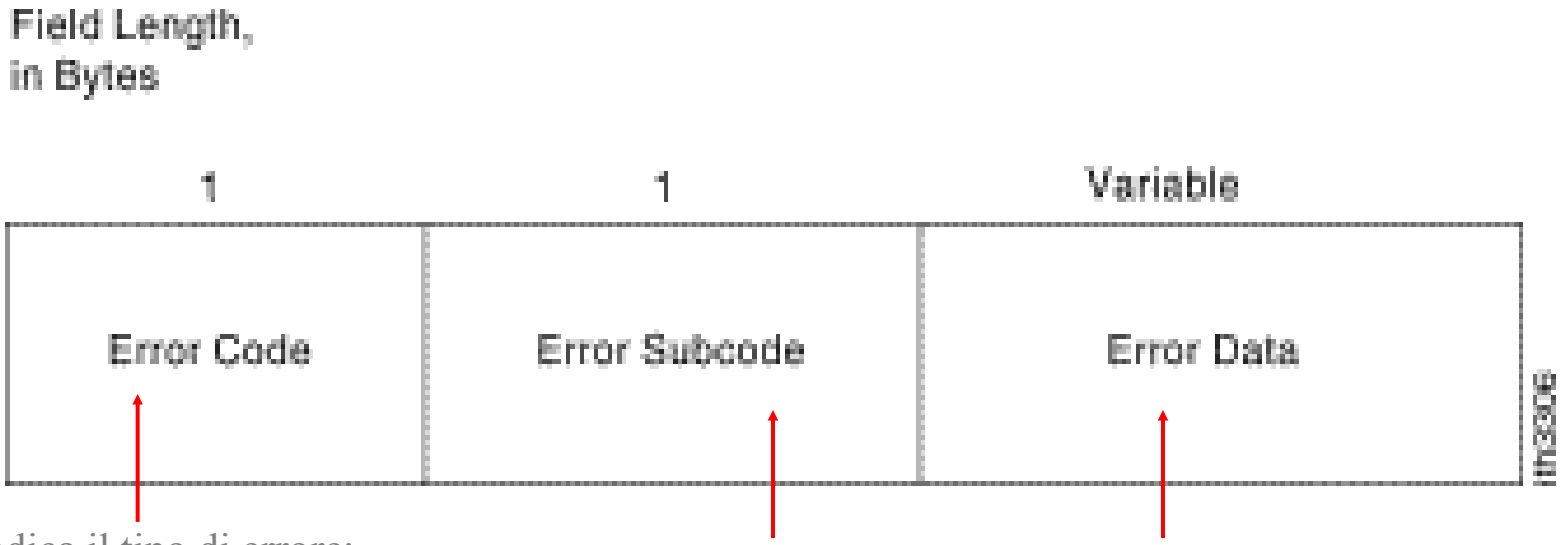
Lunghezza del campo Path Attribute

Descrive le caratteristiche del percorso annunciato:
Origin
AS path
Next Hop
Multi Exit Disc
Local Pref
Atomic aggregate
Aggregator

Contiene la lista di prefissi IP riferiti alle route annunciate

BGP: Notification message

Un *notification message BGP* è costituita da un header e da:



Indica il tipo di errore:

Message Header Error,

Open Message Error,

Update Message Error,

Holt Time Expired,

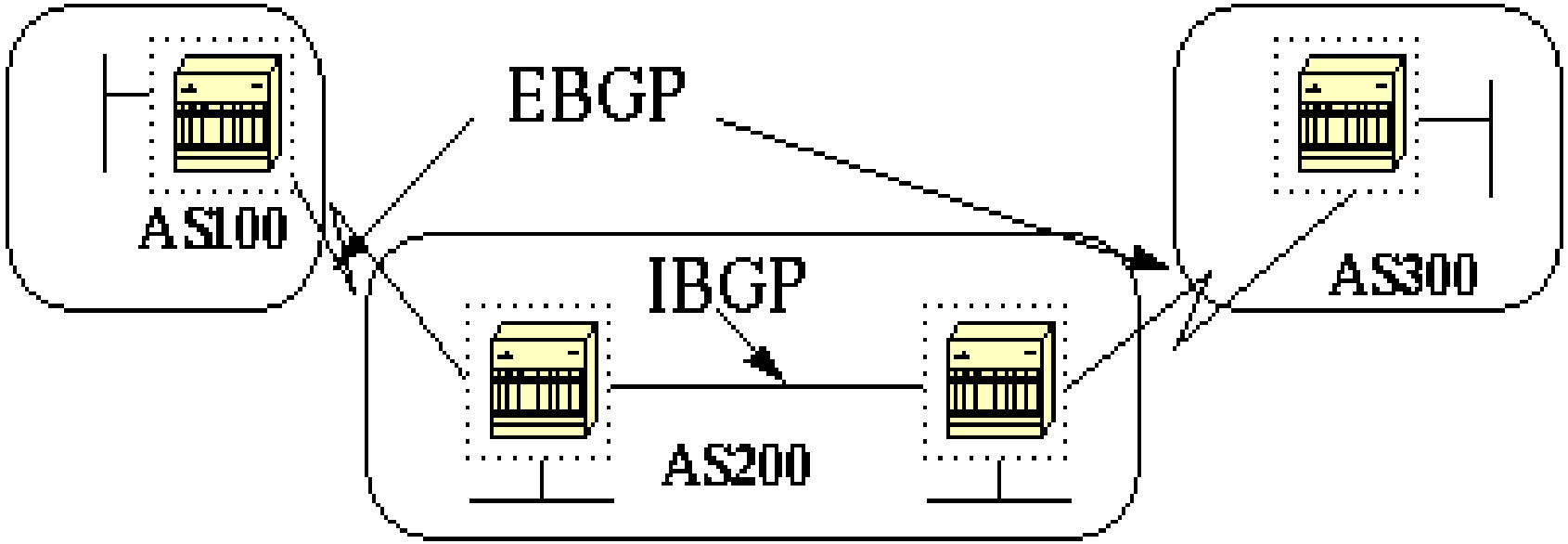
Finite State Machine Error,
Cease

Fornisce ulteriori informazioni sulla natura dell'errore riportato

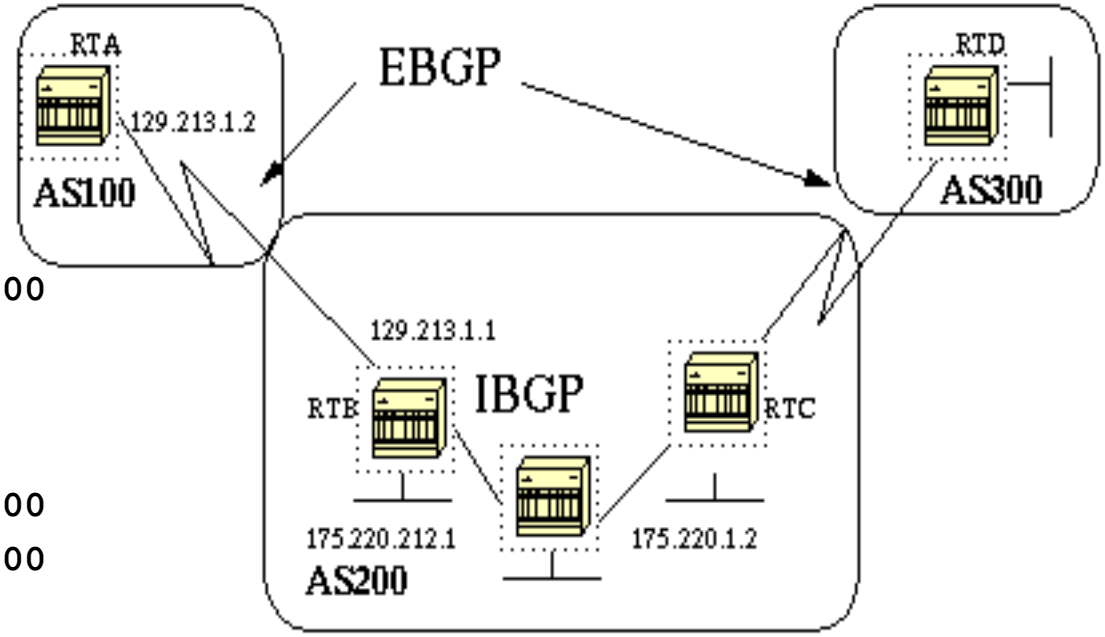
Contiene dati relativi all'errore e ai sottocodici di errore. E' un campo usato per diagnosticare la ragione del messaggio

eBGP e iBGP

- Si può distinguere tra eBGP (peers appartenenti ad AS diversi) e iBGP (peers appartenenti allo stesso AS):



BGP: esempio

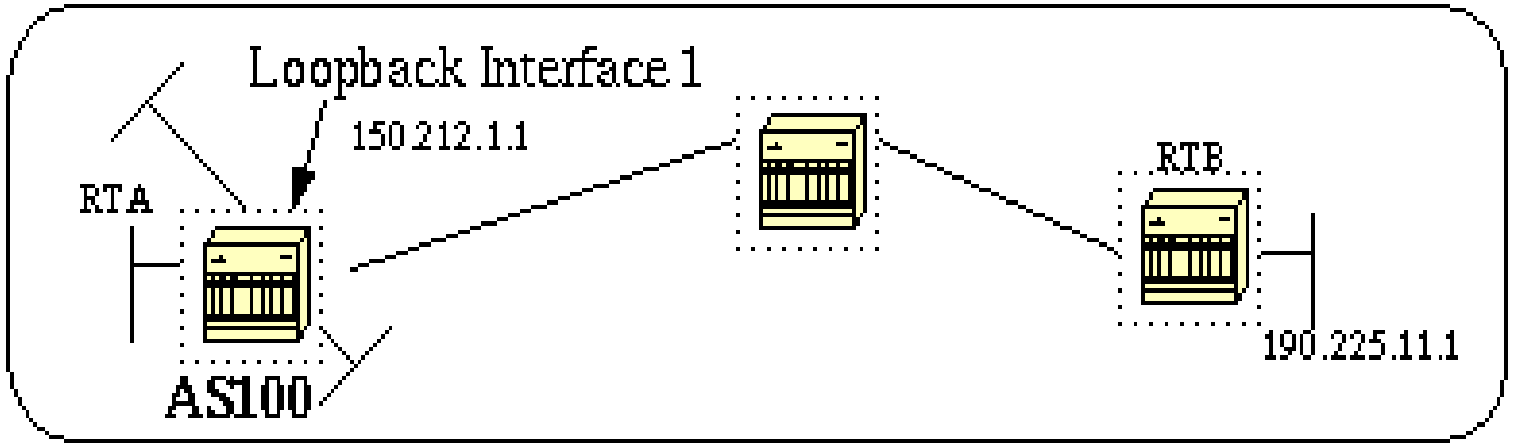



```
RTA#
router bgp 100
neighbor 129.213.1.1 remote-as 200

RTB#
router bgp 200
neighbor 129.213.1.2 remote-as 100
neighbor 175.220.1.2 remote-as 200

RTC#
router bgp 200
neighbor 175.220.212.1 remote-as 200
```

BGP: esempio

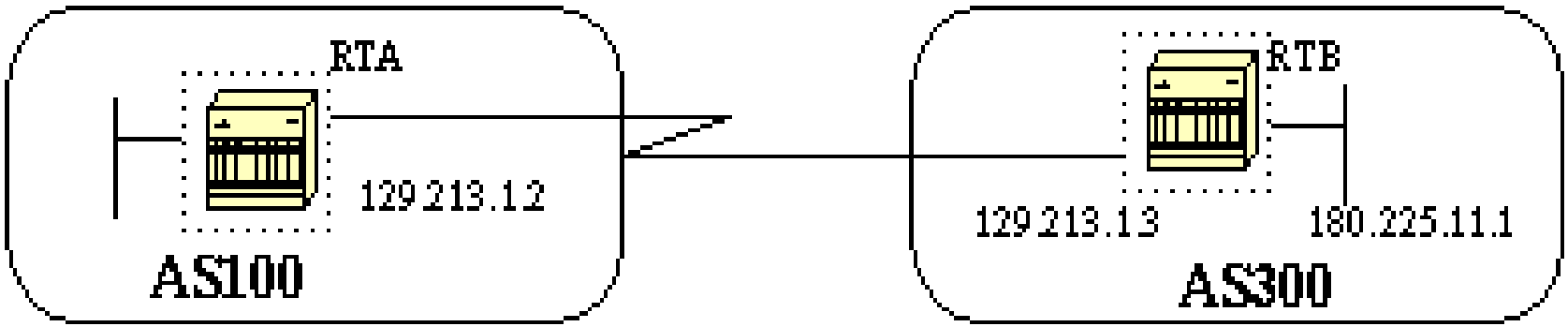
```
#show ip bgp neighbors
          BGP neighbor is 129.213.1.1, remote AS 200, external link
        BGP version 4, remote router ID 175.220.12.1
        BGP state = Established, table version = 3, up for 0:10:59
        Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
        Minimum time between advertisement runs is 30 seconds
        Received 2828 messages, 0 notifications, 0 in queue
        Sent 2826 messages, 0 notifications, 0 in queue
        Connections established 11; dropped 10
```

BGP: esempio con loopback interf.




```
RTA#
   router bgp 100
   neighbor 190.225.11.1 remote-as 100
   neighbor 190.225.11.1 update-source int loopback 1

RTB#
   router bgp 100
   neighbor 150.212.1.1 remote-as 100
```

eBGP multihop




```
RTA#
     router bgp 100
     neighbor 180.225.11.1 remote-as 300
     neighbor 180.225.11.1 ebgp-multihop

     RTB#
     router bgp 300
     neighbor 129.213.1.2 remote-as 100
```

Esempio su router Cisco

show ip bgp summary

```
gw>sh ip bgp summary
BGP router identifier 194.143.143.15, local AS number 9209
BGP table version is 16505373, main routing table version 16505373
123080 network entries and 244183 paths using 21706080 bytes of memory
67847 BGP path attribute entries using 4078320 bytes of memory
60703 BGP AS-PATH entries using 2019624 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 886376/6976543 prefixes, 3005036/2760853 paths, scan interval 60 s.

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
151.99.49.1     4  6664 5402219  568616 16505003    0    0 3w0d       122224
192.94.212.209  4  1267 3035284 4825672 16505003    0    0 15w0d      121958
```

Esempio su router Cisco (i)

show ip bgp neighbors

```
gw> sh bgp neighbors
BGP neighbor is 151.99.49.1,  remote AS 6664, external link
 Description: INTERBUSINESS
  BGP version 4, remote router ID 151.99.49.5
  BGP state = Established, up for 3w0d
  Last read 00:00:07, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Received 5399978 messages, 0 notifications, 0 in queue
  Sent 568441 messages, 4 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 16498361, neighbor version 16498339
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  122382 accepted prefixes consume 4895280 bytes
  Prefix advertised 778940, suppressed 0, withdrawn 678934

  Connections established 5; dropped 4
  Last reset 3w0d, due to BGP Notification sent, hold time expired
  External BGP neighbor may be up to 4 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 194.143.128.3, Local port: 12275
Foreign host: 151.99.49.1, Foreign port: 179

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
```

Esempio su router Cisco (ii)

(continua)

```
Event Timers (current time is 0x21F0442EC):
Timer          Starts    Wakeups            Next
Retrans         89727        865             0x0
TimeWait            0          0             0x0
AckHold        150348      75280             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3215576441  snduna: 3221188905  sndnxt: 3221188905     sndwnd:  16163
irs: 3508386839  rcvnxt: 3563173331  rcvwnd:      16249  delrcvwnd:    135

SRTT: 332 ms, RTTO: 527 ms, RTV: 195 ms, KRTT: 0 ms
minRTT: 20 ms, maxRTT: 1828 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

Datagrams (max data segment is 536 bytes):
Rcvd: 279978 (out of order: 2), with data: 193154, total data bytes: 54786491
Sent: 246410 (retransmit: 865, fastretransmit: 0), with data: 89340, total data
   bytes: 5612463
```

Internet routing table

```
gw>sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 194.143.128.34 to network 0.0.0.0

B    216.102.190.0/24 [20/0] via 151.99.49.1, 3w0d
B    208.221.13.0/24 [20/0] via 151.99.49.1, 3w0d
B    206.51.253.0/24 [20/0] via 151.99.49.1, 3w0d
B    205.204.1.0/24 [20/0] via 151.99.49.1, 3w0d
B    204.255.51.0/24 [20/0] via 151.99.49.1, 08:18:22
B    204.238.34.0/24 [20/0] via 151.99.49.1, 3w0d
B    204.153.85.0/24 [20/0] via 151.99.49.1, 2w6d
B    204.17.221.0/24 [20/0] via 151.99.49.1, 3w0d
B    203.238.37.0/24 [20/0] via 151.99.49.1, 3w0d
B    203.34.233.0/24 [20/0] via 151.99.49.1, 3w0d
B    200.68.140.0/24 [20/0] via 151.99.49.1, 3w0d
B    198.17.215.0/24 [20/0] via 151.99.49.1, 3w0d
B    192.68.132.0/24 [20/0] via 151.99.49.1, 10:08:06
     170.170.0.0/16 is variably subnetted, 3 subnets, 3 masks
B       170.170.0.0/19 [20/0] via 151.99.49.1, 3w0d
B       170.170.224.0/20 [20/0] via 151.99.49.1, 3w0d
B       170.170.254.0/24 [20/0] via 151.99.49.1, 3w0d
B    216.239.54.0/24 [20/0] via 151.99.49.1, 2w0d
B    216.103.190.0/24 [20/0] via 151.99.49.1, 3w0d
B    213.239.59.0/24 [20/0] via 151.99.49.1, 3w0d
B    212.205.24.0/24 [20/0] via 151.99.49.1, 3w0d
B    205.152.84.0/24 [20/0] via 151.99.49.1, 3w0d
B    203.254.52.0/24 [20/0] via 151.99.49.1, 3w0d
B    203.1.203.0/24 [20/0] via 151.99.49.1, 3w0d
B    202.1.202.0/24 [20/0] via 151.99.49.1, 3w0d
B    198.205.10.0/24 [20/0] via 151.99.49.1, 3w0d
B    198.69.130.0/24 [20/0] via 151.99.49.1, 14:43:27
B    192.35.226.0/24 [20/0] via 151.99.49.1, 5d22h
     170.171.0.0/16 is variably subnetted, 4 subnets, 2 masks
B       170.171.0.0/16 [20/0] via 151.99.49.1, 3w0d
B       170.171.251.0/24 [20/0] via 151.99.49.1, 3w0d
```

Perché un nuovo protocollo IP?

- Lo spazio di indirizzamento IPv4 prossimo all'esaurimento, anche se le problematiche relative sono state mitigate dall'adozione delle reti private e dalla combinazione dei protocolli DHCP e NAT.
- Migliore gestione del traffico IP e possibilità di gestire Quality of Service (QoS)
- Uno spazio di indirizzamento piu' grande, da 32 bit a 128 bit:
  - Permette una reale connettivita' globale
  - Non piu' reti o host nascosti
  - Tutti gli host possono essere raggiungibili e quindi essere "server"
  - E' possibile usare sistemi di sicurezza Punto-Punto

RFC2460: *Internet Protocol, Version 6 (Ipv6) Specification*

Perché un nuovo protocollo IP?

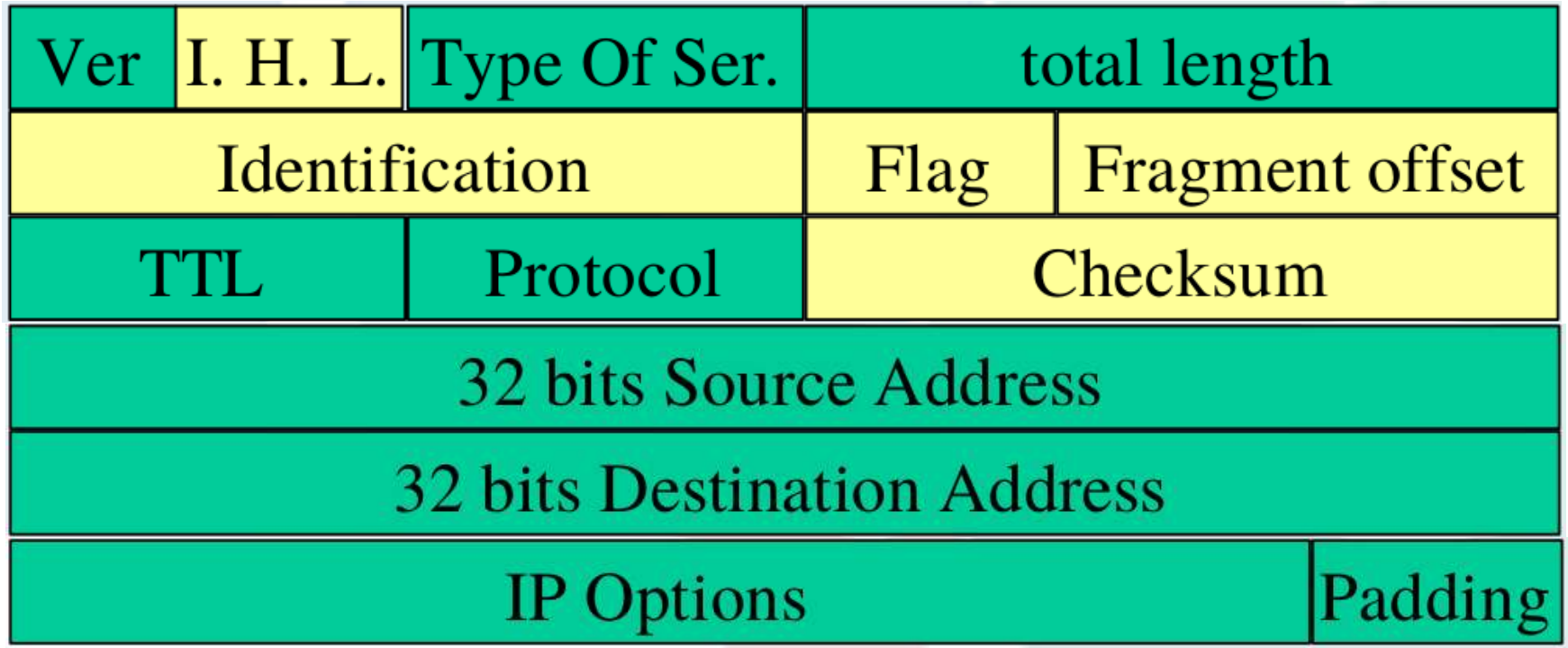
- Autoconfigurazione
  - La possibilita' di usare 64 bits per l'host con la garanzia di unicita'
  - "plug and play"
  - Possibilita' di gestire in modo piu' semplice il Multihoming
  - Facilita' nel Renumbering
- Intestazione del pacchetto IP efficiente ed estensibile:
  - Un numero minore di campi nell'header principale
    - ✓ Efficienza di Routing
    - ✓ Migliori prestazioni
  - Estendibilita' dell'header
    - ✓ Miglior gestione delle opzioni
  - Eliminata la possibilita' di frammentare un pacchetto in transito

Perché un nuovo protocollo IP?

