

PARTE 4b

LIVELLO IP

(La “dorsale” di Internet)

Modulo 6: Aumentare il numero di indirizzi

Indirizzi IP: sufficienti?

- **Attualmente ciascun indirizzo IP (IPv4) consiste di 4 byte (32 bit)**
- **In IPv4 vi sono 3.758.096.384 indirizzi IP utilizzabili per l'indirizzamento degli host**
- **Ci sono circa 500 milioni di host connessi**
 - Eppure gli indirizzi stanno (quasi!) esaurendo...

Perché?

Perché gli indirizzi IP esauriscono

- **1. Evoluzione della tecnologia e dei dispositivi che consentono connessione a Internet:**
 - Siamo partiti con un indirizzo IP (computer) per molte persone
 - Stiamo arrivando a un indirizzo IP per persona
 - Arriveremo ad aver bisogno di più indirizzi IP per persona
- **2. Gli indirizzi IP non sono e non possono essere distribuiti uniformemente**
 - Classe A: 128 reti, 16M host
 - Classe B: 16K reti, 64K host
 - Classe C: 2M reti, 256 host

Possibili soluzioni

- **Presente (la soluzione “a breve termine”)**
 - → Tecniche di Network Address Translation (“NATting” – si vedrà in seguito)
- **Futuro (la soluzione “definitiva”):**
 - → Passaggio al nuovo standard IPv6

IP version 6 (IPv6)

- **E' senza dubbio l'unica strada che bisognerà seguire per risolvere definitivamente i problemi di indirizzamento**
 - Rende lo spazio di indirizzamento enorme:
da 2^{32} a 2^{128} bit
(~4miliardi*4miliardi*4miliardi*4miliardi)
 - E risolve qualche altro problemino
- **Svantaggio (di non poco conto):**
 - Richiede l'adozione di un nuovo stack
 - → Adozione lenta, continuamente rimandata (anche per motivi di "geopolitica")

Layout dell'header IPv6

Un indirizzo IPv6 consiste di 16 byte (128 bit)!

Version (4 bit)	Priority (4 bit)	Flow label (24 bit)	
Payload length (16 bit)		Next header (8 bit)	Hop limit (8 bit)
Source address (128 bits)			
Destination address (128 bits)			

Reti private e semi-private

- **Per alcune (poche) organizzazioni è importante avere reti private in senso stretto:**
 - nessun pacchetto esce da una rete privata e nessun pacchetto entra in una rete privata
 - indirizzi univoci solo all'interno della rete privata

Reti private e semi-private

- **Per molte altre organizzazioni è importante avere reti semi-private con tre categorie di host:**
 - nessun accesso da/a host fuori “dall’organizzazione” (molti host)
 - accesso parziale (host che possono raggiungere l’esterno ma non sono raggiungibili dall’esterno)
 - accesso completo (pochi host, es. server Web)

Indirizzi IP privati per LAN

- **Un'organizzazione tipicamente ha una rete che include host visibili da Internet (pubbliche) ed altri che non lo sono (private)**
 - Gli host privati scambiano pacchetti solo con gli host (pubblici e privati) di quella che viene detta Intranet
- **Indirizzi IANA privati (Non-Internet Routable IP Addresses) per consentire la comunicazione tra macchine pubbliche e private:**