- Caratteristiche intrinseche
  - Sicurezza
  - Mobilita'
  - Maggior utilizzo del Multicast
    - ✓ Sostituisce il broadcast
  - Uso piu' efficiente della rete

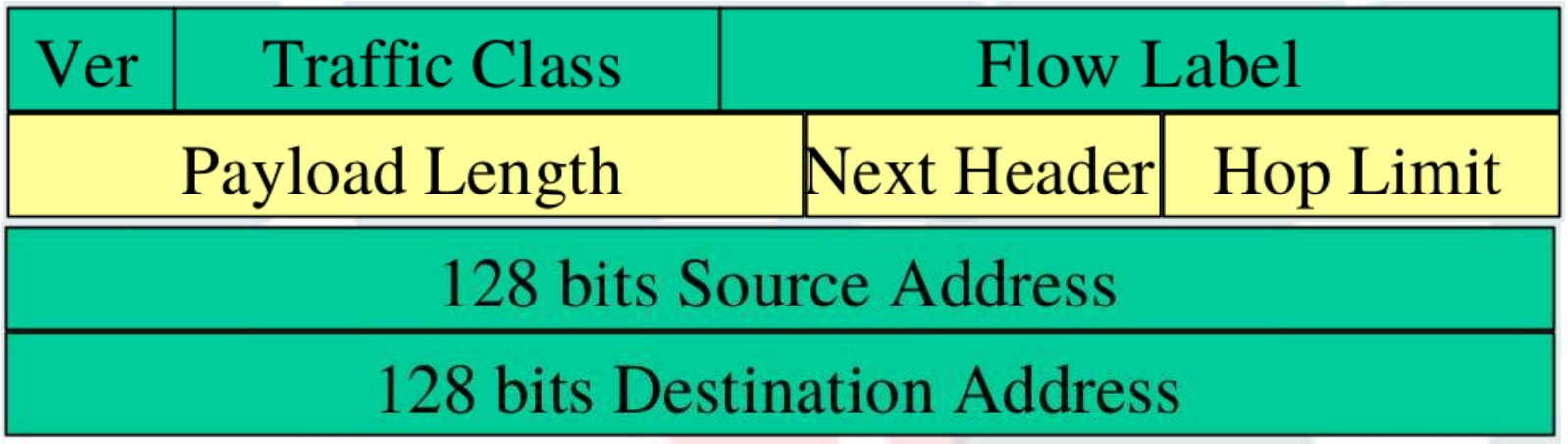
Header IPv4

- Header Ipv4
  - Allineamento a 32 bit, I campi in giallo spariscono in IPv6



Header IPv6

- Allineato a 64 bit, 40 byte senza le Header Extension



Header IPv6

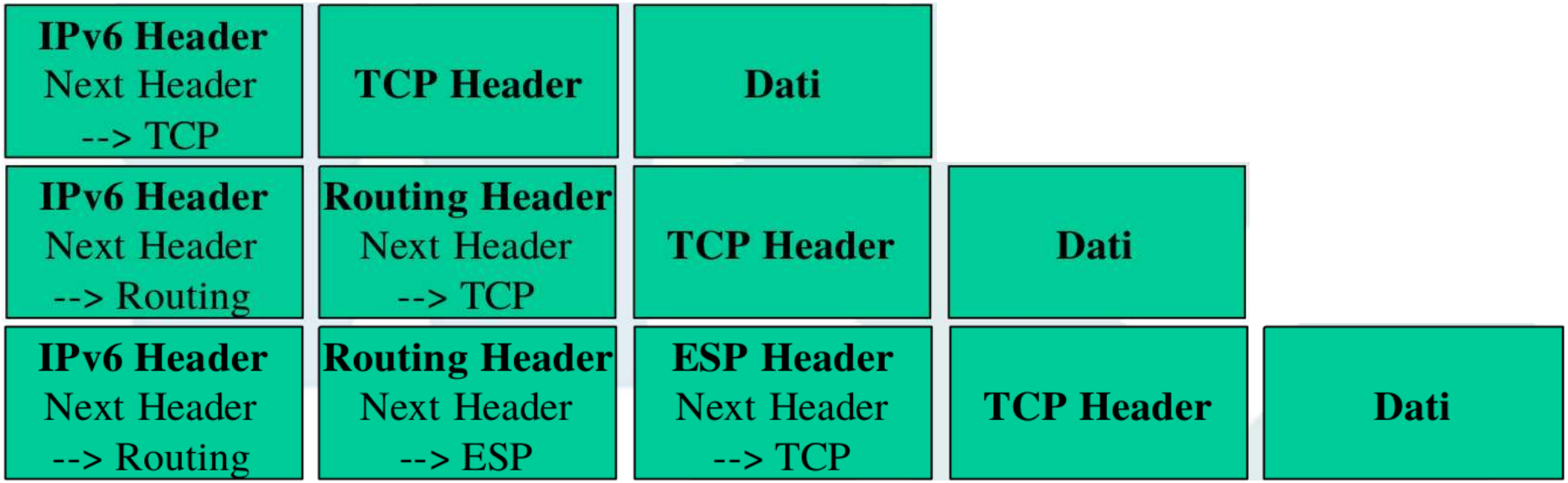
- Version. 4 bits.
  - 6 - IPv6.
- Traffic Class. 8 bits.
  - Valore per identificare la priorita' del pacchetto nel traffico Internet. (simile al TOS ipv4)
- Flow Label. 20 bits.
  - Utilizzo ancora non chiaro. Usato per specificare uno speciale trattamento dei ruoter fra la sorgente e la destinazione per il pacchetto.
- Payload Length. 16 bits, unsigned.
  - Specifica la lunghezza dei dati nel pacchetto.

Header IPv6

- Next Header. 8 bits.
  - Specifica l’header successivo. Se e' un protocollo di livello piu' alto, i valori sono compatibili con quelli specificati per l’IPv4.
- Hop Limit. 8 bits, unsigned.
  - Per ogni router che il pacchetto attraversa questo campo e' decrementato di 1. Quando il vale 0 il pacchetto e' scartato. Sostituisce il TTL Ipv4.
- Source address. 16 bytes.
  - L’indirizzo IPv6 del mittente.
- Destination address. 16 bytes.
  - L’indirizzo IPv6 del destinatario.

Extension header

- Un nuovo metodo per implementare le opzioni
- Aggiunto dopo l'header di base IPv6



ESP: Encapsulating Security Payload

Tipi di header

00 = Hop-by-Hop Options

43 = Routing

44 = Fragment

51 = Authentication

60 = Destination Options

50 = Encapsulating Security Payload

xx = Protocolli di livello piu' alto come per IPv4

58 = Internet Control Message Protocol (ICMPv6)

59 = nessun next header. Un nuovo metodo per implementare le opzioni

Tipi di header

- Hop-by-hop options (00)
  - Queste informazioni devono essere esaminate da ogni nodo lungo il percorso del pacchetto.
  - Usato per i Router Alert ed i Jumbogram
- Routing (43)
  - Simile all'opzione IPv4 Loose Source Route
  - Indica una lista di router da attraversare.
  - Usato per il mobileIPv6
- Fragment (44)
  - Usato soltanto dall’host mittente per l’host destinarario. (I router non frammentano piu'!)

Tipi di header

- Destination options (60)
  - Usato per trasportare informazioni opzionali che saranno valutate soltanto dall'host destinatario.
  - Usato per il Mobile IPv6
- Authentication Header (51)
  - Fornisce l'autenticazione; un modo per vericare che l'indirizzo del mittente sia autentico e che il pacchetto non sia stato alterato durante il percorso.
- Encapsulating Security Payload (50)
  - Garantisce che solo il destinatario autorizzato sarà in grado di leggere il pacchetto.

Tipi di header

- L’ordine degli headers nel pacchetto dovrebbe essere il seguente:
  - IPv6 header
  - Hop-by-Hop Options header
  - Destination Options header (quando e' presente il routing header)
  - Routing header
  - Fragment header
  - Authentication header
  - Encapsulating Security Payload header
  - Destination Options header
  - Upper-layer header

Indirizzi IPv6

- IPv4 = 32 bits
- IPv6 = 128 bits
  - Non 4 volte il numero di indirizzi: 4 volte il numero di bit!
  - ~3,4 * 10^{38} possibili nodi indirizzabili
  - 10^{30} indirizzi per ogni persona del pianeta
- a:b:c:d:e:f:g:h
- – Dove ogni campo è composto da 16 bit in notazione esadecimale

  2001:0000:1234:0000:0000:00D0:ABCD:0532
- Il valore e' indipendente dalla notazione maiuscola o minuscola delle lettere

  2001:0000:1234:0000:0000:00D0:abcd:0532
- • Gli zero a sinistra di ogni campo sono opzionali

  2001:0:1234:0:0:D0:ABCD:532

Formato indirizzi IPv6

- Campi successivi di zero sono rappresentati da ::

  ma solo una volta in un indirizzo.

  2001:0:1234::D0:ABCD:532

- Non e' valida la notazione:

  2001::1234::C1C0:ABCD:876

- Altri esempi:
  - FF02:0:0:0:0:0:0:1 => FF02::1
  - 0:0:0:0:0:0:0:1 => ::1
  - 0:0:0:0:0:0:0:0 => ::

Formato indirizzo in una URL

- In una URL, devono essere scritti fra parentesi quadre.

  http://[2001:1:4F3A::206:AE14]:8888/index.html
- I programmi che usano URL (browser, etc.) sono stati modificati allo scopo.
  - Scomodo per gli utenti
  - Prevalentemente usato per scopi diagnostici
  - Piu' comodo usare una notazione per nome a dominio.

Tipi di indirizzi

- Unicast
  - Unspecified
  - Loopback
  - Indirizzi Scoped
  - Link-local
  - Site-local
- Aggregatable Global
- Multicast
  - Broadcast non esiste in IPv6
- Anycast

Indirizzo Unspecified

- Indica l’assenza di indirizzo
- Puo' essere usato nella richiesta iniziale DHCP per ottenere un indirizzo
  - Duplicate Address Detection (DAD)
  - 0:0:0:0:0:0:0:0 o ::
  - Come 0.0.0.0 in Ipv4 (::/0 indica la rotta di default)

Indirizzo Loopback

- Identifica l’host stesso
- Il Localhost
- Come 127.0.0.1 in IPv4
- 0:0:0:0:0:0:0:1 o ::1
- Per controllare se lo stack IPv6 funziona:
  - Ping6 ::1

Subnet Prefix e Host Identifier

- L'indirizzo IPv6 unicast e' diviso in due parti:
  - Primi 64 bit identificano il prefisso di rete
  - Ultimi 64 bit identificano l'host
  - 0:0:0:0 : 0:0:0:0
  - L'host puo' essere identificato:
    - ✓ Manualmente 0, 1, 2, 3 etc.
    - ✓ Usando l'identificativo di interfaccia MAC o EUI 48. Viene ricalcolato per essere usato come parte host dell'indirizzo IPv6 - EUI 64.

Indirizzo Link local

- E’ uno Scoped address (novità di IPv6)
- Scope (Ambito) = local link (i.e. LAN, VLAN)
  - Può essere usato solo fra nodi dello stesso link
  - Non può essere instradato dai router
- Automaticamente configurato su ogni interfaccia
  - Usa l’interface identifier (basato sul MAC address)
- Formato:

  FE80:0:0:0:<interface identifier>

- Fornisce ad ogni nodo un indirizzo IPv6 per iniziare le comunicazioni.

Indirizzo Site local

- E’ uno Scoped address
- Scope = site (una rete di link)
  - Può essere usato soltanto fra nodi dello stesso site
  - Non puo' essere usato fuori dal site (es. Internet)
  - Molto simile agli indirizzi privati Ipv4
- Non configurato di default
- Formato:

  FEC0:0:0:<subnet id>:<interface id>

  Subnet id = 16 bits = 64K subnets
  - Permette un piano di indirizzamento per un intero sito
- Esempi d’uso:
  - Numerare un site prima di connetterlo ad Internet.
  - Indirizzamento privato (es. stampanti locali)

Aggregatable Global

- La politica dell’assegnazione di indirizzi IPv6 deve essere profondamente diversa da quella di IPv4 considerata l’abbondanza di indirizzi IPv6.
- Come Best Practice si adotta la seguente strategia:
  - /23 per i Regional Registries
  - /35 per I Local Internet Registries
  - /48 per le organizzazioni (utenti finali)
  - /64 per le sottoreti degli utenti

Multicast

- Multicast = uno a tanti
- Non esiste il broadcast in IPv6. Multicast è usato al suo posto, soprattutto nei link locali.
- Scoped addresses:
  - Node, link, site, organisation, global
  - Sostituisce il TTL dell'IPv4
- Formato:
  - FF<flags><scope>::<multicast group>
    - ✓ Flag = 0 permanente / 1 temporaneo

Indirizzi Multicast riservati

Address	Scope	Use
FF01::1	Interface-local	All Nodes
FF02::1	Link-local	All Nodes
FF01::2	Interface -local	All Routers
FF02::2	Link-local	All Routers
FF05::2	Site-local	All Routers
FF02::1:FFXX:XXXX	Link-local	Solicited-Node

Anycast

- Uno al piu' vicino: serve per le funzioni di discovery
- Gli indirizzi Anycast non sono distinguibili dagli indirizzi Unicast
  - Allocati dallo stesso spazio di indirizzamento Unicast
  - Ultimi 64 bit formati da serie di 1 e ultimi 7 bit dell'indirizzo (diversi se EUI64 o non EUI 64)
- Alcuni indirizzi anycast sono riservati per usi specifici :
  - Router-subnet
  - Mobile IPv6 home-agent discovery

Indirizzi per ogni host

- Ogni host IPv6 dovrebbe riconoscere i seguenti indirizzi come identificanti se stesso:
  - Indirizzo Link-local per ogni interfaccia
  - Indirizzi unicast/anycast assegnati (manualmente o automaticamente)
  - Indirizzo di Loopback
  - Indirizzo del gruppo All-nodes multicast
  - Indirizzi Solicited-node multicast per ogni indirizzo unicast e anycast assegnato
  - Indirizzi Multicast di tutti gli altri gruppi di cui l'host faccia parte

Come l’host seleziona un indirizzo

- Un nodo ha molti indirizzi IPv6
- Quale sara' usato come sorgente e destinazione per
- ogni flusso?
- La scelta viene fatta principalmente in base a queste
- regole:
  - ✓ Usare il giusto scope in base alla destinazione (global, site, local)
  - Usare l'indirizzo piu' simile alla destinazione (Ipv4, Ipv6)
- L'algoritmo di scelta puo' essere sovrascritto dall'applicazione o dai protocolli dello Stack TCP/IP.

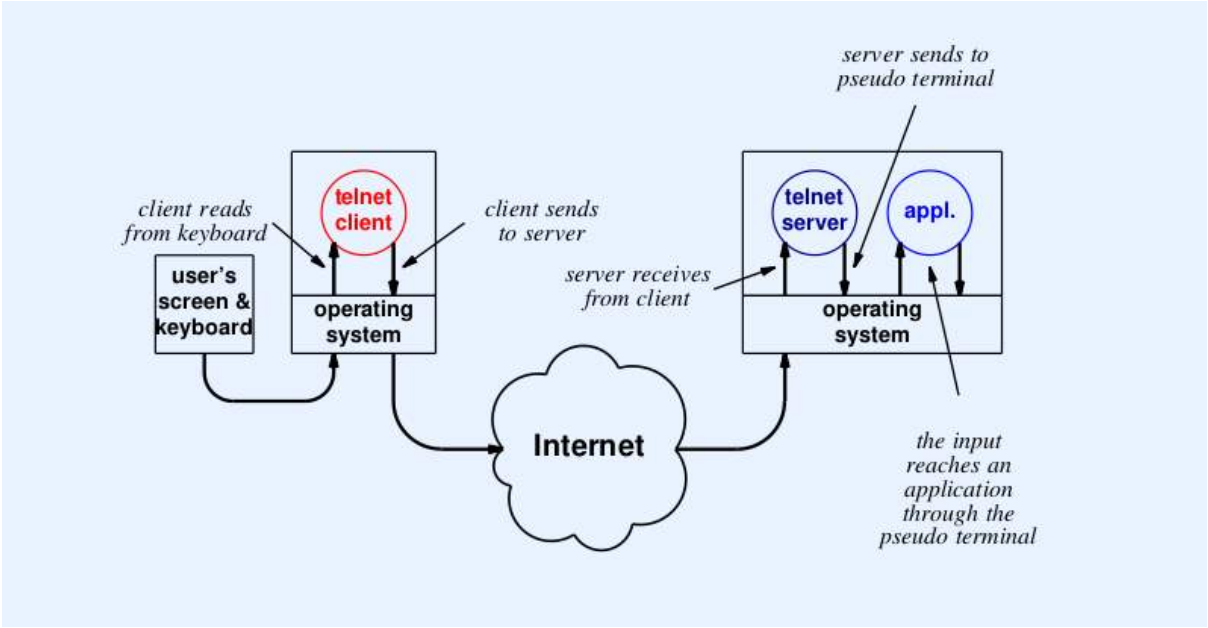
Servizi di Rete

Telnet

- E' un servizio di rete di emulazione di un terminale a carattere (ASCII). E' definito da RFC854 e RFC855.
- Effettua l'astrazione del terminale consentendo l'accesso remoto attraverso la rete
- Client
  - Invocato dall'utente
  - Realizza la connessione col server remoto
  - Passa i caratteri digitati alla tastiera dall'utente al server e visualizza il risultato del comando eseguito nel server sulla finestra dell'utente
- Server
  - Accetta connessioni di rete
  - Passa i caratteri digitati dall'utente al sistema operativo, come se fossero digitati in una tastiera locale
  - Invia l'output sulla connessione del client

Telnet

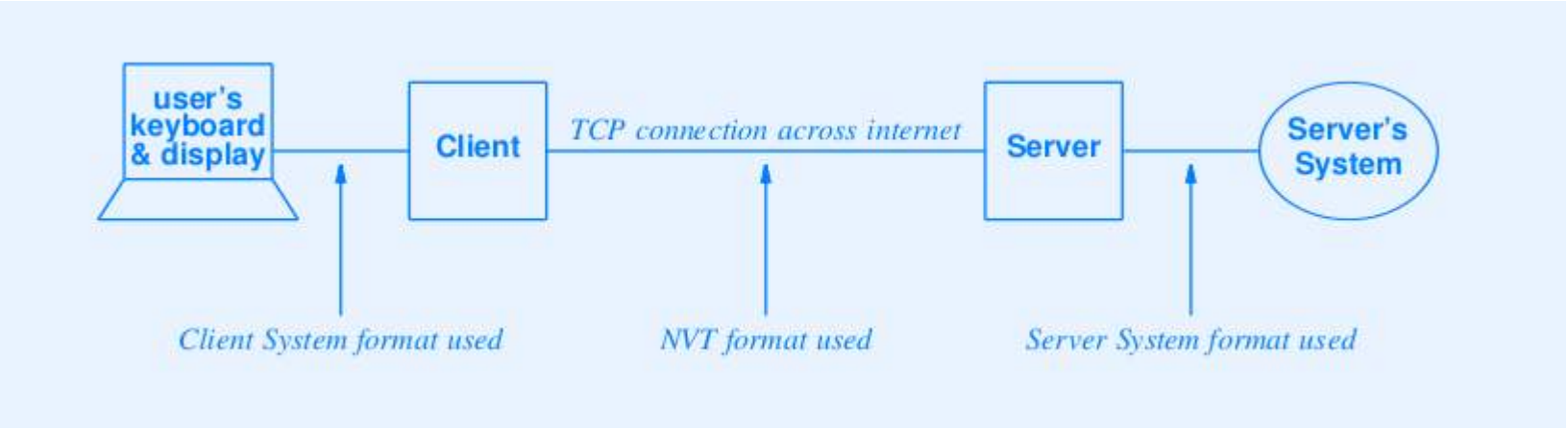
- servizio di emulazione di terminale attraverso la rete
- si basa sul protocollo TCP -> connessione affidabile
- essendo strutturato secondo il paradigma client/server:
  - client Telnet, si connette con un server Telnet in esecuzione su un altro host in ascolto sulla porta 23
  - appena connesso l'utente può eseguire comandi come se il terminale fosse locale



Telnet

- Questo servizio si basa su 3 aspetti:
  1. Network Virtual Terminal (NVT) terminale virtuale con caratteristiche generali; ogni server o client traduce i controlli nativi in quelli del NVT; permette di eliminare l'uso di specifici strumenti client e server per sfruttare questo servizio;
  2. Opzioni negoziate tra client e server per aumentare le funzionalità della sessione Telnet da aprire
  3. Viste Simmetriche che fanno si che ai lati della comunicazioni ci siano dei programmi invece di una tastiera ed un monitor fisici. La negoziazione delle opzioni può generare cicli di opzioni senza fine (errata interpretazione)

Telnet



- Funzioni di controllo standard
  - Essendo un servizio funzionante su sistemi eterogenei, i client e server possono essere implementati in modo diverso
  - Sono state standardizzate le definizioni di 7 funzionalità di controllo (Interrupt process, abort output, break, erase character, erase line, syncronize, are you there)

Definizione del Network Virtual Terminal

	ASCII Control Code	Decimal Value	Assigned Meaning
	NUL	0	No operation (has no effect on output)
bell	BEL	7	Sound audible/visible signal (no motion)
backspace	BS	8	Move left one character position
Horiz. tab	HT	9	Move right to the next horizontal tab stop
Line feed	LF	10	Move down (vertically) to the next line
Vert. tab	VT	11	Move down to the next vertical tab stop
Form feed	FF	12	Move to the top of the next page
Carriage ret.	CR	13	Move to the left margin on the current line
	other control	–	No operation (has no effect on output)

Funzioni di controllo NVT

Signal	Meaning
IP	Interrupt Process (terminate running program)
AO	Abort Output (discard any buffered output)
AYT	Are You There (test if server is responding)
EC	Erase Character (delete the previous character)
EL	Erase Line (delete the entire current line)
SYNCH	Synchronize (clear data path until TCP urgent data point, but do interpret commands)
BRK	Break (break key or attention signal)

Comandi Telnet

Command	Decimal Encoding	Meaning
IAC	255	Interpret next octet as command (when the IAC octet appears as data, the sender doubles it and sends the 2-octet sequence IAC-IAC)
DON'T	254	Denial of request to perform specified option
DO	253	Approval to allow specified option
WON'T	252	Refusal to perform specified option
WILL	251	Agreement to perform specified option
SB	250	Start of option subnegotiation
GA	249	The "go ahead" signal
EL	248	The "erase line" signal
EC	247	The "erase character" signal
AYT	246	The "are you there" signal
AO	245	The "abort output" signal
IP	244	The "interrupt process" signal
BRK	243	The "break" signal
DMARK	242	The data stream portion of a SYNCH (always accompanied by TCP Urgent notification)
NOP	241	No operation
SE	240	End of option subnegotiation
EOR	239	End of record

rlogin

- Inventato per i sistemi BSD Unix
- Include delle facilitazioni specifiche per Unix
- Permette all'amministratore di configurare una serie di macchine in modo tale che se un utente ha uno stesso identificativo in queste macchine, l'accesso avvenga senza digitare la password. Questa soluzione molto comoda perché facilita la configurazione di ambienti distribuiti, porta con sé forti problematiche di sicurezza.
- Permette altre forme di autenticazione