Intervallo di indirizzi

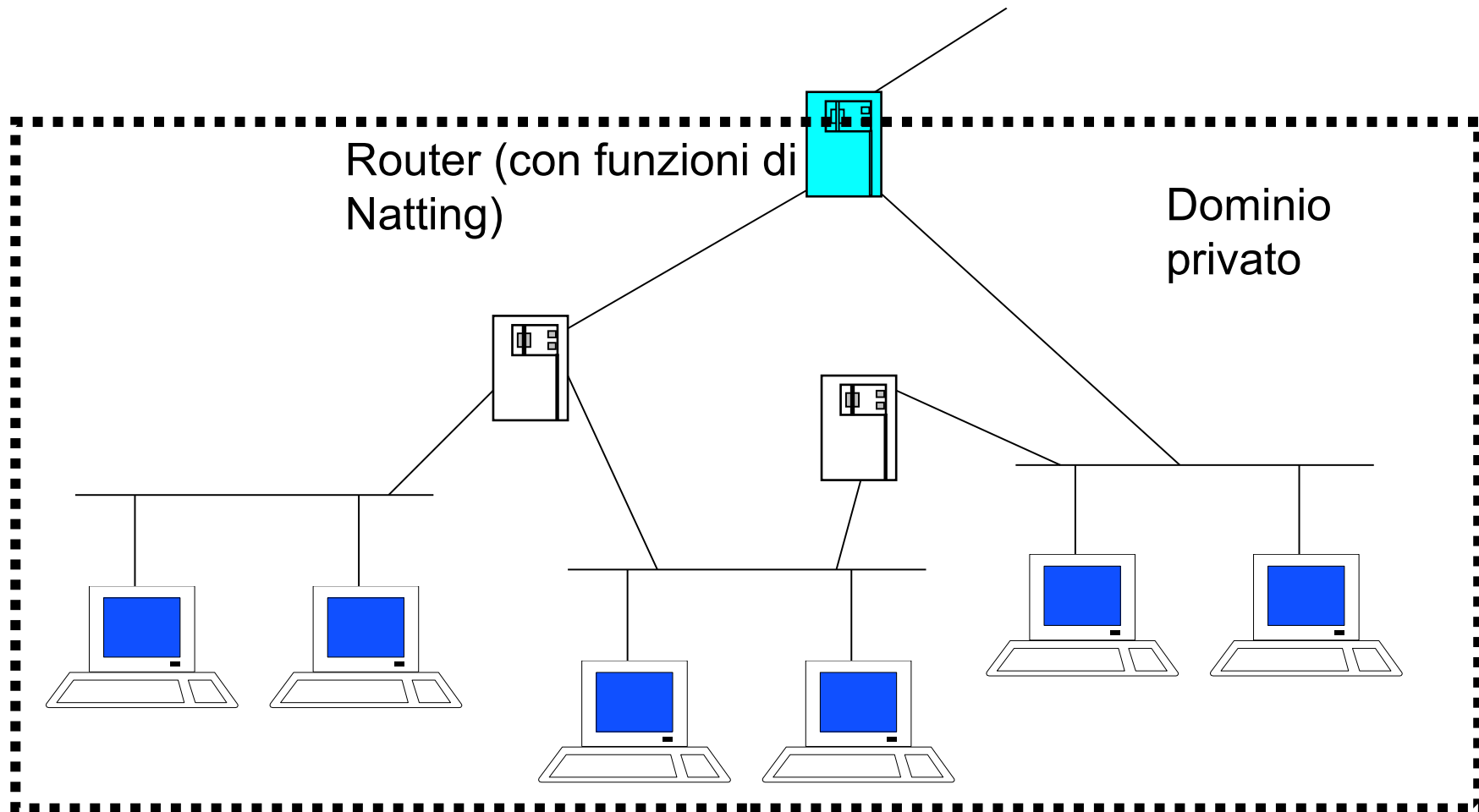
Classe A:	[10.0.0.0 - 10.255.255.255]	(10.0.0.0/8)	– 1 rete
Classe B:	[172.16.0.0 - 172.31.255.255]	(172.16.0.0/12)	– 16 reti
Classe C:	[192.168.0.0 - 192.168.255.255]	(192.168.0.0/16)	– 256 reti

NATting per reti semi-private

- Il NATting è una funzionalità attivabile sul router “al bordo” della rete dell’organizzazione