Remote shell (rsh)

- Simile ad rlogin
- Anch'esso parte dei sistemi BSD Unix
- Permette l'esecuzione remota di un singolo comando
- L'esito del comando viene visualizzato nella finestra dell'utente nel sistema locale, che quindi deve prevedere un'applicazione che consenta l'accesso da terminale a carattere

Port forwarding

- E' una nuova funzionalità implementata da ssh (secure shell)
- E' simile al Network Address Translation (NAT)
- Permette di istradare connessioni TCP in un canale cifrato

Remote desktop

- Disegnato per sistemi che consentono un accesso di tipo grafico (Graphical User Interface, GUI) a finestre
- Permette ad utenti remoti di visualizzare lo schermo grafico di un computer e di usare mouse e tastiera
- Esempi:
  - Virtual Network Computing (VNC)
  - Remote Desktop Protocol (RDP)

Obsolescenza di telnet

- A causa del passaggio dei dati sensibili in chiaro, che permette ad esempio ad un programma di “sniffing della rete” di catturare le informazioni sensibili, l'applicazione telnet viene bloccata nei sistemi attuali.
- Se si cerca di eseguire il comando si ottiene qualcosa del tipo:

```
osvaldo@woodiep:~$ telnet localhost
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
osvaldo@woodiep:~$
```

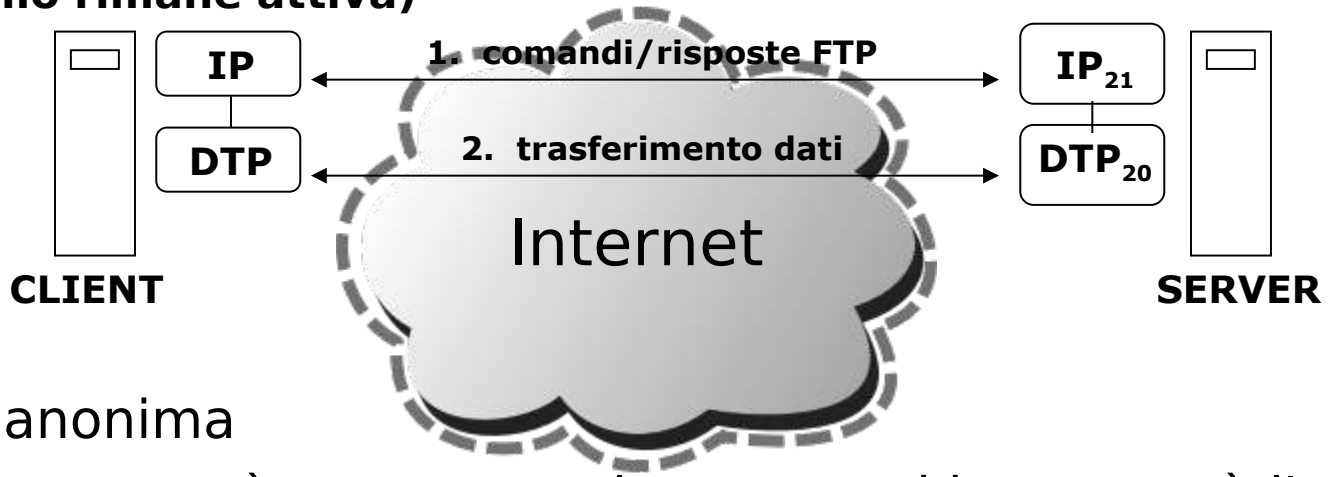
- Al posto di telnet si usa ssh, il quale trasmette informazioni crittografate.
- In windows ci sono varie soluzioni, la più semplice è putty. In ambiente Linux e Unix si dispone di openssh.

FTP (File Transfer Protocol)

- Protocollo per il trasferimento di file tra host in una rete TCP/IP (**RFC 959**)
- Essendo basato sul protocollo di trasporto TCP è orientato alla connessione ed è affidabile
- In ogni trasferimento dati intervengono 2 processi
  - Il Data Transfer Process (DTP) che si occupa del trasferimento vero e proprio tra un client e un server FTP
  - Il Protocol Interpreter che si occupa di trasmettere comandi fra il client e il server FTP (dà inizio al processo FTP)

FTP

- Una sessione FTP si compone di 2 sessioni/connessioni (bidirezionali):
  - **la prima (detta di controllo e denominata IP) viene creata tra i processi server e client; lato client viene stabilita una connessione verso il server attraverso la porta 21 (del server);**
  - **alla richiesta di trasferimento dati, il DTP server apre una apposita connessione (porta 20) con il DTP client (durante questa, la sessione di controllo rimane attiva)**



- Sessione anonima
  - account usato è **`anonymous`**, la password in genere è l'email
  - i client hanno il solo diritto di lettura, il che evita l'upload sul server di dati non autorizzati

FTP

- Client:
  - Contatta il server
  - Specifica i file
  - Specifica la direzione del trasferimento (download/upload)
- Server:
  - Mantiene un insieme di file nel disco locale
  - Rimane in attesa di richieste di connnessione
  - Onora le richieste dei client
- Caratteristiche:
  - Accesso interattivo
  - Specifica del formato (ASCII o EBCDIC)
  - Controllo dell'autenticazione (login e password)

FTP

- Per il Data Transfer il client diventa server ed il server diventa client:
  - Il Client:
    - ✓ Crea il processo per gestire il trasferimento dati
    - ✓ Alloca la porta e invia il numero al server attraverso la connessione di controllo
    - ✓ Il processo attende richieste
  - Il Server:
    - ✓ Riceve le richieste
    - ✓ Crea il processo per gestire il trasferimento dati
    - ✓ Il processo contatta il lato client

Uso interattivo di FTP

- All'inizio in protocollo FTP era usato da linea di comando:
  - L'utente invoca il client e specifica il server remoto
  - L'Utente si collega e immette la password
  - L'Utente specifica una serie di richieste
  - L'Utente chiude la connessione
- Oggi:
  - Gran parte delle richieste FTP originano da browser
  - L'Utente specifica la URL o click sul link
  - Il Browser usa FTP per contattare il server remoto ed ottiene:
    - ✓ La lista dei files
    - ✓ L'Utente seleziona il file per il download

FTP

- Comandi FTP per
  - controllo dell'accesso
    - ✓utilizzati per stabilire e terminare una sessione FTP
      - **`OPEN` *nomehost***
      - **`USER` *nomeutente* (utente che esegue i comandi FTP)**
      - **`PASS` *password***
      - **`QUIT`**
  - configurare i parametri del trasferimento
    - ✓permettono di modificare i valori di default
      - **`PORT` *indirizzIP+numero_porta***
      - **`PASV` (server passivo, il client dà inizio alla connessione)**
  - trasferimento dei file
      - **`TYPE` (ascii o binario)**
      - **`RECV` *file_remoto file_locale* (o `GET`)**
      - **`SEND` *file_locale file_remoto* (o `PUT`)**

FTP

- Comandi FTP per
  - gestione di directory e file
    - ✓ comandi usati dal client ed operanti sul server
      - **`DELETE`** ***file_remoto***
      - **`CD`** **(per cambiare directory corrente)**
      - **`MKDIR / RMDIR`** **(crea / elimina directory)**
      - **`LS / DIR`**
- ad ogni comando inviato dal client FTP, il server risponde con appositi codici di risposta
- Sicurezza e FTP
  - **Nelle versioni iniziali FTP prevedeva il trasferimento in chiaro delle password**
  - **Con `RFC 2228` sono stati introdotti nuovi comandi per aumentare la sicurezza**
    - **`AUTH` (il client specifica quale meccanismo intende usare per il trasferimento protetto delle informazioni)**

FTP

- **PROT** , livello di protezione che verrà usato
  - ***Clear***
  - ***Safety*** (richiesta la verifica sull'integrità dei dati)
  - ***Confidential*** (trasmissioni cifrate)
  - ***Private*** (trasmissioni cifrate e verifica integrità)
- **MIC** , comando per il trasferimento dati con livello di sicurezza ***Safety***
- **CONF** , comando per il trasferimento dati con livello di sicurezza ***Confidential***
- **ENC** , comando per il trasferimento dati con livello di sicurezza ***Private***

- Es. psftp e winscp (Windows) , scp (Linux)

Sicurezza di telnet e FTP

- Presentano l'inconveniente che il traffico attraversa la rete in chiaro, pertanto si presta a violazioni di dati sensibili (login, password, dati sensibili in generale)
- Meglio utilizzare le versioni che utilizzano ssh (Secure Shell) e scp (Secure Copy), che scambiano i dati in modo cifrato. Queste procedure generano un maggior carico computazionale sia sul server che sul client. Molti software che implementano ambienti client di questi servizi hanno la possibilità di usare la versione sicura
- I socket ssh e scp in genere sono lasciati aperti sui firewall

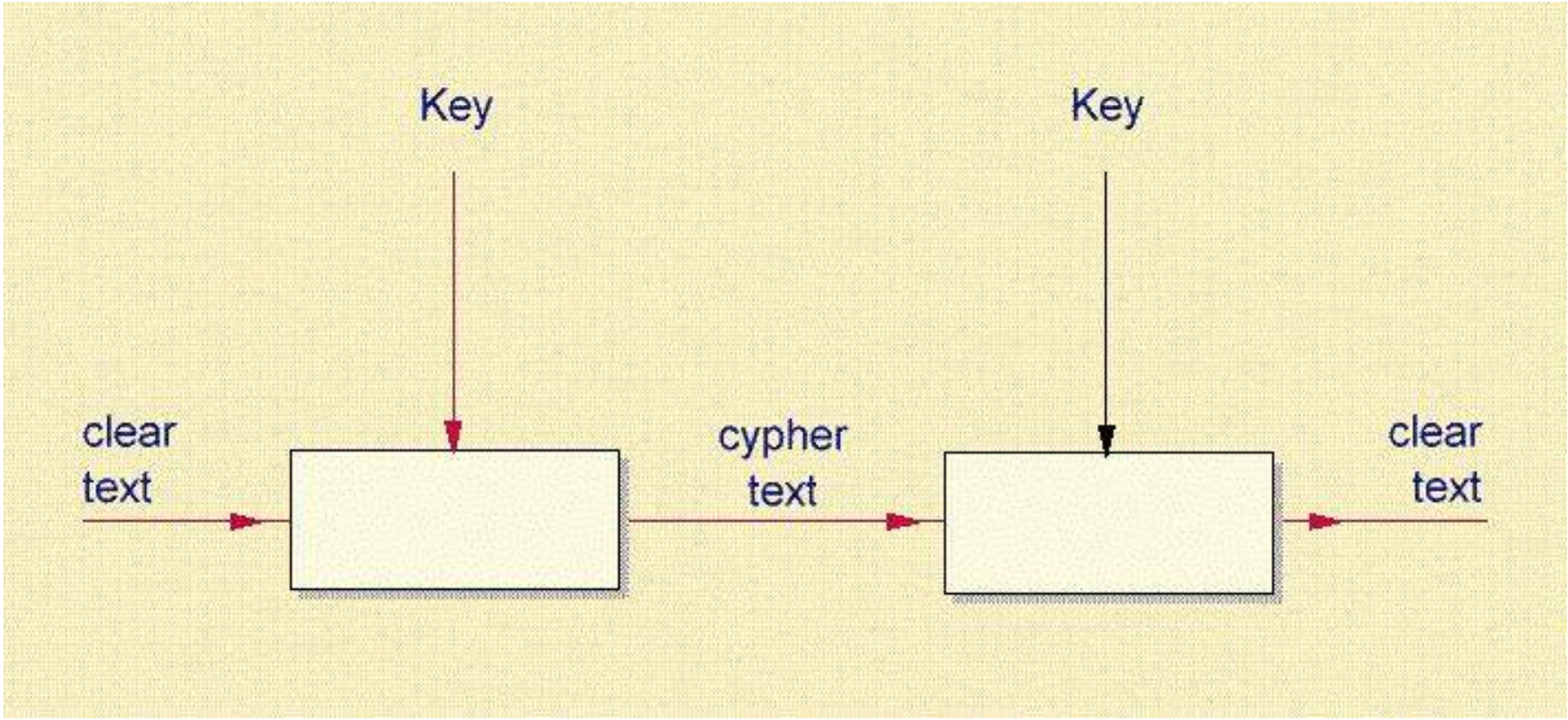
Trivial FTP (TFTP)

- Alternativo a FTP
- Copia file interi
- Minori funzionalità di FTP
- Il codice è più leggero
- Inteso per essere usato in Local Area Network
- Si esegue usando UDP
- Macchine Diskless lo utilizzano per ottenere l'immagine al bootstrap

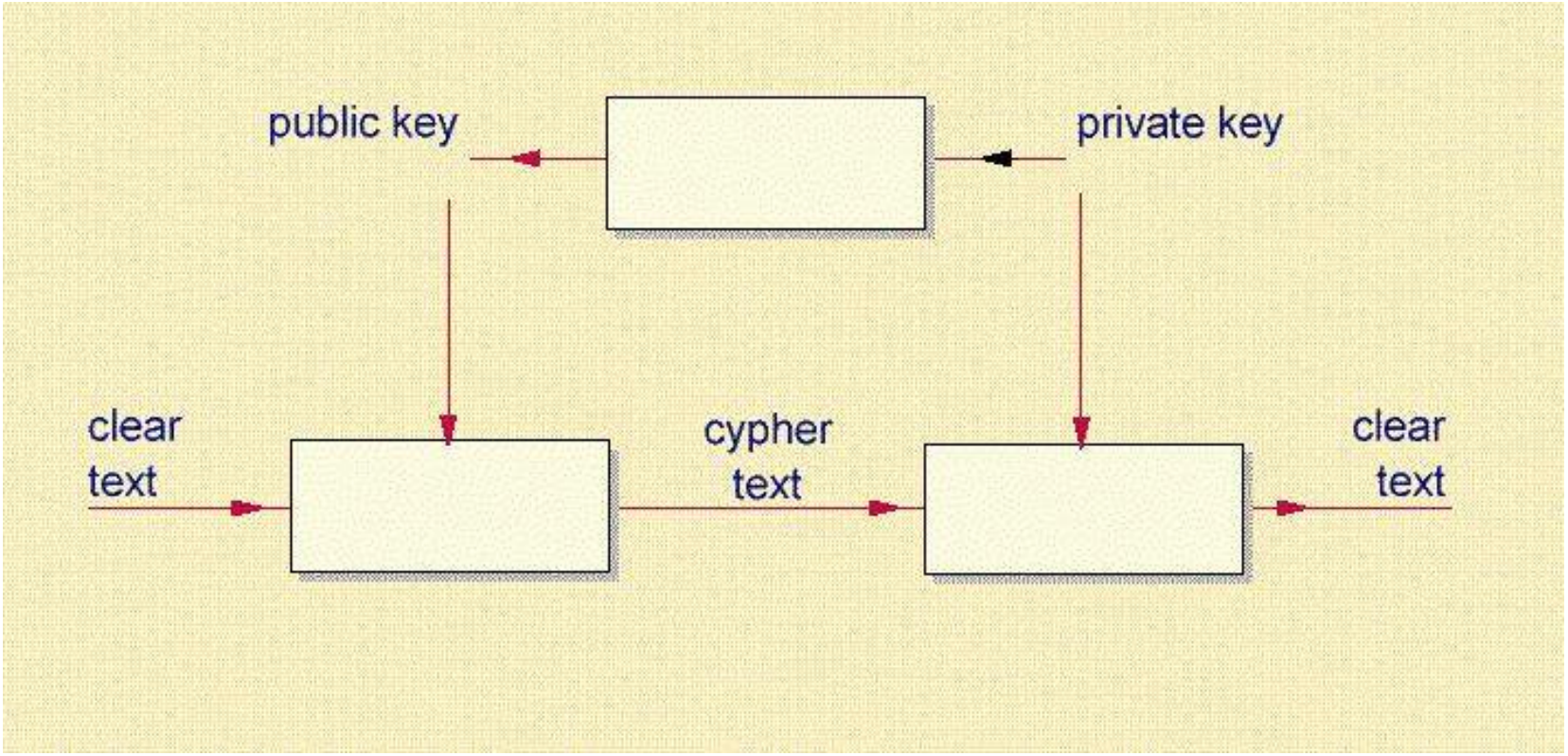
Encryption technology

- Crittografia Simmetrica o Private key encryption (Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish)
  - Stessa chiave per encryption e decryption
  - Entrambi i partner devono conoscere la chiave
- Crittografia Asimmetrica o Public key encryption (RSA)
  - Ciascuno ha una coppia di chiavi univoca
  - Le chiavi sono collegate nel crypt/decrypt
  - una chiave è resa **pubblica**, l'altra è tenuta segreta (**privata**)

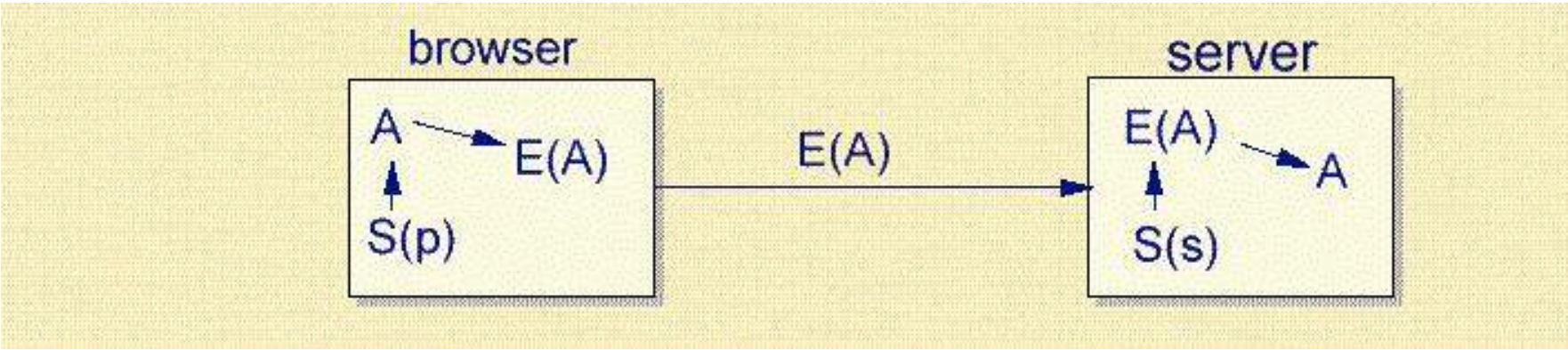
Shared key encryption



Public key encryption

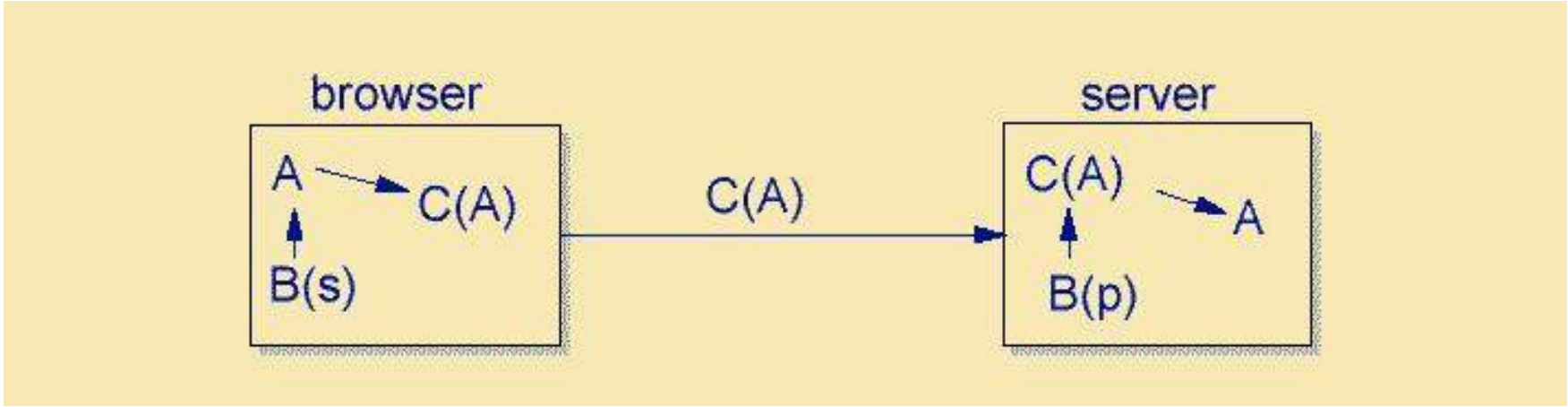


Public key encryption



- Confidentiality: Yes
- Authentication: Yes
- Non repudiation: No

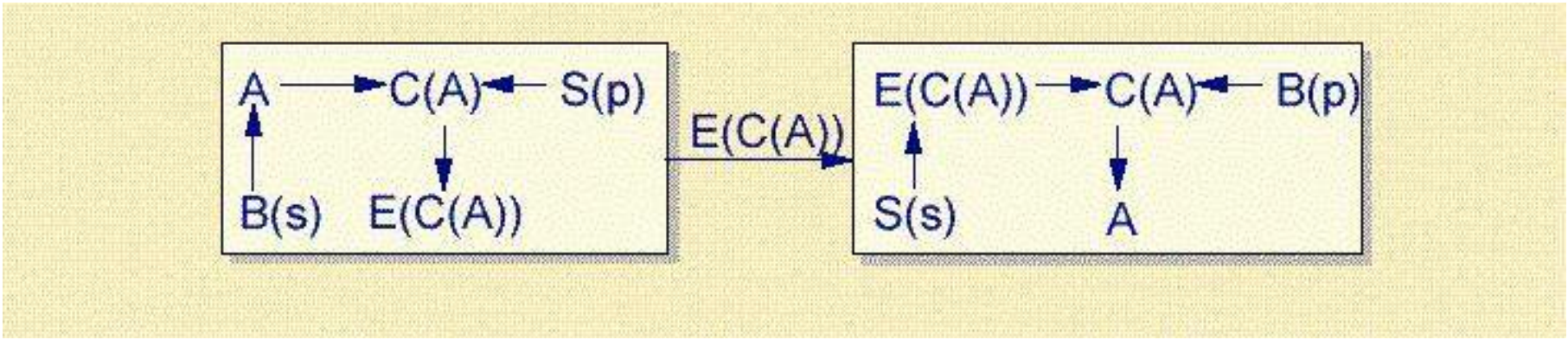
Public key encryption (digital signatures)



- Confidentiality: No
- Authentication: No
- Non repudiation: Yes

Public key encryption

(digital signatures and confidentiality)



- Confidentiality: Yes
- Authentication: Yes
- Non repudiation: Yes

www.openssh.com

- Supporta i protocolli SSH1 e SSH2.
- E’ un versione Free sviluppata nell’ambito del progetto OpenBSD (**http://www.openbsd.org**) ed è basata sulla libreria OpenSSL (**http://www.openssl.org**) per molte delle sue potenzialità crittografiche, la quale non è regolata dalla licenza Gnu Public License (GPL, che definisce un prodotto FreeSoftware)
- Il protocollo SSH è disponibile in due versioni, tra loro incompatibili: SSH1 e SSH2.

Generazione delle chiavi ssh

```
teststud@woodiep:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/teststud/.ssh/id_rsa):
Created directory '/home/teststud/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/teststud/.ssh/id_rsa.
Your public key has been saved in /home/teststud/.ssh/id_rsa.pub.
The key fingerprint is:
71:70:1e:9a:cc:ef:0f:2e:48:d3:1f:33:f4:37:6c:91 teststud@woodiep
The key's randomart image is:
+--[ RSA 2048]----+
|         . o     |
|       o * .     |
|        * o    . |
|         +.   E  |
|       .S... . . |
|      o ..+ . =  |
|     . o .o+ o . |
|      . ...o     |
|         .. .    |
+-----------------+
teststud@woodiep:~$
```

OpenSSH

- SSH versione 1 è presente in due varianti principali: la 1.3 e la 1.5, entrambe supportate da OpenSSH
- Queste versione utilizzano l'algoritmo di crittografia asimmetrica RSA (il cui patent è terminato e pertanto può essere utilizzato liberamente) per la negoziazione delle chiavi, poi gli algoritmi simmetrici 3DES, AES e Blowfish per crittografare i dati. Alcune implementazioni del protocollo SSH utilizzano l'algoritmo simmetrico IDEA, ma essendo questo coperto da patent in alcuni stati, OpenSSH non supporta IDEA.
- OpenSSH usa un semplice algoritmo Cyclic Redundancy Check (CRC) per verificare l'integrità dei dati.

OpenSSH

- La seconda implementazione del protocollo è SSH 2, introdotta a suo tempo per superare le limitazioni di patent di RSA e per risolvere alcuni problemi legati all'algoritmo CRC di SSH1.
- SSH 2 usa gli algoritmi asimmetrici Digital Signature Algorithm (DSA) e Diffie-Helmann (DH), che sono liberi da patent
- Al posto dell'algoritmo CRC in SSH2 si usa l'algoritmo Keyed-Hash Message Authentication Code (HMAC)
- Per molte funzioni SSH2 utilizza la libreria OpenSSL

Gestione delle chiavi

- SSH memorizza in file ascii le chiavi pubbliche e private nella directory $HOME/.ssh (permesso di accesso: 700)
- Nella stessa directory viene salvato anche il file known_hosts il quale contiene le chiavi pubbliche dei server ai quali ci si collega.
- Per gli host le cui chiavi pubbliche sono salvate nel file authorized_keys, al momento del login non viene chiesta password
- Alcuni software SSH consentono di gestire le chiavi pubblica e privata mediante un certificato X.509.

authorized_keys

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDY82oCuVqp0H68pebF9kjC9x5EdBg2XIMpjGl8U9mSH
F6WBmktYJED77zEVmAD7LlsPzrkMDzqxCB+Vly3h2Iq8+EDT92lQ8iILPvPKarRFCmglLmjS+8TEg
VlZ4J/ZCM4nV9tCIjvPj+s9lDcP4uYcxAfEovE93VwGJn/
lOGqGERfkTV3nBzfJWolZOWdWkM7fPPRK732scK6+OVoT8DXb2JJFv6f9Z/
L3N5RcaR61hGZWZ+MQEnsiokKA0Oiy1uRxL5OKGBKkksxfHBvxrLwkO56leGNYJEqc0yg8Bb0dF4
PaG3XCbdTSqZWBSyMOPh0TU9siEHYPFQSVU9J6K/v osvaldo@woodie-pc

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAvaR5Rg5vn3jIJ7Gtjb9swS6CbCyFUUtQR/nf+DHWTRaXFgP
CeUV3xMIZfU+oUdnchE8ZAGYA4+TwaWJxUVIxaXCl64/
DW8tsH1lut2VE5X690/8LOmNtEBrTdnE1RFRl0YvDKgs4DNY9HPuEbf4TchypqryqT5KO+yST57wK
bs6yqO/qulTi37Z1xCWSD5g/
qMOQHvj+AS0AbnxlgH2OAq1xMjn4qvTjwIwEldcAB6MJCDbeb61CrQUlbjQsWbePvPiACyIgZTI1Yj
u5CnG725nk8YFkJcCQiqc++U0fQSB552Fj5O4u71c7WnfmWa4Zz5OJeYPVgB7cu5TQAawgQQ==
osvaldo@di.uminho.pt

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCuWhh9W6z3X8pFu7hFdxU2MMlWDsIhbAS+gsWUU6
GtKzKBpIFXQRkaR8lF9s4BJJ8NYmVctdBDoMhrMU6GpolbD84fvm2Y22jKBf4KHNBAvidoaOY4LQ
qhFUySRvi7xtQW7UxXvKgtzhwLPMb5dl39xIdU9FxyX37B9ZOdyJ/
iMSBtcllZS+eFx96eERiCW21NDSAiPPsqMAcNm57stqrhIu3TRBprKflxay65z6oy8cg3lr7yhs9k/
luZxr2dFo/tMZtMBiYroidSHXbBZDvFZTwlZCV7+kfxevh1Hxt3408DN4ohVP9cnrXiFcuOFtpTz6y/
6c06l90JpupU01oR osvaldo@woodiep

known_hosts

labhpc.dipmat.unipg.it ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA4YF4rmru4YTtZljXKnCX4qg5DfISvpLh126sqk5biinsXCPUIF3
ERGngMKTAIUy2QyMSeL1pj1Bf+HkvhVy2ehLYR8JTDj8jewJ/fR0Gxl/sX/
tdo8fpSGsi03JJn1poCDcap/Jg/VT/1FpAJ85YdGYw6gH/lLYNGZOTt3hUAT0=

di.uminho.pt,193.136.19.139 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAuwXc9rUJYrzL0xbQYyEZBd7uL0sX1B8+nXet7Y3RG4CFrKb
BEdwLsNBPKOc0HRt0MuFVqxzDChH3U3Ek1z/b4KhTxUU1oU5/+
+3CFlNbrm0Tz9KxLGzgbORcUuzUQ2mutCFk2ifb+/qXMXyqN6/N/cYAV9IDT/
zpCT1YSb8LSBPw83lULiKan1Ap0ydjXGHp9nnOtPNsXbvc5YwzJv8xxepH6oE0qt89TGdOHpqJ5q
hQnqZ6+1lHH6tls2Uce9+ia56+RuAZEz2Xu7/apFSUKY3HcHY3xz2m8ADskmi/
iJlarpcH41rSa0LhFJ5gdsDDEzgDme2pqvxc8FzhRQXgLw==

141.250.243.2 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAxYgGg3gAb2gER4jNbG4KuTQTIpQKOKZ5mHPBRVnL/
HYH7Hm2T9/DH5FIGDdWLGQQWEKTBeDZrJ/2ARVOOsTrRg/
uZNHerswSLC58hGRKgzHiDgchFfszhqgJQgg4VPod2Y5kqSi5D5w91TPANHuK8FERcp0mQoj7+G
To1MvghNPuJm62tCndh3kzZyWryMUq8dIlCAvbCd/
iKN0VgCZaV6P7XqmljmXMLX0mX+TOD7f9MLajgiIqBS6JTNu833HTsmTCB+qYD2x68ABkYjWS/
Z7kZiMISWlecvlU7WkQCMaPfiFSxq3i/JQ2dh0M/nSUlQJASXucqY1wI/iA05x1PQ==

OpenSSH

- L'insieme di programmi di OpenSSH comprende:
  - **`ssh`** che sostituisce **`rlogin`** e **`telnet`**
  - **`scp`** che sostituisce **`rcp`**, usa il tunnel ssh
  - **`sftp`** che sostituisce **`ftp`**, usa il tunnel ssh
  - **`sshd`** daemon per server ssh
  - **`ssh-add ssh-agent ssh-keygen`** programmi di utilità per gestione chiavi
  - **`sftp-server`** daemon per server sftp

sshd

- Il programma sshd gira sul server per rispondere alle richieste **`ssh`** dei client.
- Tra le opzioni maggiormente significative che troviamo nel file di configurazione (**`/etc/ssh/sshd_config`**) abbiamo:
  - **`PermitRootLogin without-password`**
  - **`MaxAuthTries 3`**
  - **`AuthorizedKeysFile  .ssh/authorized_keys`**
  - **`PasswordAuthentication yes`**
  - **`X11Forwarding yes`**
  - **`Subsystem  sftp  /usr/libexec/openssh/sftp-server`**

Domain Name System
DNS

DNS

- Gli umani preferiscono i nomi agli indirizzi numerici
- Ci sono due possibilità:
  - Spazio dei nomi piatto
  - Spazio dei nomi gerarchico

- Se si sceglie la seconda possibilità, abbiamo di nuovo due possibili soluzioni:
  - Suddivisione in base alla topologia della rete
  - Suddivisione per organizzazione, pertanto indipendente dalle interconnessioni fisiche delle reti.
- Internet usa una suddivisione per organizzazione
  - E' uno schema universale di denominazione (lo usano tutti)
  - Ogni organizzazione definisce liberamente la struttura interna.

DNS

- Si usa un insieme di parole separate da un campo delimitatore, il punto. Es:

dmi.unipg.it

- Anche la stringa

unipg.it

è a sua volta un dominio

- Il top level domain è **.it**
- I top level domain (TLD) sono definiti da ICANN (in precedenza da IANA). Al seguente link è possibile visionare gli ultimi TLD proposti: **http://newgtlds.icann.org/en/announcements-and-media/video/applicants**

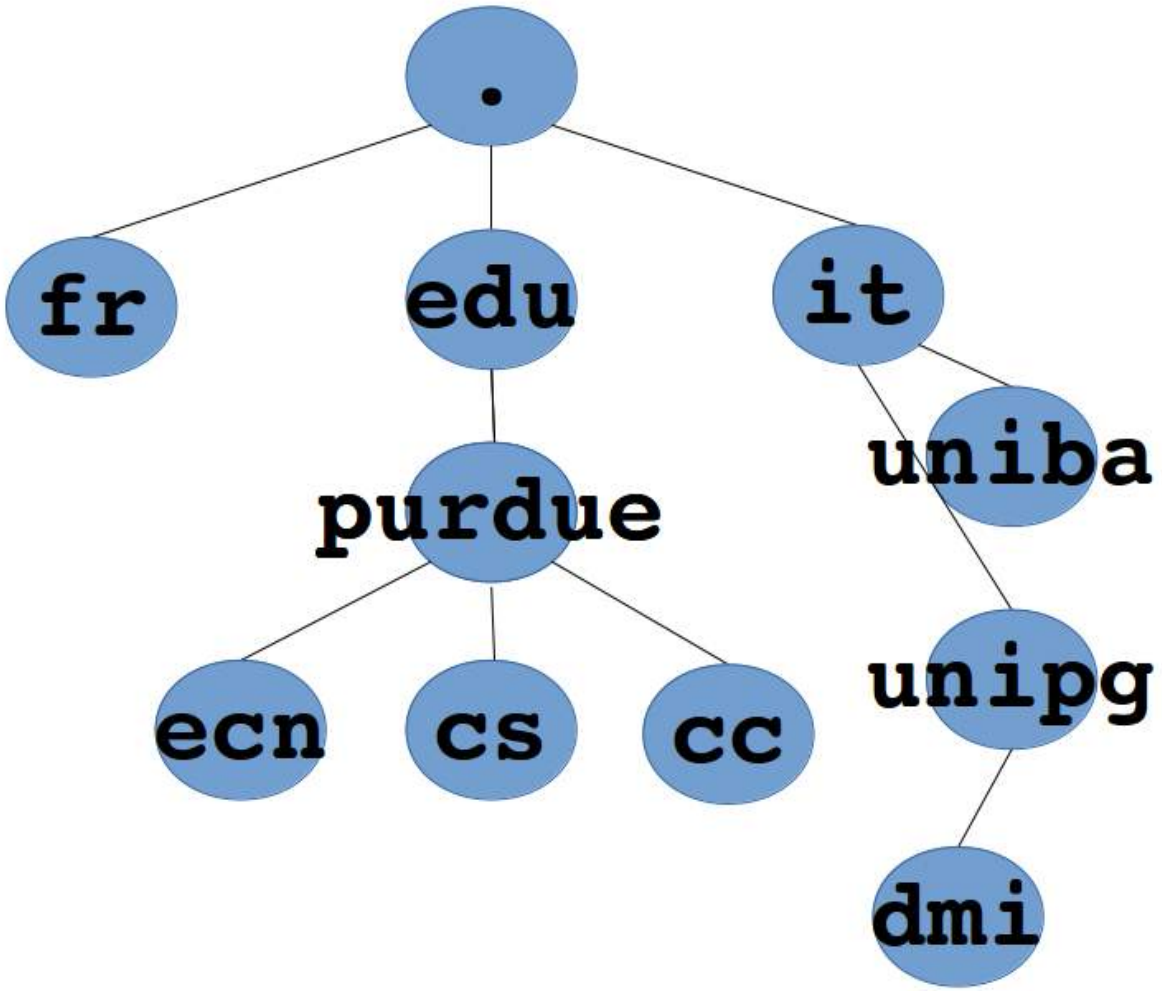
DNS

- L'RFC 2606 definisce alcuni domini riservati per evidente significato intrinseco:
  - **`.example`**
  - **`.invalid`**
  - **`.localhost`**
  - **`.test`**
- IANA ha suddiviso I TLD in tre categorie:
  - **ccTLD** country-code TLD, lista delle sigle dei paesi del mondo. Molti coincidono con I nomi specificati nello standard **ISO 3166-1**.
  - **gTLD**: generic TLD, usati da particolari organizzazioni (`.com`, `.mil`, `.edu`, `.gov`)
  - **Infrastrutturali** (l'unico è **`.arpa`** usato nella risoluzione inversa dei nomi)

DNS

- Si pensava (impropriamente) che senza l'aggiunta di nuovi nomi, il DNS sarebbe collassato.
- Ora il proliferare dei nomi sta creando grossi problemi legali.
- Diventa impossibile proteggere un brand in questo modo

TLDs



Autorità responsabili dei nomi

- L'Università di Perugia si registra presso un ente preposto (registrar) e diventa responsabile del nome `.unipg.it`
- Il Dipartimento di Matematica e Informatica chiede all'Università la registrazione di dominio `.dmi.unipg.it` e diventa responsabile per tale dominio. Ottiene così la delega amministativa e tecnica per tale nome a dominio
- I singoli soggetti che hanno bisogno di un nome a dominio, ad esempio per un server o una stazione di lavoro, contattano l'amministratore di rete del Dipartimento perché gli assegni un indirizzo IP ed un nome, e conseguentemente di gestire la registrazione del nuvo nome e indirizzo mediante il DNS

Database DNS

- Il database mantenuto dal DNS è costituito da:
  - Record
  - Nomi
  - Classi
- Un certo nome può essere associato a diverse classi (host, mail exchanger, server DNS, etc) del database DNS.
- Il client specifica il tipo di oggetto richiesto una volta che chiede di risolvere il nome, il server ritorna la descrizione della classe specificata per quel nome.

DNS

- Pertanto è possibile associare ad ogni interfaccia di rete (su reti di tipo TCP/IP, ad ogni IP address) un nome (hostname).
- Perché si fa questo? Perché i nomi sono più facili da ricordare e da scrivere correttamente rispetto agli indirizzi numerici.
  - Es: 141.250.1.7 oppure teseo.unipg.it

DNS

- Quasi sempre gli indirizzi numerici e i nomi sono intercambiabili, ma in tutti i casi prima di effettuare una connessione il sistema converte l'hostname in un IP address.
- L'amministratore di rete è responsabile dell'assegnazione dei nomi e degli indirizzi e della loro memorizzazione.
- La traduzione di nomi in indirizzi deve essere nota a tutti gli host della rete

DNS

Risoluzione nome-indirizzoIP statica

- l'associazione (mapping) tra indirizzo IP e hostname viene stabilito una volta per tutte tramite una **host table**
- **host table** è memorizzata un semplice file ASCII **/etc/hosts**, ad esempio:

Indirizzo IP	Hostname	Alias
192.168.130.1	moe.unipg.it	moe
192.168.132.2	larry.unipg.it	Larry
192.168.130.40	omniw.unipg.it	omniw
192.168.132.20	pserver.unipg.it	pserver
192.168.132.45	powerbook.unipg.it	powerbook

DNS

Risoluzione nome-indirizzoIP dinamica

- l’associazione (mapping) tra indirizzo IP e hostname viene stabilito dinamicamente
- ogni host all'avvio richiede a server DNS le informazioni sui nomi da assegnare alle proprie interfacce
- attraverso appositi file di configurazione ogni host sa quali server interrogare e i server quali nomi assegnare

DNS

- In ambiente UNIX esiste una implementazione dei protocolli del Domain Name System (DNS): il Berkeley Internet Name Domain (BIND)
- **BIND** è un package di software comprendente:
  - i principali componenti del DNS, tra cui:
    - ✓ un server DNS (named);
    - ✓ una libreria di risoluzione di DNS (resolver);
  - strumenti per la verifica del corretto funzionamento del server DNS (**`dig`** o **`nslookup`**);
- La release corrente sono la BIND 9.13.x e la BIND 9.12.x (9.13.1: Bind 9, Major release 13 (dev) o 12 (stable), Minor release 1). Minor release originano da: Security Releases o Roll-up Bugfixes Releases

DNS

- Il **resolver** (BIND client) è una libreria di funzioni che permette di generare e inviare al server le richieste di informazioni sui nomi dei domini;
- Il **named** (BIND server) è un processo demone in grado di servire le richieste del resolver, il quale deve essere in esecuzione sull'host locale;
- La configurazione del BIND (sia lato client che server) avviene tramite specifici file di testo che ne descrivono il tipo di servizio fornito.

DNS

- **Configurazione del resolver** (BIND client)
  - le funzioni del resolver sono configurate nel file **`/etc/resolv.conf`**
  - contiene una serie di istruzioni per l'esecuzione delle richieste.
  - viene letto all'avvio del processo che usa il resolver
- Le voci da inserire nel file sono:
  - **`nameserver`** ***`address`***

    le richieste vengono inviate all'indirizzo IP ***`address`*** specificato. Si possono specificare più **`nameserver`** fino ad un max di 3 (valore dipendente dal sistema): se il primo non risponde entro un tempo prestabilito, la richiesta viene passata al secondo e così via.

DNS

- **`domain`** ***`name`***

definisce il nome di dominio di default. Il resolver aggiunge ***`name`*** a qualsiasi nome host che non contiene il carattere punto.

Esempio: se il dominio è definito come **`dipmat.unipg.it`** per accedere un servizio dell'host cartesio.dipmat.unipg.it basta specificare il nome cartesio . Il resolver chiede di ottenere l'indirizzo IP di cartesio.*dipmat.unipg.it*. In caso di fallimento richiede l'IP di cartesio.*unipg.it* e così a salire nella gerarchia.

- **`search`** ***`domain1, domain2, … domain`***

ha la stessa funzione di **`domain`** con la possibilità di avere più domini da provare ad aggiungere al nome dell'host. La differenza con **`domain`** è che viene aggiunto solo l'intero nome dei domini indicati.

DNS

Se si usa DHCP questa tabella viene riscritta ogni volta che ci si collega via DHCP

- Esempio del file di configurazione del resolver

```
# cat /etc/resolv.conf
search dmi.unipg.it unipg.it
nameserver      141.250.1.7
nameserver      141.250.1.6
```

- Verifica del corretto funzionamento

```
# host teseo
teseo.unipg.it is 141.250.1.7
```

DNS

- Rispetto al resolver più file sono utilizzati per la **configurazione di named**:
  - **named.conf**
    contiene i parametri generali di configurazione del **named** ed i puntatori ai file contententi le informazioni dei domini gestiti dal server (zone files)
  - **named.ca**
    puntatori ai root domains server
  - **named.local**
    reverse per l'indirizzo loopback
  - **named.hosts**
    zone file per la risoluzione diretta
  - **named.rev**
    zone file per la risoluzione inversa

NB: i nomi utilizzati sono del tutto generici ed arbitrari

DNS

- **BIND** può essere configurato in 3 diversi modi:
  - ***caching-only***
    il processo è in esecuzione ma non esiste nessun nameserver database file. Ogni richiesta (dal resolver) viene rediretta su altri server ed il risultato memorizzato in una cache locale per servire future richieste (necessari solo **`named.conf`** e **`named.ca`**)
  - ***primary***
    è il gestore (authoritative server) di informazioni riguardanti specifici domini. Legge le informazioni da appositi file (configurati dall'amministratore) detti **zone files**.
  - ***secondary***
    Scarica gli zone file dal primary server e li memorizza localmente in appositi file detti **zone file transfer**: copia completa di tutte le informazioni sui domini.

DNS

named.conf (1/4)

- Consente a **named** di puntare ai file contenenti le informazioni sui domini, sia locali che remoti.

- Ci sono appositi comandi per configurare questo file (**directory**, **primary**, **secondary**, **cache**, …)

DNS

named.conf (2/4)

- caching-only -

Vengono omessi i comandi di configurazione del primary e del secondary server ad eccezione per il dominio di loopback

```
primary       0.0.127.IN-ADDR.ARPA                /etc/named.local

cache         .                                   /etc/named.ca
```

Indica a **named** che il server locale è primary server per il proprio dominio di loopback e che le relative informazioni sono contenute in **/etc/named.local**

Indica a **named** di memorizzare in una cache locale le risposte ottenute dai nameserver (a cui redirige le richieste dai resolver) e di inizializzare la cache con la lista dei root server contenuta nel file /etc/named.ca

DNS
named.conf (3/4)
- primary server -

Supponendo che il dominio sia `unipg.it` e che il primary server sia `moe`:

```
directory                               /etc

primary         unipg.it                named.hosts

primary         250.141.IN-ADDR.ARPA    named.rev

primary         0.0.127.IN-ADDR.ARPA    named.local

cache           .                       named.ca
```

Dichiara che il server locale è il primary server per `unipg.it` e il relativo zone file è `named.hosts`

Puntatore al file `named.rev` in cui c'è l'associazione tra gli indirizzi IP, nel `192.168.0.0`, con i relativi `hostnames`

Indica inoltre che il server locale è il primary server per il reverse domain `250.141.IN-ADDR.ARPA`, con le informazioni relative nel file `named.rev`

DNS
named.conf (4/4)
- secondary server -

Supponendo che il dominio sia `unipg.it` e che il primary server sia `moe`:

```
directory                                                    /etc

secondary      unipg.it                    141.250.1.1       unipg.it.hosts

secondary      250.141.IN-ADDR.ARPA        141.250.1.1       250.141.rev

primary        0.0.127.IN-ADDR.ARPA                          named.local

cache          .                                             named.ca
```

Dichiara che il server locale deve scaricare le info. sul dominio `unipg.it` dal server con indirizzo IP `141.250.1.1` e memorizzarle nel file `/etc/unipg.it.hosts`

Indica inoltre che il server locale è il secondary server per il reverse domain `250.141.IN-ADDR.ARPA`, e che i relativi dati vanno scaricati dal server con IP `141.250.1.1` e memorizzati nel file `/etc/250.141.rev`

named.ca

```
                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
; formerly NS1.ISI.EDU
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     128.9.0.107
; formerly C.PSI.NET
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
; formerly TERP.UMD.EDU
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
; formerly NS.NASA.GOV
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
; formerly NS.ISC.ORG
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
; formerly NS.NIC.DDN.MIL
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
; formerly AOS.ARL.ARMY.MIL
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
; formerly NIC.NORDU.NET
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
; temporarily housed at NSI (InterNIC)
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     198.41.0.10
; housed in LINX, operated by RIPE NCC
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
; temporarily housed at ISI (IANA)
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     198.32.64.12
; housed in Japan, operated by WIDE
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
; End of File
```

puntatori ai root domains server

DNS
named.local

- **E' lo *zone file* per la traduzione del reverse domain `0.0.127.IN-ADDR.ARPA`.**
- **Scopo: permette la conversione dell'indirizzo IP `127.0.0.1` (detto loopback address) nell'hostname `localhost`.**

In sede di analisi del file di configurazione, al carattere @ verrà sostituito il nome del dominio corrispondente a questo file, definito in `named.conf`

```
$TTL    86400
@       IN      SOA     localhost. root.localhost.  (
                        2014030101      ; Serial
                             10800      ; Refresh after 3 hours
                              3600      ; Retry after 1 hour
                            604800      ; Expire after 1 week
                             86400 )    ; Minimum TTL of 1 day
        IN      NS      localhost.
1       IN      PTR     localhost.
```

Definisce il nameserver con autorità sul dominio

Utimo numero dell'indirizzo `127.0.0.1` ; i primi 3 numeri sono desunti dalla definizione `0.0.127.IN-ADDR.ARPA`

Hostname associato all'indirizzo `127.0.0.1`

DNS

named.hosts

- E' lo *zone file* per la conversione diretta
- Scopo: permette la conversione di hostname in indirizzi IP.
- Contiene la maggior parte delle informazioni sui domini.

```
@ IN SOA moe.unipg.it. root.moe.unipg.it. (
                                2014030101 ; Serial
                                10800      ; Refresh
                                3600       ; Retry
                                604800     ; Expire
                                86400 )    ; Minimum

                IN NS           moe.unipg.it.
 plant          IN NS           pack.plant.unipg.it.

  @             IN MX 10        moe.unipg.it.
  @             IN MX 20        larry.unipg.it.
localhost       IN A            127.0.0.1

moe.unipg.it.   IN A            141.250.1.1
larry.unipg.it. IN A            141.250.1.2
omniw.unipg.it. IN A            141.250.1.40

www             IN CNAME        moe.unipg.it.

ns133.unipg.it. IN A            141.250.5.51
```

Name servers

Mail server

Name to IP mapping

Alias

Interface specific name

DNS

named.rev

- **E' lo *zone file* per la traduzione dei reverse domain inseriti nel `named.conf`.**
- **Scopo: permette la conversione di indirizzi IP in hostname.**

```
@ IN SOA moe.unipg.it. root.moe.unipg.it. (
                              2014030101 ; Serial
                              10800      ; Refresh
                              3600       ; Retry
                              604800     ; Expire
                              86400 )    ; Minimum
```

```
250.141.in-addr.arpa.    IN NS   moe.unipg.it.

250.141.in-addr.arpa.    IN NS   larry.unipg.it.
```

→ **Name server**

```
1.1.250.141.in-addr.arpa. IN PTR moe.unipg.it.

2.1.250.141.in-addr.arpa. IN PTR larry.unipg.it
```

→ **Addresses point to canonical names**

DNS
zone files (1/2)

Semplici file ASCII che contengono records del database DNS. Hanno un formato fisso ed uno stesso metodo per definire i record di un dominio. I principali componenti di un zone file sono detti **standard resource record (RR)**: **SOA**, **NS**, **A** (**AAAA** per IPv6), **PTR**, **MX**, **CNAME**.

Il formato di un resource record (RR) del DNS è:

[name] [ttl] IN *type data*

name , nome di uno specifico host op di un dominio a cui Il RR si riferisce; generalmente si utilizza il carattere @ per riferirlo al dominio che viene definito dallo zone file stesso.

DNS
zone files (2/2)

`ttl` , (**`time-to-live`**) definisce il tempo massimo (in secondi) oltre cui l'informazione nel RR non può essere considerata valida in una cache di un sistema remoto

`IN` , indica che il record successivo è un Internet DNS RR

`type` , identifica il tipo del RR (SOA, NS, A, AAAA, PTR, MX, CNAME)

`data` , informazione specifica del tipo RR

DNS

SOA (1/3)

SOA (Start Of Authority): segna l'inizio di un zone file e generalmente è anche il primo record ad essere utilizzato. Esiste un solo SOA associato ad ogni zone file

Formato:

```
[name] [ttl] IN SOA origin contact (
                    serial
                    refresh
                    retry
                    expire
                    minimum
                )
```

origin, indica il primary master server per questo dominio;

contact, email address dell'amministratore del dominio. A differenza di un indirizzo email non compare il carattere @, che viene sostituito dal punto. Se `postmaster@unipg.it` è l'amministratore del dominio apparirà `postmaster.unipg.it`

DNS

SOA (2/3)

serial, indica la versione dello zone file. E' conveniente esprimerlo nella forma yyymmddnn. E' estremamente importante in quanto permette ai secondary server di stabilire se lo zone file in loro possesso è stato modificato: confrontando questo campo con quello nello zone file nel primary server.

refresh, esprime il tempo che deve aspettare il secondary server prima di controllare il SOA sul primary server. Generalmente un giorno (86400 secondi)

DNS

SOA (3/3)

retry, indica il tempo che dovrà aspettare il secondary server prima di effettuare una nuova richiesta se la prima fallisce. Generalmente un'ora (3600 secondi).

expire, indica il tempo dopo il quale il secondary server dovrà riprendere lo zone file. Generalmente 604800 secondi pari a 7 giorni.

minimun, è il valore di default del Time To Live (TTL) per tutti i record del dominio dove non è espresso.

DNS

NS

NS (Name Server): identifica il nome del server che ha l'autorità per il dominio.

Formato: **[domain] [ttl] IN NS *server***

Estensioni: permette di indicare i server autorizzati a rispondere per il sottodominio

es. dominio **unipg.it**, sottodominio **plant.unipg.it** (in **named.hosts**)

```
plant  432000  IN  NS pack.plant.unipg.it
```

DNS

A

A (Address record): utilizzato per associare un hostname ad un indirizzo IP

Formato: **[hostname] [ttl] IN A *address***

hostname, nome che si vuol assegnare all'indirizzo IP *address*

address, l'indirizzo IP corrispondente

Estensioni: uso di @ come ***name*** per indicare il dominio corrente

DNS

AAAA

AAA (Address record): utilizzato per associare un hostname ad un indirizzo **IPv6**

Formato: **[hostname] [ttl] IN AAAA *address***

hostname, nome che si vuol assegnare all'indirizzo IP *address*

address, l'indirizzo IP corrispondente

Estensioni: uso di @ come ***name*** per indicare il dominio corrente

Con BIND:

```
$ORIGIN 6net.garr.it
www in aaaa 3ffe:b00:c18:1:290:27ff:fe17:fc1d
```

DNS

MX

MX (Mail eXchanger): definisce il server che gestisce la posta per un singolo host o un intero dominio; tutta la posta viene rediretta sul server specificato

Formato: **[name] [ttl] IN MX *preference host***

name, di host o dominio a cui le email verrando indirizzate

preference, permette di stabilire un ordine di preferenza se sono presenti più mail server; Più è basso, maggiore sarà la priorità. I valori partono da 0 e sono multipli di 5.

host, nome del mail server

Estensioni: uso di @ come ***name*** per indicare il dominio corrente

DNS

CNAME

CNAME (Canonical NAME): definisce un alias per il nome di un host

Formato: **nickname [ttl] IN CNAME *host***

DNS

PTR

PTR (domain name PoinTR): permette di associare indirizzi IP ad un nome di host.

Formato: **[name] [ttl] IN PTR *host***

name, numero che identifica n-esimo indirizzo IP nella rete

host, nome completo dell'host

IPv6 PTR record (ip6.arpa):

```
$ORIGIN 1.0.0.0.8.1.c.0.0.0.b.0.e.f.f.3.ip6.arpa
d.1.c.f.7.1.e.f.f.f.7.2.0.9.2.0 in ptr www.6net.garr.it
```

DNS

named (1/3)

Comando utilizzato per avviare il servizio DNS.

Sintassi:

```
named [-c configfile
       -d level
       -p port
       -n ncpus
       -t directory
       -u user
      ]
```

-c configfile : utilizzato per specificare la posizione del file **named.conf** se diversa da **/etc/named.conf**

-d level : utilizzato per attivare il debug (maggiore *level*, maggiore il dettaglio) salvando le informazioni nel file ***$dir*/named.run**

DNS

named (2/3)

`-p port` : per default il servizio risponde alla porta 53 (TCP/UDP), con questa opzione si può specificare una porta diversa.

`-n ncpus` : il kernel istanzia *ncpus* thread per sfruttare i sistemi multiprocessore

`-t directory` : il processo esegue un cambio di directory appena letto il file di configurazione.

`-u user` : il processo named viene eseguito dall'utente specificato, invece che da root

DNS
named (3/3)

Script per la gestione di named: /etc/rc.d/inetd.d/named

```
/etc/rc.d/init.d/functions
    case "$1" in
      start)
            # Start daemons.
            echo -n "Starting BIND Name Server Daemon: "
            daemon /usr/local/sbin/named
            echo
            ;;
      stop)
            # Stop daemons.
            echo -n "Shutting Down BIND Name Server Daemon: "
            killproc named
            echo
            ;;
      *)
            echo "Usage: $0 {start|stop}"
            exit 1
    esac
    exit 0
```

Per attivare il programma del DNS si deve dare il comando:

/etc/rc.d/init.d/named start

Esempio di `named.conf`

```
acl unipg { 141.250.0.0/16; 127.0.0.1/8;  };
options {
        listen-on port 53 { 127.0.0.1; 141.250.5.116; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        allow-recursion { unipg; };
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
        version "Ignota";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
```

DNS
dig

Tool di debugging che consente di interrogare direttamente un nameserver per ottentere informazioni e verificarne la configurazione.

Sintassi: **dig @server *hostname***

dig @teseo.unipg.it posta.unipg.it

```
; <<>> DiG 9.9.4-P2-RedHat-9.9.4-12.P2.fc20 <<>> @teseo.unipg.it posta.unipg.it
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49317
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;posta.unipg.it.                 IN      A
;; ANSWER SECTION:

posta.unipg.it.                 86400   IN      CNAME   zimbrauniv-prod-8.cineca.it.
zimbrauniv-prod-8.cineca.it. 202 IN     A       130.186.28.197
;; AUTHORITY SECTION:
cineca.it.              76925   IN      NS      dns.cineca.net.
cineca.it.              76925   IN      NS      dns.cineca.com.
;; ADDITIONAL SECTION:
dns.cineca.com.         35504   IN      A       130.186.84.216
dns.cineca.net.         2502    IN      A       130.186.1.1

;; Query time: 1 msec
;; SERVER: 141.250.1.7#53(141.250.1.7)
;; WHEN: Mon Nov 24 20:55:28 CET 2014
;; MSG SIZE  rcvd: 186
```

Network Information Service (NIS)

NIS

- E’ un servizio che permette di definire delle risorse (di amministrazione) comuni ad un insieme di host (grandi comunità di utenti), in modo tale che l’utente possa "spostarsi" da un host all’altro mantenendo le stesse caratteristiche fondamentali: login, password, home directory, autorizzazioni possedute.
- realizza un database di amministrazione che permette un controllo centralizzato e la condivisione automatica di risorse.
- Fondamentale anche per applicazioni parallele e distribuite e per la creazione di cluster di computer, poiché consente di usare una notazione semplificata per l’accesso a file e risorse, a prescindere dal singolo nodo di elaborazione.

NIS

- Converte i principali file UNIX (file ASCII) in un formato database (detto **NIS map**) che può essere interrogato per rendere le informazioni disponibili attraverso la rete
- Il vantaggio nell'uso di NIS è quello di avere un **controllo centralizzato** degli **administrative files** in un singolo server contattabile da ogni altro host in rete.
- L'utilizzo di NIS è completamente trasparente per l'utente finale

NIS

- I database creati dai file ASCII sono chiamati **NIS map** e vengono creati dai seguenti file di sistema:
  - **/etc/passwd** definisce login, password, shell e home directory => ***passwd.byname*** e ***passwd.byaddr***
  - **/etc/group**, definisce i gruppi di utenti, elencando i nomi di login di ogni gruppo => ***group.byname*** e ***group.byaddr***
  - **/etc/netgroup** definisce le autorizzazioni da assegnare ad host ed utenti per l'accesso alle risorse locali (influenza i permessi dichiarati in hosts.equiv, NFS, .rhosts) => ***netgroup.byname*** e ***netgroup.byaddr***
  - **/etc/auto.home** definisce la posizione assoluta delle home directory associate agli utenti => ***passwd.byname*** e ***passwd.byaddr***
  - **/etc/ethers** informazioni usate da RARP per la conversione da ethernet address a IP address => ***ethers.byaddr*** e ***ethers.byname***

NIS

- **/etc/hosts**, ascii file che associa un indirizzo IP ad un nome => ***hosts.byname e hosts.byaddr***
- **/etc/networks**, ascii file per mappare i network address in network name => ***networks.byname*** *e* ***network.byaddr***
- **/etc/netmasks**, utilizzato per definire la subnet mask. E' una tabella con 1 sola riga contentente indirizzo della rete e netmask relativa => ***netmasks.byaddr***
- **/etc/protocols**, una tabella contenente il nome del protocollo, il numero ed il nome => ***protocols.byname*** *e* ***rotocols.byaddr***
- **/etc/services**, contenente l'elenco dei servizi e relativa porta utilizzata con specificato il protocollo => ***services.byname***
- **/etc/aliases**, contiene gli alias agli indirizzi e-mail => ***mail.byname e mail.byaddr***

NIS

- Le **NIS map** vengono memorizzate nel **master server** che le rende disponibili ai client tramite il processo **`ypserv`**.
- I client possono aggiornare le loro informazioni ricevendo i database tramite il demone **`ypbind`**.
- Sia il NIS server che i clients fanno parte del **NIS domain** il cui nome può essere verificato o stabilito con il comando:

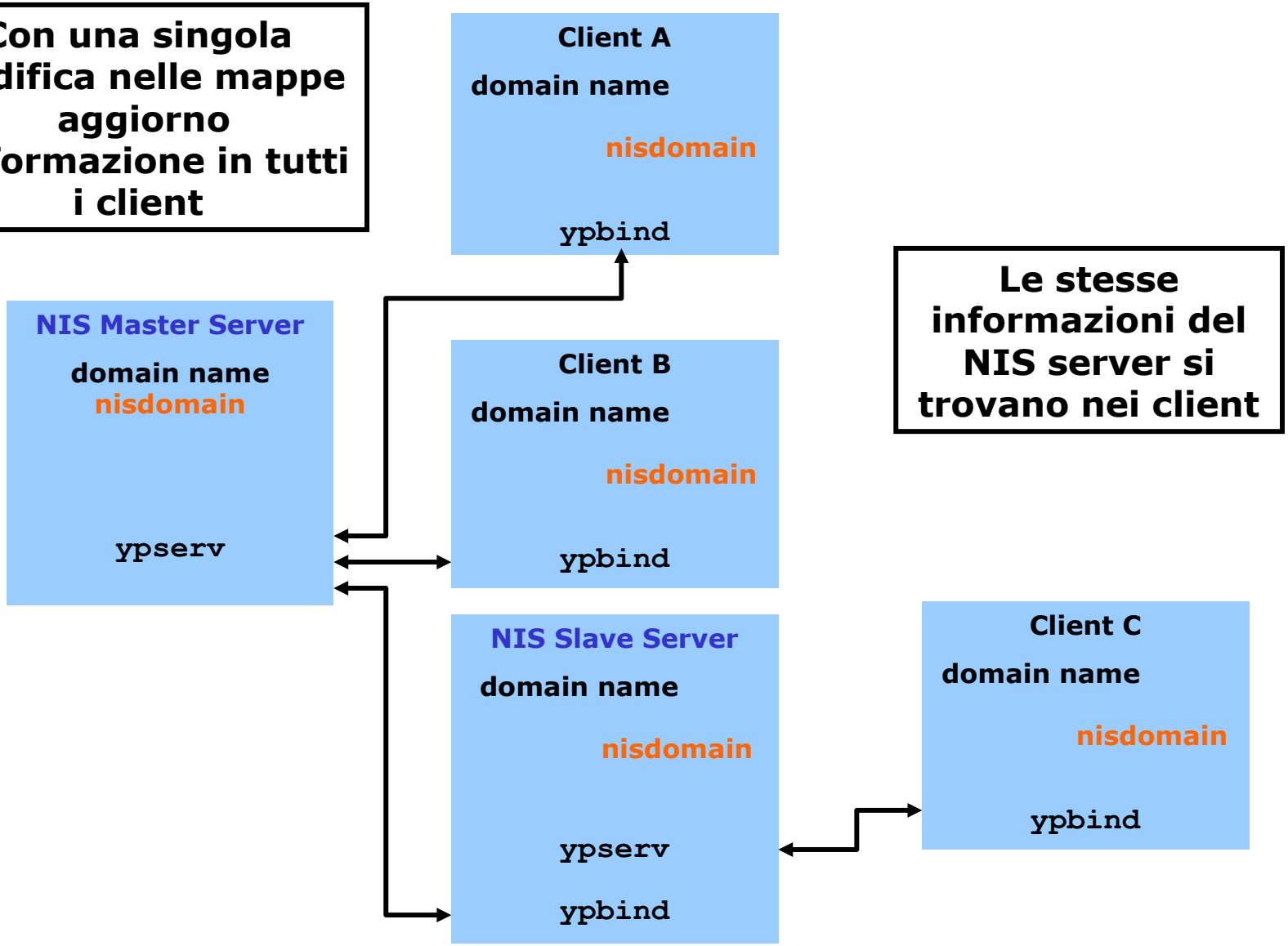
  # **`domainname`** ***`domain`***
- Per visualizzare l'indirizzo del server da cui sono prese le mappe si utilizza :

  # **`ypwhich`**
- Nei client, per ciascuna tabella che si vuol utilizzare dal server occorre inserire i caratteri:

  +::::::

NIS

Con una singola modifica nelle mappe aggiorno l'informazione in tutti i client



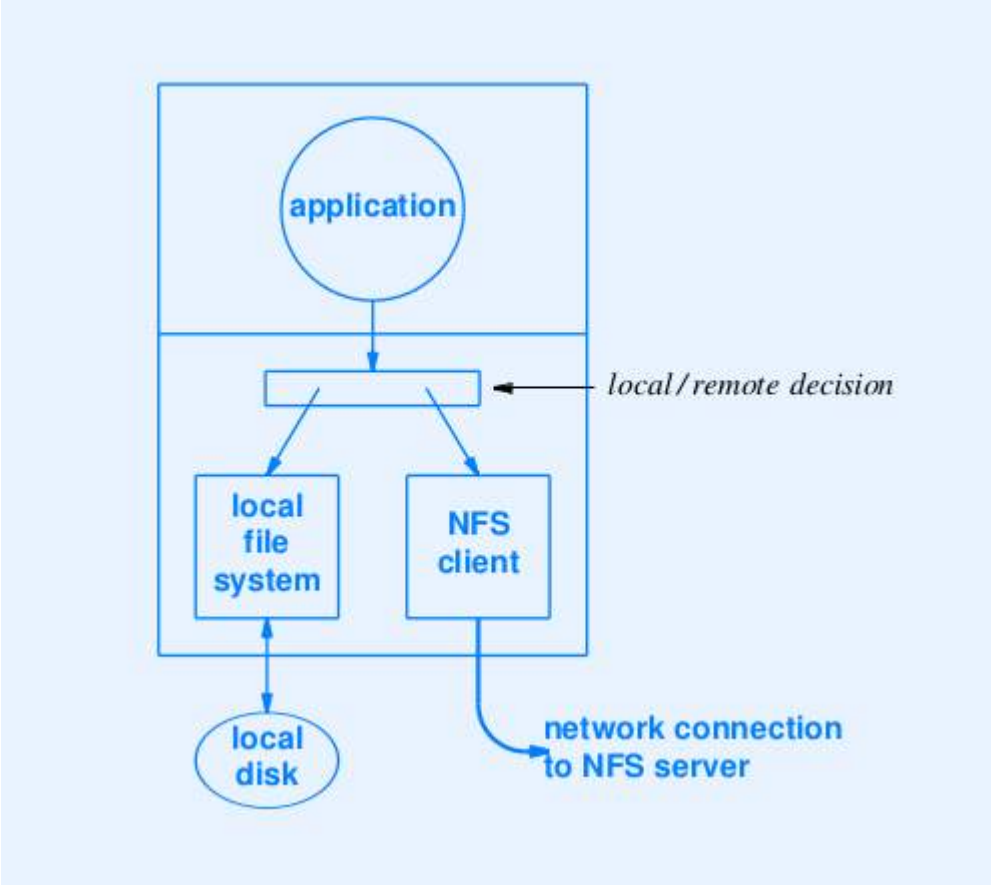
Le stesse informazioni del NIS server si trovano nei client

NIS

- Generalmente le informazioni NIS sono memorizzate nella directory **`/var/yp`** e vanno ridistribuite ogni volta che viene effettuata una modifica al Master Server (la rigenerazione delle mappe NIS viene effettuata mediante l'utility **`makefile`**).
- Servizi condivisi attraverso NIS:
  - Autenticazione (login, passwd)
  - Home directory
  - Accesso a stampanti, via **`lpr`**
  - NFS
  - Risorse di rete

Network File System (NFS)

Implementazione di NFS



NFS

- Il **Network File System** (**NFS**) permette di condividere su una rete directory e file.
- Con NFS utenti e programmi possono accedere file memorizzati su sistemi remoti come se fossero file locali.
- I vantaggi di NFS sono:
  - riduzione spazio disco locale (una singola copia per directory)
  - semplificazione dei task di supporto (aggiornamento centralizzato dei file, ma accessibili da tutta la rete)
  - manipolazione dei file remoti con comandi UNIX locali (es. **`cp`**)

NFS

- Esistono due componenti fondamentali di NFS
  - il client utilizza le directory remote come se fossero parte del filesystem locale;
  - il server mette a disposizione le proprie directory per l'uso da parte dei client
- Lato client, l’inserimento di una directory di un host remoto nel filesystem locale è detto mounting e viene realizzato mediante il comando

  ```
  # mount
  ```

- Lato server, la condivisione di una directory locale ad host specifici per l'accesso remoto è detta sharing (il file system locale diventerà parte del filesystem remoto) e viene realizzata mediante il comando

  ```
  # export
  ```

NFS

Programmi NFS:

- **nfsd** ***[nservers]*** demone che gestisce le richieste NFS
  nservers indica il numero di processi da eseguire; è presente solo nel server.
- **biod** ***[nservers]*** demone che gestisce I/O dal lato client
- **rpc.lockd** gestisce i lock file (server - client)
- **rpc.statd** controlla lo stato della rete (server - client)
- **rpc.mountd** esegue le richieste di mount del client (server)

NFS

Esempio di script per avvio NFS:

```
if [ -f /usr/sbin/biod -a -f /usr/sbin/rpc.statd -a -f
   /usr/sbin/rpc.lockd ]; then
   biod 8;              echo -n   'biod'
   rpc.statd &          echo -n 'statd'
   rpc.lockd &          echo -n 'lockd'
Fi
```

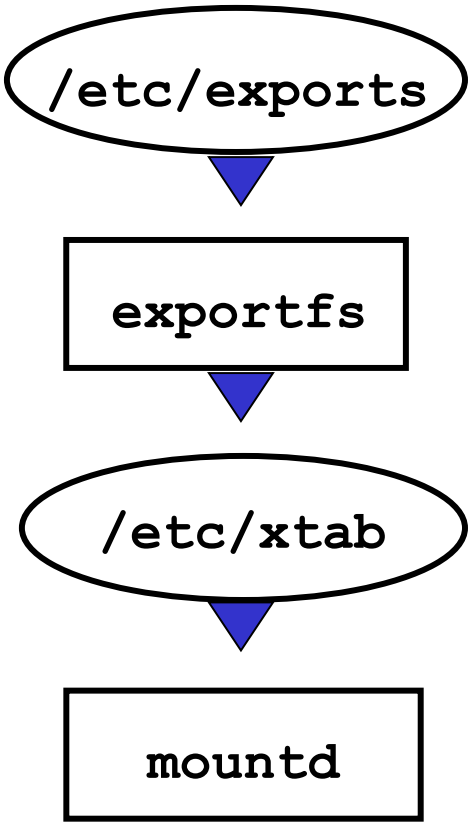
Client

```
if [ -f  /etc/export ]; then
   > /etc/xtab
   exportfs -a
   nfsd 8 &     echo -n   'nfsd'
   rpc.mound
fi
```

Server

NFS

Export filesystems



Definisce le directory da esportare e le condizioni

Rende le directory disponibili per il **`mount`** e aggiorna il file **`/etc/xtab`**

Contiene le informazioni delle directory esportate

Esamina le richieste di mount dei clients leggendo **`/etc/xtab`**

NFS

Exporting filesystems

- sul server NFS (**nfsserver**) configurare: **/etc/exports**, un file ASCII che contiene le directory da esportare e l'elenco degli host che hanno accesso a questi file. Esempio:

```
/usr/public
 /usr/man -rw=mailhost:dnsserver
 /usr/local -ro
 /u1 - access=netgrp1,root=mailhost:dnsserver,rw
  /home/research -access= mailhost:dnsserver:netgrp2
```

NFS

Il formato è : **directory *[-option][,option]*…**

directory : nome della directory o file che si vuol esportare

-ro : read-only non permette di poter modificare le directory exportate

-rw *[=hostname][:hostname]*… : permette la lettura e scrittura delle directory. Se presente hostname restringe questa possibilità all'elenco specificato

***-access=hostname[:hostname]*…** : limita l'accesso ai soli host nell'elenco. Si può anche utilizzare con un netgroup

NFS
Mounting Remote Filesystems via NFS

`showmount -e` ***`[hostname]`*** : per visualizzare l'export list dell'host specificato

`mount` ***`hostname`*****`:`*****`remote-directory local-directory`** :

`hostname` identifica l'NFS server a cui si richiede la remote directory e che sarà disponibile nel sistema nella local directory

Esempio:

```
mkdir /home/ricerca
mount nfsserver:/home/ricerca /home/ricerca
umount /home/ricerca
umount nfsserver:/home/ricerca
```

- Per effettuare il mount nfs automatico ad ogni reboot del client NFS occorre aggiungere un record al file **`/etc/fstab`** del tipo :

```
nfsserver:/home/research /home/research nfs rw 0 0
```

NFS
RPC e XDR

Gli sviluppatori hanno scelto di implentare NFS creando tre parti indipendenti. Oltre ad NFS hanno creato i due sottosistemi *Remote Procedure Call* (RPC) e *eXternal Data Representation* (XDR) per consentire l'uso degli ultimi due anche ad altri protocolli e da parte di programmi applicativi.

Usando NFS i programmi accedono ai file remoti con le stesse procedure che utilizzano per accedere ai file locali, grazie all'uso di RPC e XDR.

Ad esempio un programmatore può suddividere un'applicazione in una parte client ed una parte server, che utilizzano RPC per comunicare.

NFS
RPC

Programmando sul lato client delle procedure remote, viene incorporato il codice RPC in fase di compilazione, mentre sul lato server implementa le funzioni volute e incorpora le funzioni RPC per dichiararle parte del server. Quando il programma client esegue una delle procedure remote, RPC riunisce gli argomenti, forma il messaggio lo invia al server remoto, aspetta una risposta e memorizza i valori restituiti negli argomenti opportuni.

Il protocollo RPC nasconde tutti i dettagli dei protocolli, consentendo anche ai programmatori che non conoscono i protocolli di comunicazione sottostanti di scrivere programmi distribuiti.

NFS

XDR

XDR consente ai programmatori di scambiare dati tra macchine con architettura eterogenea, senza preoccuparsi della conversione tra le diverse rappresentazioni dei dati a livello hardware.

XDR fornisce una rappresentazione dei dati indipendente dalla macchina.

Ai lati del canale di comunicazione i programmi usano le procedure XDR per convertire i dati dalla rappresentazione hardware locale ad una indipendente dall'architettura del computer.

Una volta che i dati sono stati ricevuti, questi vengono convertii dalla rappresentazione XDR indipendente a quella locale.

Simple Network Management Protocol (SNMP)

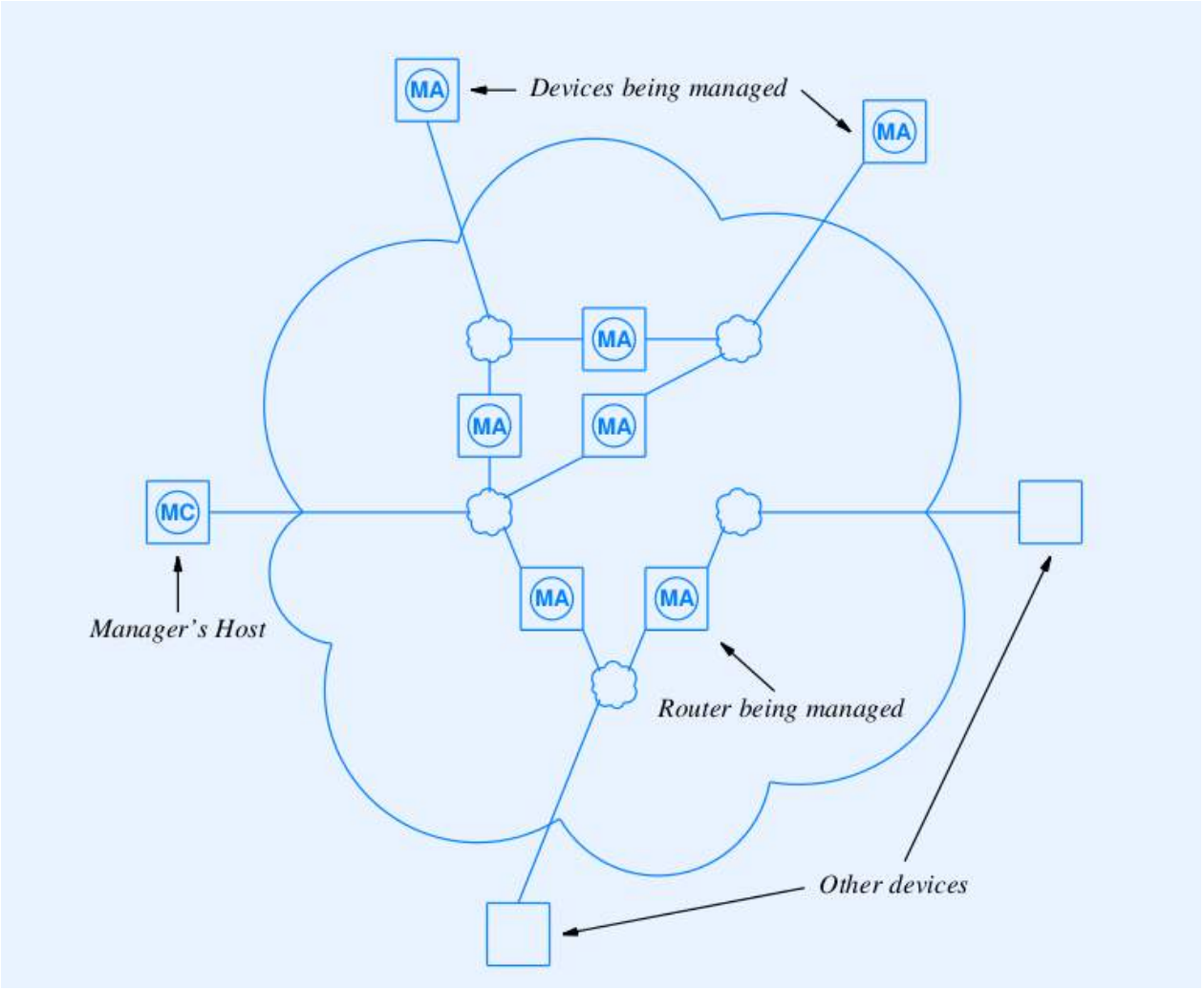
SNMP

- Il problema della gestione delle reti riveste una importanza enorme, in continuo sviluppo, data la crescente importanza che le reti e i servizi hanno sia per le aziende che per i singoli e le istituzioni.
- In molti contesti oggi avere la rete ferma coincide con il blocco parziale o totale delle attività.
- **Simple Network Management Protocol (SNMP)** è oggi il più potente e diffuso protocollo di gestione di reti, sistemi e applicazioni.
- Usando SNMP gli amministratori di sistema possono indirizzare richieste e comandi ai nodi della rete, monitorando lo stato delle risorse e delle applicazioni.

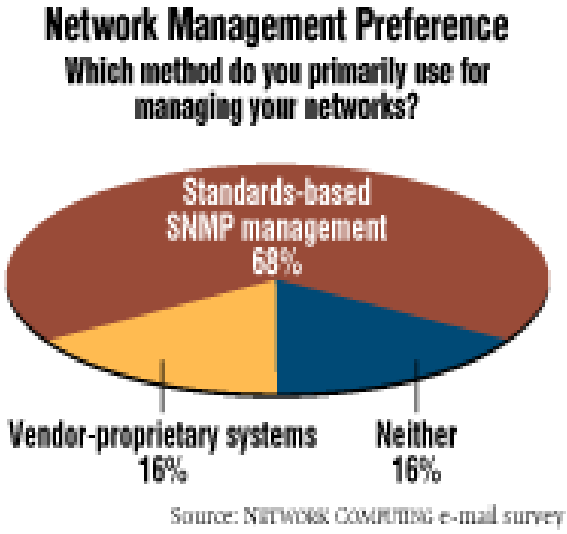
SNMP

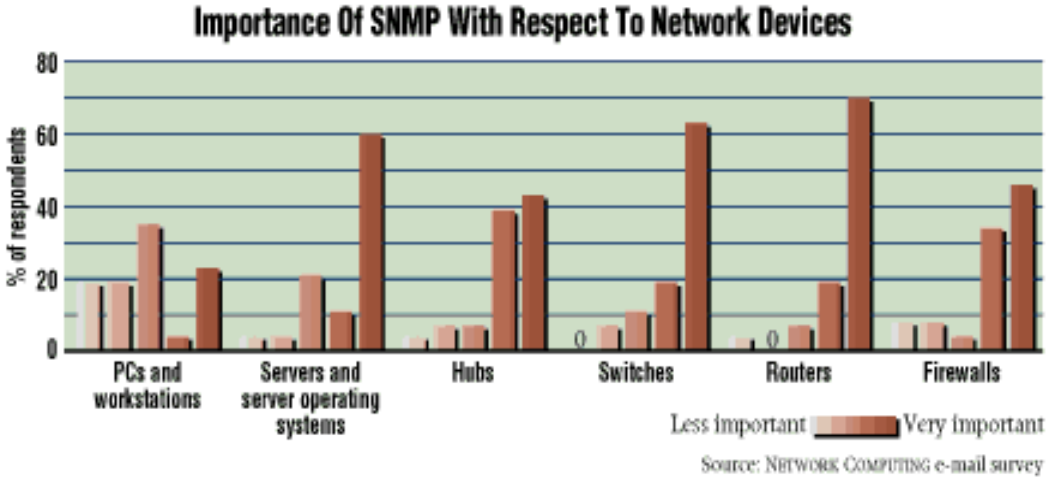
- In una rete Internet, un host con funzioni di manager controlla lo stato dei router e degli altri dispositivi di rete
- Il protocollo SNMP gira a livello applicazione e comunica con i dispositivi usando i servizi di trasporto del TCP/IP, in modo da poter controllare qualsiasi dispositivo connesso in Internet, invece che limitare il controllo ai dispositivi di rete locale.

SNMP


MA
Devices being managed
MA
MA
MA
MA
MC
Manager's Host
MA
MA
Router being managed
Other devices

SNMP


Network Management Preference
Which method do you primarily use for managing your networks?
Standards-based SNMP management 68%
Vendor-proprietary systems 16%
Neither 16%
Source: NETWORK COMPUTING e-mail survey


Importance Of SNMP With Respect To Network Devices
% of respondents
80
60
40
20
0
PCs and workstations
Servers and server operating systems
Hubs
Switches
Routers
Firewalls
Less important
Very important
Source: NETWORK COMPUTING e-mail survey

SNMP

- L’architettura di SNMP si compone di:
  - ***Nodi gestiti*** *o* ***Agent***: qualsiasi dispositivo in grado di collezionare dati SNMP e di rispondere alle richieste del *Manager (host, stampante, router, switch, hub, etc)*
  - ***Stazione di gestione*** *o* ***Manager***: un programma che interroga e invia comandi agli agent, che consente la gestione intelligenti degli eventi
  - ***Informazioni di gestione*** *o* ***Management Information Base (MIB)***: un archivio di informazioni di gestione immesse dagli agent, detti oggetti.
  - ***Protocollo di gestione (SNMP)***: definisce le modalità di interazione tra il Manager e gli Agent
  - ***Struttura dell'informazione di gestione (SMI)***: definisce la struttura delle informazioni da gestire.

SNMP

- SNMP si è evoluto in tre principali versioni:
  - SNMPv1 (RFC 1157)
  - SNMPv2p (RFC 1441, RFC 1445, RFC 1446, RFC 1448, RFC 1449)
  - SNMPv2 (RFC 1901, RFC 1902, RFC 1903, RFC 1904 , RFC 1905, RFC 1906, RFC 1907, RFC 1908, RFC 1909, RFC 1910)
  - SNMPv3 (RFC 2026, RFC 2200)
- La grossa limitazione mostrata fino alla versione SNMPv2 riguarda la sicurezza (credenziali in chiaro).
- SNMPv3 è la versione più recente, che corregge queste limitazioni

Riferimenti

- IETF : archivio degli RFC riguardanti SNMP:

http://datatracker.ietf.org/doc/search/name=snmpv3&activedrafts=on&rfcs=on

- Simple Times, la rivista che si propone la diffusione di SNMP

  http://www.simple-times.org/

- Numero speciale di Simple Times su SNMPv3:

  http://www.simple-times.org/pub/simple-times/issues/5-1.html

- Homepage di SNMP Technology Inc.:

  http://www.snmp.com/snmpv3/

- Altre risorse:

  http://www.ibr.cs.tu-bs.de/projects/snmpv3/

  http://www.net-snmp.org/wiki/index.php/Tutorials

SNMP v3

- **Authentication**: per proteggere contro modifiche delle informazioni, il mascheramento e la modifica della sequenza dei messaggi;
- **Privacy**: per garantire la riservatezza delle informazioni;
- **Nuovi strumenti di controllo**, inclusi strumenti grafici per la definizione delle regole di accesso
- **Configurazione remota** di sistemi gestibili, mediante un insieme di operazioni sicure

MIB

- Ogni oggetto mantiene una serie di variabili SNMP che descrivono il suo stato
- La collezione di tutti i possibili oggetti in una rete è chiamata Management Information Base, MIB
- Il Manager comunica con gli Agent mediante il protocollo SNMP che gli consente di conoscere lo stato delle variabili MIB e di modificarle se opportuno
- A volte capitano eventi imprevisti: si genera un SNMP trap
- La stazione (manager) può chiedere informazioni sullo stato delle variabili mediante messaggi. Se si verificano trap i messaggi si intensificano: questo modo di operare è denominato polling orientato ai trap.

Structure of Management Information (SMI)

- E' l'insieme delle regole che definiscono il nome delle variabili MIB
- Include definizioni di base come:
  - Indirizzo (valori costituiti da 4 byte)
  - Contatore (intero da 0 a 2^{32} -1)
- Specificato con l'Abstract Syntax Notation 1 (ASN.1)
- ASN.1 è uno standard ISO
- Specifica:
  - La sintassi dei nomi (in formato leggibile all'utente)
  - La codifica binaria (nel formato usato nei messaggi)
- Lo spazio dei nomi è assoluto e gerarchico

ASN.1

- Il nucleo dell'SNMP è costituito dagli oggetti gestiti dagli agenti che vengono letti e scritti dal Manager
- E' fondamentale uno standard per la definizione degli oggetti SNMP e per il modo di codificare e trasferire queste informazioni in rete.
- SNMP per questa funzione usa un sottoinsieme delle regole definite nell'Abstract Syntax Notation 1 (ASN.1) del protocollo ISO/OSI.
- I tipi permessi in SNMP dell'ASN.1 sono: **`INTEGER`**, **`BIT STRING`**, **`OCTET STRING`**, **`NULL`**, **`OBJECT IDENTIFIER`**

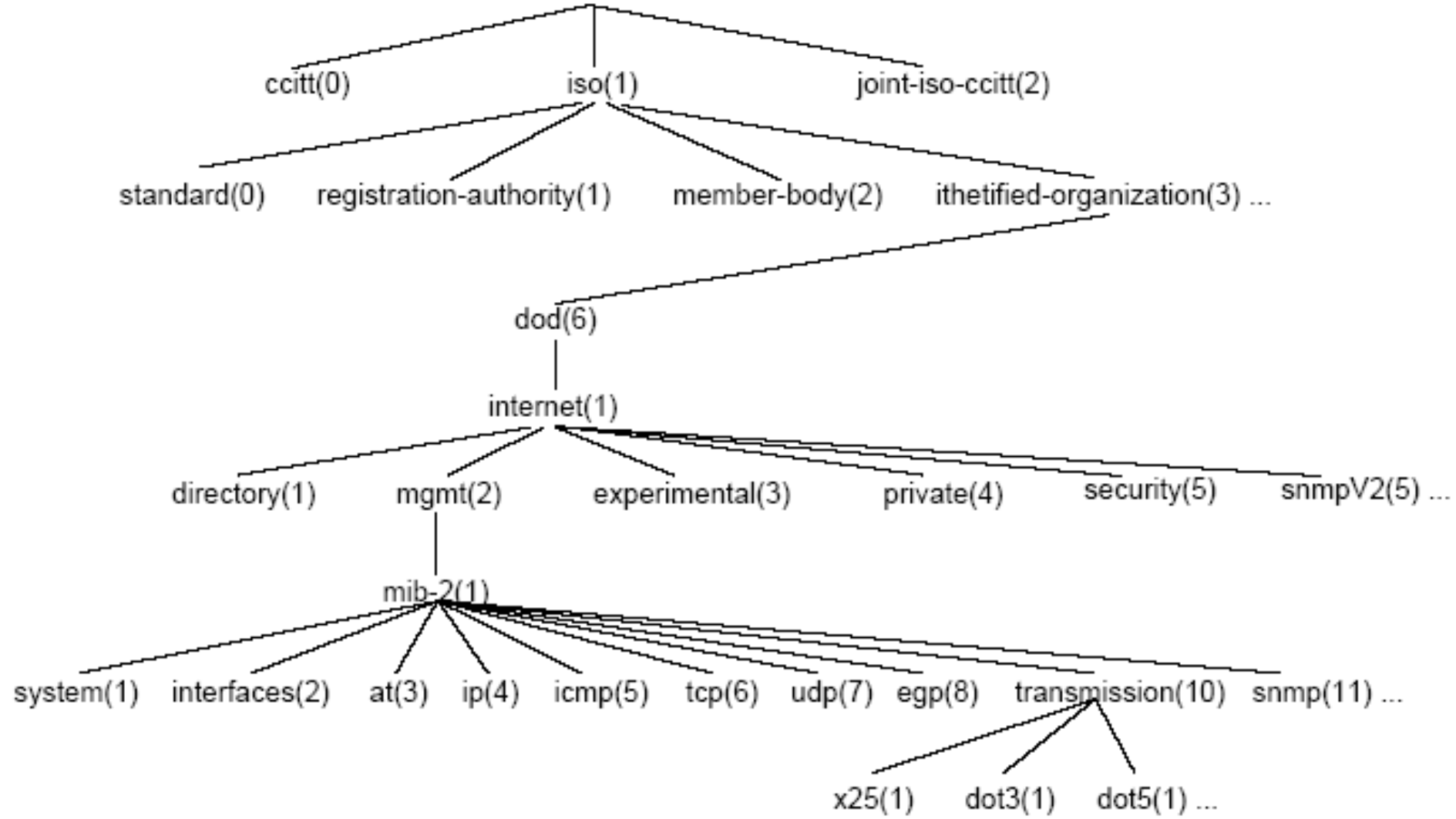
Object IDentifier

- **Object IDentifier** contiene i criteri per definire un oggetto. Si segue una struttura ad albero di standard e si pone qualsiasi oggetto o standard in una regione precisa dell'albero.
- La porzione usata da SNMP ha come radici gli organismi di standardizzazione ISO e CCITT (ora ITU) dalla radice si dipartono degli archi che definiscono sotto-organizzazioni, le quali hanno associato sia una etichetta che un numero.
- Tutti gli oggetti MIB SNMP vengono identificati da un'etichetta (cammino sull'albero) del tipo:

  {iso (1) identified-organization (3) dod (6) internet (1) mgmt (2) mib-2 (1) …}

  o, alternativamente: { 1 3 6 1 2 1 …}

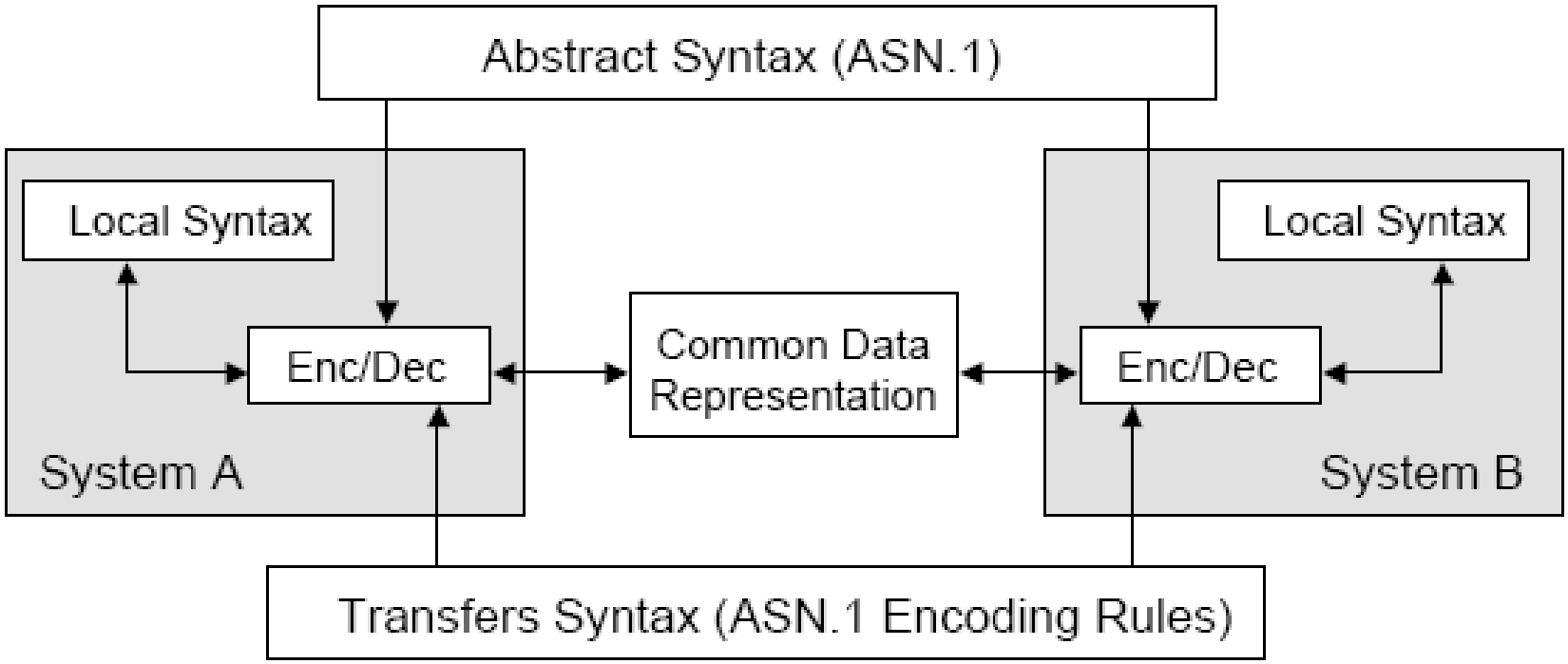
SMI


ccitt(0)
iso(1)
joint-iso-ccitt(2)
standard(0)
registration-authority(1)
member-body(2)
ithetified-organization(3) ...
dod(6)
internet(1)
directory(1)
mgmt(2)
experimental(3)
private(4)
security(5)
snmpV2(5) ...
mib-2(1)
system(1)
interfaces(2)
at(3)
ip(4)
icmp(5)
tcp(6)
udp(7)
egp(8)
transmission(10)
snmp(11) ...
x25(1)
dot3(1)
dot5(1) ...

Basic Encoding Rules

- ASN.1 definisce il modo univoco in cui i valori dei tipi ASN.1 sono convertiti senza ambiguità in una sequenza di bytes, che viene detta Basic Encoding Rules (BER).
- La codifica è ricorsiva, così che la codifica di un oggetto composto risulta dalla concatenazione delle codifiche degli oggetti componenti.
- Ciascun valore trasmesso deve essere costituito dai campi:
  - Identificatore (tipo o estensione)
  - Lunghezza del campo dati in bytes
  - Campo dati
- A seguito dell'adozione dell'ASN.1 per SNMP sono state definite 4 macro e 8 tipi di dati che sono usatissimi in SNMP, descritti da Structure of Management Informations (SMI)

ASN.1


Abstract Syntax (ASN.1)
Local Syntax
Enc/Dec
Common Data Representation
Enc/Dec
Local Syntax
System A
System B
Transfers Syntax (ASN.1 Encoding Rules)

MIB

- La collezione degli oggetti gestita da SNMP viene definita nel MIB.
- Gli oggetti che appartengono a MIB sono raggruppati in 12 categorie che corrispondono a 12 nodi al di sotto del nodo mib-2 della struttura ad albero descritta prima.
- Esse servono per definire le categorie di base per ciò che deve essere compreso dal Manager.
- In futuro verranno aggiunte altre categorie e oggetti
- I produttori di hardware di rete potranno definire oggetti aggiuntivi per i loro prodotti

Categorie MIB

MIB category	Includes Information About
system	The host or router operating system
interfaces	Individual network interfaces
at	Address translation (e.g., ARP mappings)
ip	Internet Protocol software
icmp	Internet Control Message Protocol software
tcp	Transmission Control Protocol software
udp	User Datagram Protocol software
ospf	Open Shortest Path First software
bgp	Border Gateway Protocol software
rmon	Remote network monitoring
rip-2	Routing Information Protocol software
dns	Domain Name System software

Variabili MIB

MIB Variable	Category	Meaning
sysUpTime	system	Time since last reboot
ifNumber	interfaces	Number of network interfaces
ifMtu	interfaces	MTU for a particular interface
ipDefaultTTL	ip	Value IP uses in time-to-live field
ipInReceives	ip	Number of datagrams received
ipForwDatagrams	ip	Number of datagrams forwarded
ipOutNoRoutes	ip	Number of routing failures
ipReasmOKs	ip	Number of datagrams reassembled
ipFragOKs	ip	Number of datagrams fragmented
ipRoutingTable	ip	IP Routing table
icmpInEchos	icmp	Number of ICMP Echo Requests received
tcpRtoMin	tcp	Minimum retransmission time TCP allows
tcpMaxConn	tcp	Maximum TCP connections allowed
tcpInSegs	tcp	Number of segments TCP has received
udpInDatagrams	udp	Number of UDP datagrams received

Forma Sintattica MIB

- Le variabili sono scritte come sequenze di numeri, con il punto come delimitatore.
- Nei messaggi viene usata la codifica numerica
- Ad es. Il prefisso per il nodo di gestione è

1.3.6.1.2.1

- Tutti i comandi di gestione sono codificati come operazioni di lettura o scrittura di variabili. Ad es. per effettuare il reboot di un dispositivo si scrive `0` nella variabile che corrisponde al tempo che manca fino al reboot...
- MIB è un insieme di variabili e la semantica per effettuare operazioni di lettura e scrittura su di esse.

Esempio di variabile MIB

- Il prefisso per la variabile *ipInReceives* è:

  iso.org.dod.internet.mgmt.mib.ip.ipInReceives

- *Il suo valore numerico è:*

  1.3.6.1.2.1.4.3

MIB

Group	#obj	Description
sistema	7	nome, locazione e descrizione del sistema
interfacce	23	interfacce di rete e misura del traffico
AT	3	traduzione di indirizzo
IP	42	statistiche di pacchetti IP
ICM	26	statistiche Sui messaggi ICMP ricevuti
TCP	19	algoritmi, parametri e statistiche TCP
UDP	6	statistiche di traffico UDP
EGP	20	statistiche sui protocolli di routing Exterior Gateway Protocol
SNMP	29	statistiche sul traffico SNMP

MIB

- Il gruppo sistema consente di capire il tipo di dispositivo chiamato, chi lo ha chiamato, hardware e software che contiene, persona da contattare. Se un'azienda appalta la gestione, i gestori sapranno chi contattare in caso di guasti o malfunzionamenti
- Il gruppo interfacce contiene i Network Interface Controller (NIC, le schede di rete) che tengono traccia dei pacchetti e byte inviati e ricevuti, il numero di quelli rifiutati, il numero di broadcast e la dimensione della coda di uscita
- Il gruppo AT teneva traccia delle conversioni indirizzo Ethernet – indirizzo Internet, ora è vuoto, in quanto questi oggetti sono stati spostati negli specifici protocolli in SNMPv2

MIB

- Il gruppo *IP* si occupa del traffico a livello Rete, dell'Internet Protocol (IP), dal nodo e al nodo. E' ricco di contatori che tengono traccia dei pacchetti persi per diversi motivi. Tiene traccia del riassemblaggio e della frammentazione dei pacchetti IP
- Il gruppo *ICMP* riguarda i messaggi di errore IP, perché l'Internet Control Message Protocol (ICMP) è un protocollo di gestione dell'IP. Aggiorna contatori per i vari tipi di messaggio ICMP, registrandone il numero.
- Il gruppo *TCP* riguarda il traffico a livello Trasporto, del Trasmission Control Protocol. Aggiorna contatori riguardo alle connessioni aperte, in totale e attuali, segmenti inviati e ricevuti e altre statistiche.

MIB

- Il gruppo EGP tiene conto del traffico di tipo Exterior Gateway Protocol (EGP), protocolli di routing esterni agli Autonomous System (AS). Tiene traccia di quanti pacchetti sono stati inviati e ricevuti, delle eventuali anomalie.
- Il gruppo trasmissione contiene i MIB specifici di dispositivo. Per es. qui vengono mantenute le statistiche specifiche per il protocollo Ethernet.
- Il gruppo SNMP colleziona statistiche sul protocollo Simple Network Management Protocol (SNMP) stesso: quanti sono i messaggi inviati, di che tipo, etc
- MIB II è definito nell'RFC1213. Nel documento sono definiti 175 oggetti appartenenti ai gruppi visti, con gli oggetti suddivisi per gruppo. Per ciascun oggetto viene descritta la funzione.

SNMP

- Il modello SNMP prevede un Manager che invia richieste agli Agent, interrogando le 175 variabili di MIB II più quelle create dai singoli produttori hardware.
- Il protocollo che Manager e Agent utilizzano, l'SNMP vero e proprio, è codificato nell'RFC1448.
- Il Manager invia all'Agent richiesta di informazioni o un aggiornamento di un suo stato secondo la sintassi dell'ASN.1
- Possono essere riportati errori
- SNMP definisce 7 tipi di messaggi per svolgere queste funzioni: 6 di query ed 1 di risposta

Messaggi

Messaggio	Descrizione
get-request	Richiede il valore di una o più variabili MIB
get-next-request	Richiede il valore della variabile MIB successiva
get-bulk-request	Richiede una grande tabella
response	Una risposta a qualsiasi richiesta
set-request	Aggiorna una o più variabili
inform-request	Messaggio da un Manager a un altro Manager che descrive quali variabili sono gestite dallo stesso Manager
snmpv2-trap	Segnalazione di SNMP trap dall'Agent al Manager
report	non definito

Nagios®

- Nagios è uno dei software Open Source più popolari per la gestione delle reti utilizzando SNMP
- http://www.nagios.org
- Ci sono una serie di plugins e di frontend, sempre Open Source che ne estendono le potenzialità
-

Nagios®

Nagios XI

Logged in as: nagiosadmin

System Ok:

Home | Views | Dashboards | Reports | Configure | Tools | Help | Admin

Search...

Dashboard Tools

- Add New Dashboard
- Deploy Dashboards

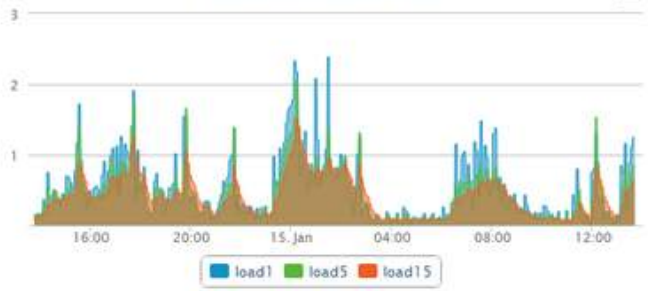
My Dashboards

- Database Server Group
- Groups
- Home Page
- Map
- Stacked Graphs
- Visualizations

Add Dashlets

- Available Dashlets
- Manage Dashlets

localhost : Current Load



Host Status Summary

Up	Down	Unreachable	Pending
33	4	0	0
Unhandled	**Problems**	**All**	
4	4	37	

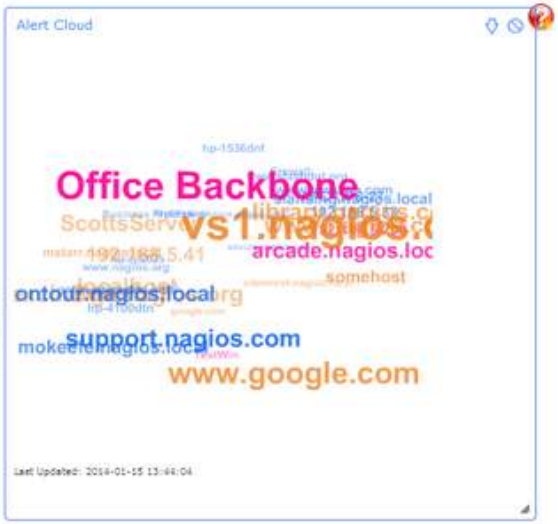
Last Updated: 2014-01-15 13:45:04

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
279	5	1	48	1
Unhandled		**Problems**		**All**
51		53		333

Last Updated: 2014-01-15 13:45:04

Alert Cloud



Last Updated: 2014-01-15 13:44:04

Disk Usage

Host	Service	% Utilization	Details
localhost	Root Partition	75.0%	DISK OK - free space: / 1516 MB (21% inode=83%):
ScottsServer	Drive D: Disk Usage	69.4%	D:\ - total: 232.88 Gb - used: 161.71 Gb (69%) - free 71.17 Gb (31%)
ScottsServer	Drive C: Disk Usage	29.1%	C:\ - total: 452.96 Gb - used: 131.70 Gb (29%) - free 321.26 Gb (71%)
vs1.nagios.com	/ Disk Usage	27.8%	DISK OK - free space: / 56392 MB (71% inode=97%):
exchange.nagios.org	/ Disk Usage	6.6%	DISK OK - free space: / 73482 MB (93% inode=98%):

Last Updated: 2014-01-15 13:44:06

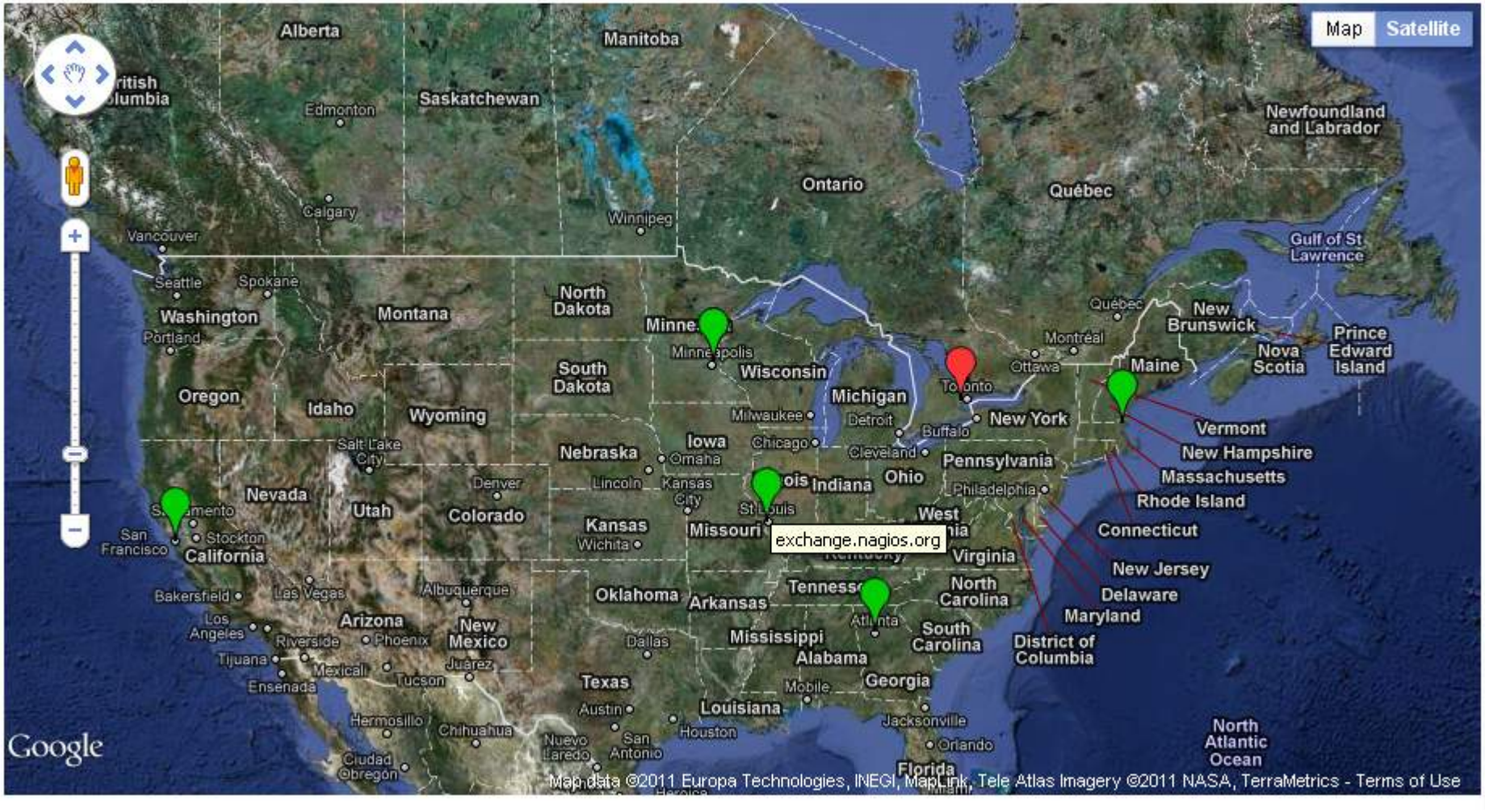
Status Grid

Hosts	Services
192.168.5.200	
192.168.5.33	
192.168.5.41	
abc.com	
APC-UPS-27	
arcade.nagios.local	
Business Process	
conference.nagios.lo	
exchange.nagios.org	
firewall	
gateway.nagios.local	
google.com	
hp-1536dnf	
hp-4100dtn	
hp-cp2025	
kmontour.nagios.loca	
library.nagios.com	

Nagios®


Minemap
Status Grid
Hosts
Services
192.168.5.200
192.168.5.33
192.168.5.41
abc.com
APC-UPS-27
arcade.nagios.local
Business Process
conference.nagios.lo
exchange.nagios.org
firewall
gateway.nagios.local
google.com
hp-1536dnf
hp-4100dtn
hp-cp2025
kmontour.nagios.loca
library.nagios.com
localhost
mokeefe.nagios.local
mstarr.nagios.local
MyBPI Host
Office Backbone
resellers.nagios.com
ScottsServer
sdemoret.nagios.loca
secure.nagios.com
slansing.nagios.local
somehost
support.nagios.com
Switch 1
TestWin
vs1.nagios.com
www.amazon.com
www.google.com
www.nagios.com
Last Updated: 2014-0

Nagios®



Dynamic Host Configuration Protocol (DHCP)

DHCP

- Il Dynamic Host Configuration Protocol (DHCP, RFC 2131) fornisce il supporto per lo scambio tra host di informazioni di configurazione degli stessi host in una rete TCP/IP.
- DHCP è realizzato da 2 componenti:
  - un protocollo per la trasmissione dei parametri di configurazione specifici di un host da un DHCP server all'host interessato
  - un meccanismo per assegnare gli indirizzi di rete agli host
- DHCP non è utilizzato per configurare i router;
- si basa sul paradigma client-server: gli host designati (dall'amministratore) ad essere server DHCP assegnano indirizzi di rete e comunicano i relativi parametri di configurazione ai client.

Dynamic Host Configuration Protocol (DHCP)

- DHCP (RFC 2131) estende il protocollo Bootstrap (BOOTP, RFC 1534) con:
  - l'*automatic allocation* di indirizzi di rete (riusabili);
  - opzioni di configurazione aggiuntive.
- BOOTP è un meccanismo di trasporto per la raccolta delle informazioni di configurazione di host:
  - utilizza il protocollo di trasporto UDP sulla porta 67 (lato server) e 68 (lato client).
  - sfrutta gli indirizzi di broadcast, sia lato client che server, per permettere l'assegnamento degli indirizzi IP
- Uno dei limiti del BOOTP è l'uso degli indirizzi di broadcast che ne limita l'uso solo in segmenti di rete, poiché i router non fanno passare i pacchetti bradcast.
- Limite superato (RFC 1542) configurando un router (o un host) (detto *DHCP/BOOTP Relay Agent*) per riconoscere il traffico BOOTP e permettere al server di distribuire indirizzi IP a più sottoreti

DHCP

- C'e' un'apparente contraddizione dovuta al fatto che DHCP usa lo stack TCP/IP senza che questo sia completamente inizializzato (il client non sa ancora quale sia il suo indirizzo IP).
- DHCP gira come applicazione ed è in grado di utilizzare i servizi broadcast limitati di IP per inviare dei broadcast IP in rete locale anche quando IP non è completamente inizializzato
- Il server non può utilizzare i servizi ARP perché ancora il client non conosce il proprio IP address.
- Per usare DHCP un host diventa client inviando dei messaggi broadcast a tutti i server della rete locale.

  L'host raccoglie poi le offerte dei server, ne seleziona una e ne verifica l'accettazione con il server.

DHCP

- DHCP fornisce 3 meccanismi di allocazione degli indirizzi IP:
  - *automatic allocation*, DHCP assegna un indirizzo IP ad un client permanentemente;
  - *dynamic allocation*, DHCP assegna un indirizzo IP ad un client per un limitato periodo di tempo (oppure fintanto che il client non rilascia l'indirizzo assegnatogli):
    - ✓ permette (automaticamente) il riuso di indirizzi non più utilizzati dai client;
  - *manual allocation*, l'indirizzo IP è assegnato ad un client dall'amministratore e il DHCP è utilizzato semplicemente per comunicare l'indirizzo scelto al client:
    - ✓ permette di eliminare la tendenza a commettere errori mediante configurazione manuale degli host
- quale/i meccanismo/i utilizzare in una rete, dipende dalle regole stabilite dall'amministratore di rete.

DHCP

- Il processo che consente di assegnare gli indirizzi IP agli host prevede 4 fasi (a cui corrispondono altrettanti messaggi del DHCP):
  1. Discovering, il messaggio **`DHCP Discover`** viene inviato dal client per richiedere l'assegnamento di un indirizzo
  2. Offering, il messaggio **`DHCP Offer`** viene inviato da un qualunque server (con un indirizzo a sua disposizione) che ha ricevuto la richiesta inviata da un client nella fase 1 (possono essere ricevute più offerte);

DHCP

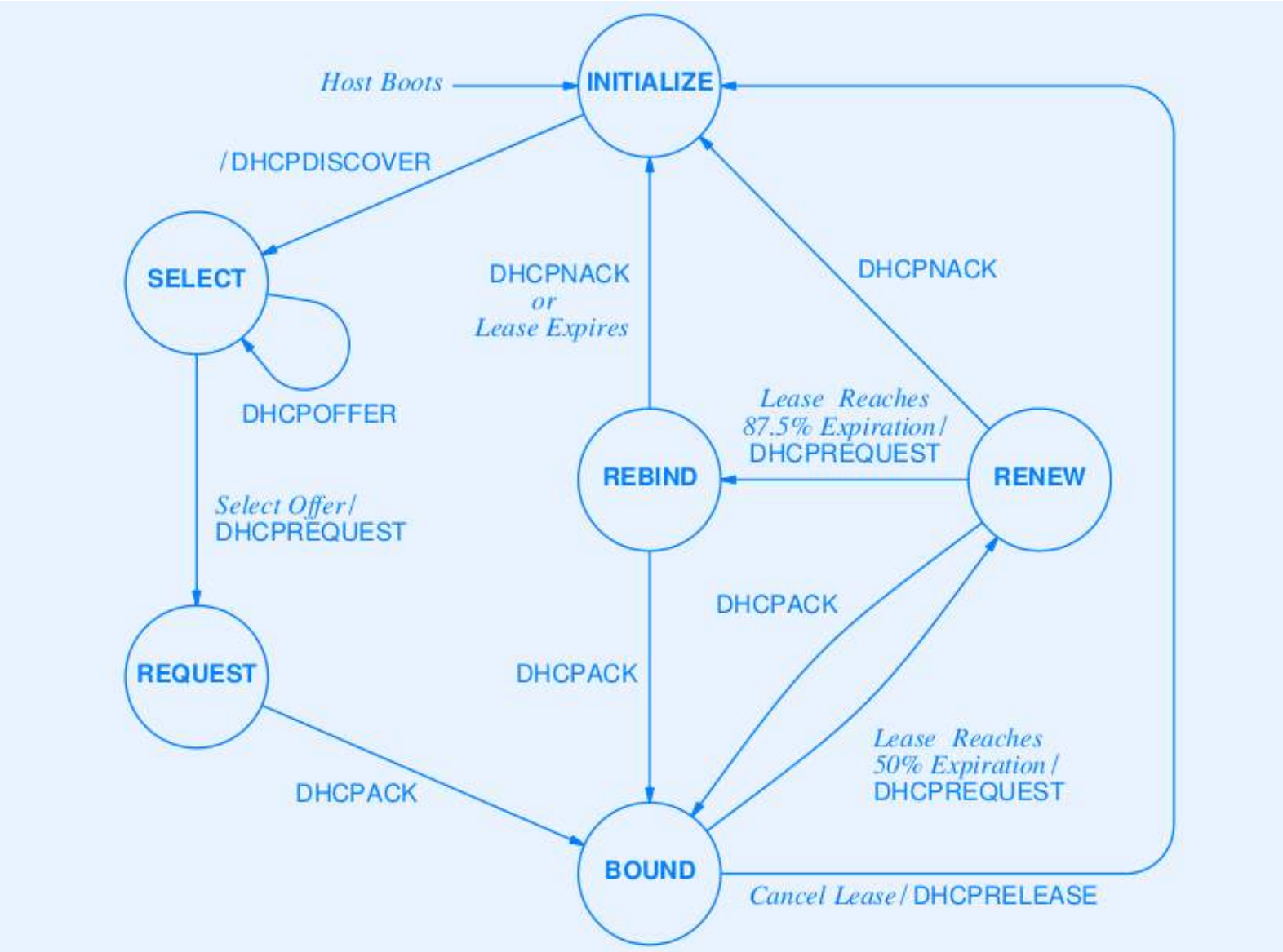
3. Requesting, il messaggio **`DHCP Request`** viene inviato dal client (ancora in broadcast) per comunicare quale offerta ha accettato

4. Acknowledgment, il messaggio **`DHCP Acknowledgment`** viene inviato dal server per conferma (se non ci sono errori) dell'assegnamento dell'indirizzo al particolare client. In caso di errori (es. client richiede un indirizzo non valido) viene inviato **`DHCP NACK`** (negative acknowledgement)

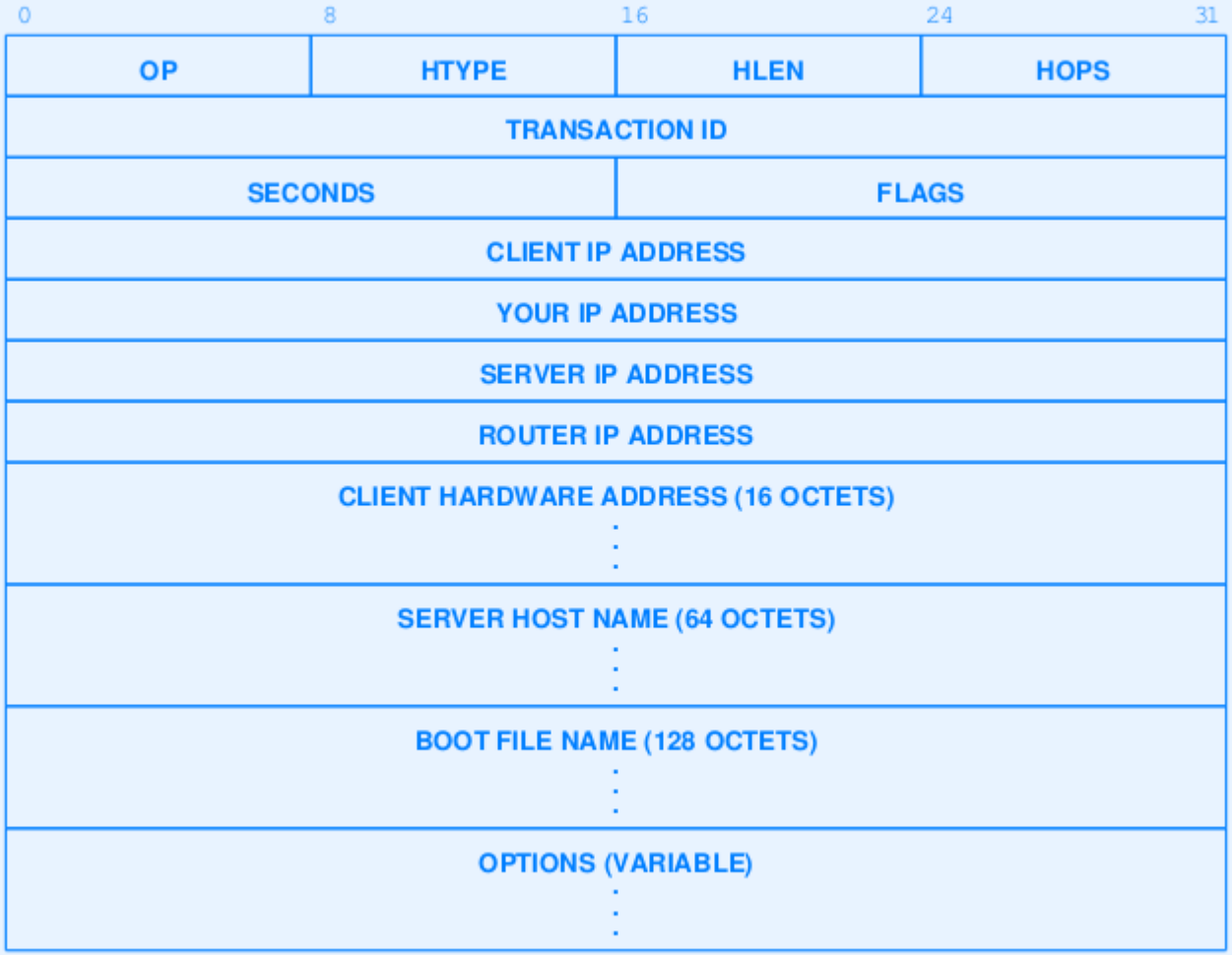
DHCP

- Con il meccanismo di assegnamento dinamico il rinnovo dell'indirizzo IP avviene:
  - al riavvio del client DHCP;
  - a metà durata dell'assegnamento il client;
  - in prossimità dello scadere dell'assegnamento

Macchina a stati finiti DHCP



Formato messaggio DHCP



Tipi di messaggio

TYPE FIELD	Corresponding DHCP Message Type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNACK
7	DHCPRELEASE
8	DHCPINFORM

DHCP

- Configurazione di un server DHCP
  1. Installazione del software

     dipende dal SO usato nel host server

  1. Configurazione di un pool di indirizzi IP

     definizione di un pool di indirizzi da assegnare ai client:

     - ✓ indirizzo iniziale e finale del pool
     - ✓ eventuali intervalli da escludere (quelli già assegnati staticamente come quello del server DHCP e dei router)
     - ✓ durata della validità degli indirizzi assegnati
       - ✓ Tempo finito (es. un giorno quando il numero di client è prossimo a quello degli indirizzi disponibili)
       - ✓ Tempo illimitato
     - un server DHCP può avere configurati più pool di indirizzi

DHCP

1. Opzioni di configurazione dei client DHCP
   - ✓ vengono applicate a tutti i client DHCP che ottengono un indirizzo IP nel pool definito al punto 2
   - ✓ possono essere configurate opzioni globali in server con più pool
   - ✓ Es. opzioni di base (per un client in una certa sottorete)
     - ✓ Pad (permette l'allineamento dei campi successivi a multipli di parole da 32 bit)
     - ✓ Subnet mask (maschera della sottorete)
     - ✓ Router (elenco di indirizzi IP di router)
     - ✓ DNS server (elenco indirizzi IP di server accessibili)
     - ✓ Host name
     - ✓ Domain name
     - ✓ End (fine opzioni nel pacchetto)

DHCP

- Es. opzioni livello IP (per ogni host)
  - IP layer forwarding (abilita o meno il forward dei pacchetti al client)
  - Default Time-To-Live (definisce il TTL per i datagram in uscita dal client)
- Es. opzioni livello IP (per ogni interfaccia di un host)
  - interface MTU (stabilisce la dimensione del Maximum Transmission Unit)
  - Broadcast address (indirizzo di bradcast per la sottorete)
- Es. opzioni livello Link (per ogni interfaccia di un host)
  - Ethernet encapsulation (indica se il client deve usare l'incapsulamento Ethernet)

DHCP

- Es. opzioni livello TCP
  - Default Time-To-Live (definisce il TTL per i segmenti in uscita dal client)
  - Keepalive interval (in secondi, il tempo che il client deve attendere prima di inviare il messaggio Keepalive attraverso la connessione TCP)
- Es. opzioni livello Applicazione
  - NIS domain name (stringa ASCII)
  - NIS server (lista di indirizzi IP di server NIS raggiungibili)

DHCP

- DHCP Client Reservation
  - È possibile riservare un particolare indirizzo IP ad un client; si associa l'indirizzo IP con quello MAC di una interfaccia di rete del client
- Server DHCP in una rete con più segmenti
  - è necessario un DHCP server per ogni sottorete?
  - per ogni segmento di rete si può configurare un DHCP Realy Agent che monitorizza i broadcast DHCP
  - se rileva un pacchetto Discovery o Request lo inoltra verso i server DHCP aggiungendo al pacchetto il proprio indirizzo

DHCP

- Esistono diverse implementazioni di DHCP sotto Unix (commerciali e non)
- **dhcpd** è una implementazione non commerciale del Internet Software Consortium (ISC) compatibile con diverse versioni di Unix

DHCP

Nel file ASCII `/etc/dhcpd.conf` vanno inserite le istruzioni di configurazione quali le sottoreti e gli host client, quali informazioni di configurazioni deve fornirgli; il seguente esempio prevede l'assegnamento dinamico degli indirizzi ai client nella sottorete con supporto a client BOOTP

```
# impostazioni ed opzioni globali
default-lease-time 86400; # tempo medio (in secondi) di
                            # assegnamento di un indirizzo
max-lease-time 604800;    # max tempo di assegnamento
option subnet-mask 255.255.255.0;
option domain "unipg.it";
option domain-name-servers 192.168.12.1 192.168.3.5;

#impostazioni ed opzioni per ogni sottorete servita
subnet 192.168.12.0 netmask 255.255.255.0 {
        option routers 192.168.12.1;
        option broadcast-address 192.168.12.255;
        range 192.168.12.64 192.168.12.192;
        range 192.168.12.200 192.168.12.250;
}
```

DHCP

```
#impostazioni per i BOOTP client
group { # applica il seguente parametro a tutti gli
          # host appartenenti a questo qruppo
    use-host-decl-names true
    host moe {
        hardware ethernet 00:80:c7:aa:a8:04
        fixed-address 192.168.12.4
    }
    host larry {
        hardware ethernet 08:80:20:01:59:c4
        fixed-address 192.168.3.16
    }
}
```

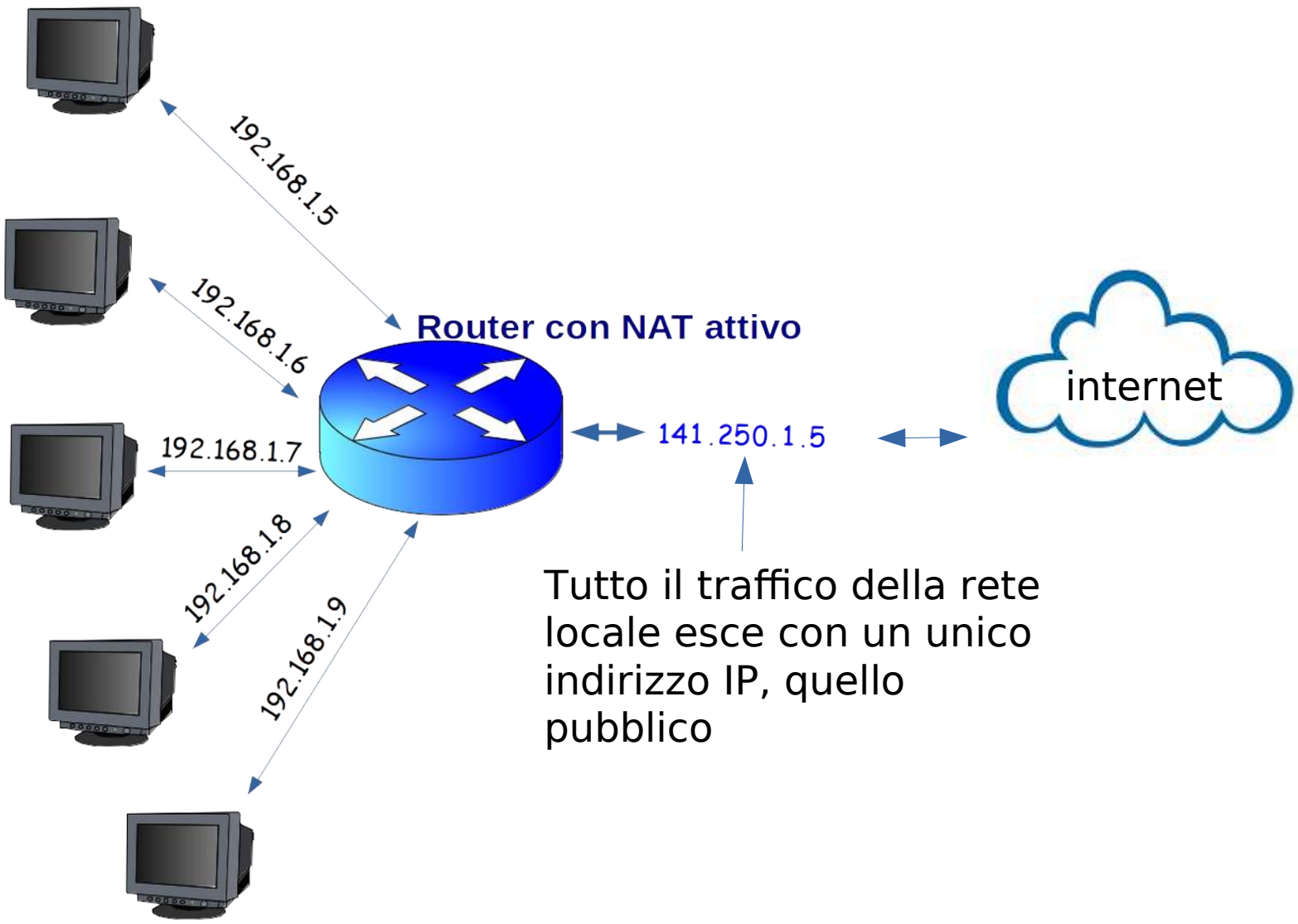
Network Address Translation (NAT)

- NAT è definito dall'RFC 1631
- NAT è un servizio concepito per realizzare la conservazione degli indirizzi IP. E' un servizio che permette a reti IP private di connettersi ad Internet.
- NAT viene eseguito da un router, che connette normalmente due reti, traducendo gli indirizzi della rete interna in indirizzi IP pubblici, ritornando al client la rispettiva risposta.
- NAT viene configurato in modo da convertire tutti gli indirizzi di una rete privata in un unico indirizzo pubblico. Questo fornisce un elemento di sicurezza molto robusto, perché nasconde la rete all'esterno.

Network Address Translation (NAT)

- Vengono usati indirizzi privati invece degli indirizzi di classe A, B e C
  - Gli indirizzi privati permettono di lavorare all'interno di reti locali private
  - Pacchetti con indirizzi IP privati NON SONO GESTITI dai router
- NAT è un metodo che permette di far attraversare la rete Internet a pacchetti originatisi in reti private
  - Un componente (computer, router o firewall) funge da agente tra un rete privata e la rete Internet
  - Un grande numero di host può condividere un ristretto numero di indirizzi IP

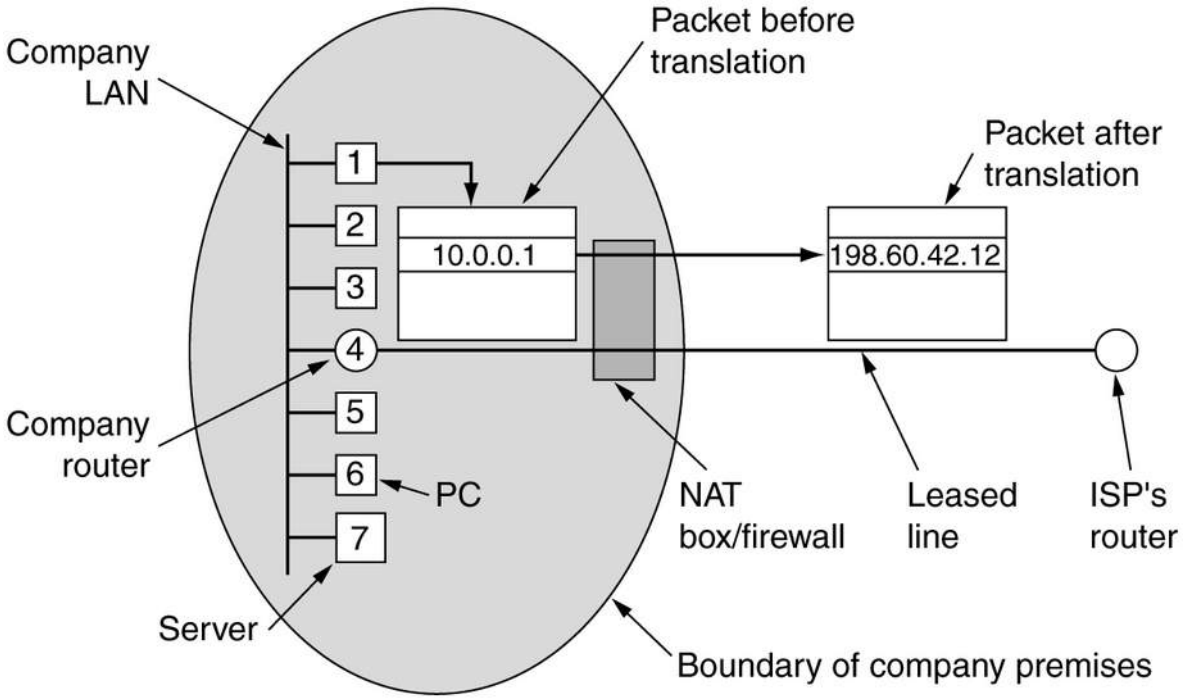
Network Address Translation (NAT)



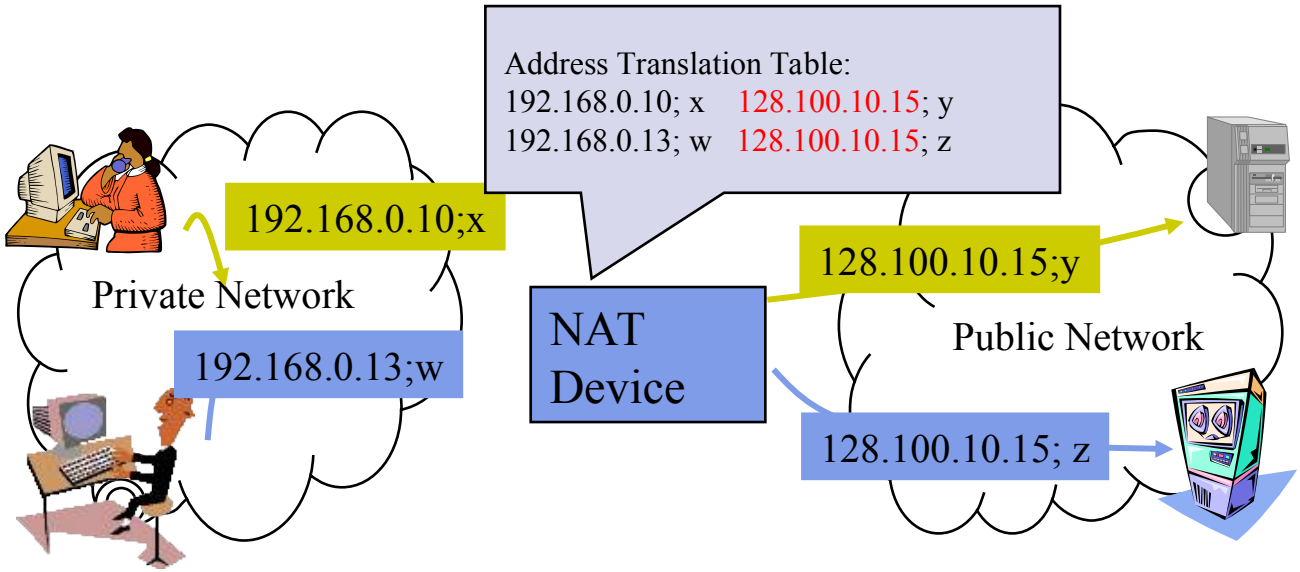
Tutto il traffico della rete locale esce con un unico indirizzo IP, quello pubblico

Network Address Translation (NAT)

- Fornisce la mappatura tra indirizzi IP pubblici e indirizzi privati



Network Address Translation (NAT)



- Gli host della rete locale generano pacchetti con indirizzi IP privati e porte TCP/UDP
- NAT mappa ogni indirizzo privato + porta nel corrispondente indirizzo IP pubblico + porta
- Una tabella di traduzione permette ai pacchetti di essere istradati in modo non ambiguo