Dominio esterno

Dominio privato

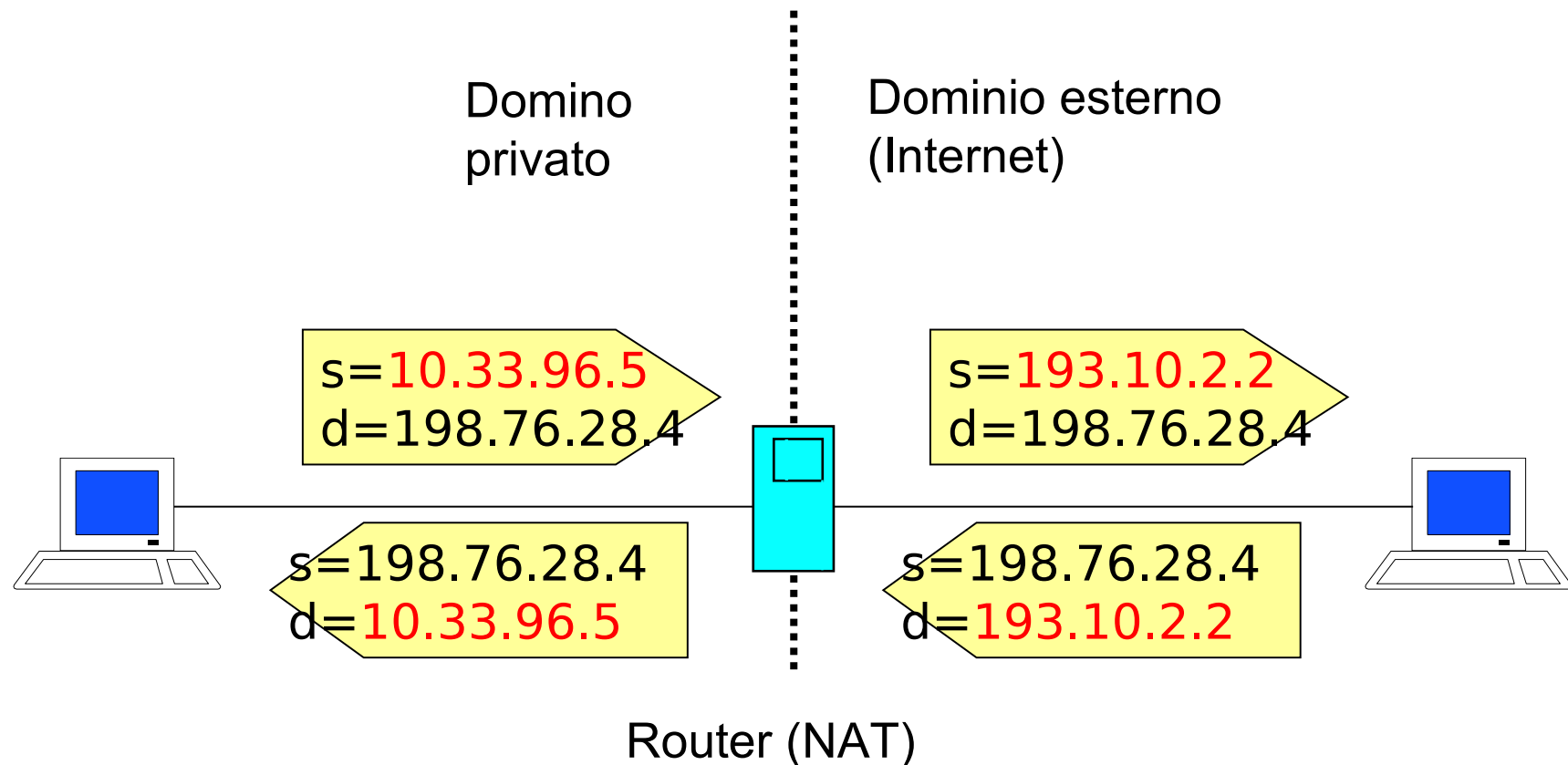


- **Il NATting si interpone tra la rete locale di una organizzazione e Internet con i seguenti compiti:**
 - Mappa gli indirizzi IP tra due domini (interno-esterno)

indirizzi locali → indirizzi IP globali

- Garantisce la trasparenza del routing tra gli end system
- “Moltiplica” le possibilità di interconnessioni di host di una organizzazione (nel caso in cui l'organizzazione abbia a disposizione un numero di indirizzi IP inferiore al numero di host)
- Aumenta la sicurezza evitando di rendere visibili all'esterno alcuni computer di una organizzazione

Traduzione indirizzi



Modifica del datagram IP

vers	len	type of service	total length	
ident			flags	fragment offset
time to live	proto		<i>header checksum</i>	
<i>source IP address</i>				
<i>destination IP address</i>				
options				padding
data				

modificato in uscita

modificato in entrata

Binding degli indirizzi

- **Il router gestisce una corrispondenza (binding) tra gli indirizzi dei due domini tramite una TABELLA:**
- **binding statico**
 - la tabella viene configurata manualmente

Binding degli indirizzi

- **binding dinamico**

- la tabella viene calcolata dinamicamente
- cambia nel tempo a seconda del traffico
- ciascuna “sessione” ha una riga nella tabella
- gli indirizzi privati vengono mappati in indirizzi presi da un pool di indirizzi pubblici
- il pool può essere molto piccolo rispetto alla rete locale: questo determina il numero massimo di connessioni contemporanee a internet, le altre vengono rigettate dal router

Binding degli indirizzi

- **binding on-demand**
 - Si utilizzano protocolli specifici per configurare il binding statico
 - Usato principalmente per il reverse NAT
 - Esempio: protocollo UPnP

Natting: pro e contro

Svantaggi

- Distrugge la semantica della comunicazione end-to-end in quanto gli host interni non possono essere raggiunti dall'esterno
- La cosiddetta NAT box modifica i pacchetti al volo:
 - qualche volta questo richiede modifiche a livello di informazioni application e non solo header del datagramma IP (es., indirizzo IP nel protocollo FTP)
 - È necessario usare dei gateway NAT box livello application

Natting: pro e contro

Vantaggi

- Distrugge la semantica della comunicazione end-to-end in quanto gli host interni non possono essere raggiunti dall'esterno
→ Ottima cosa per la SICUREZZA
- Soluzione economica, relativamente facile e veloce
- Consente massima flessibilità nella gestione interna degli indirizzi senza richiedere alcun permesso al proprio ISP ...

RFC per NAT

- **RFC 1631**

The IP Network Address Translator (NAT)

K. Egevang, P. Francis

May 1994

- **RFC 2663**

IP Network Address Translator (NAT)

Terminology and Considerations

P. Srisuresh, M. Holdrege

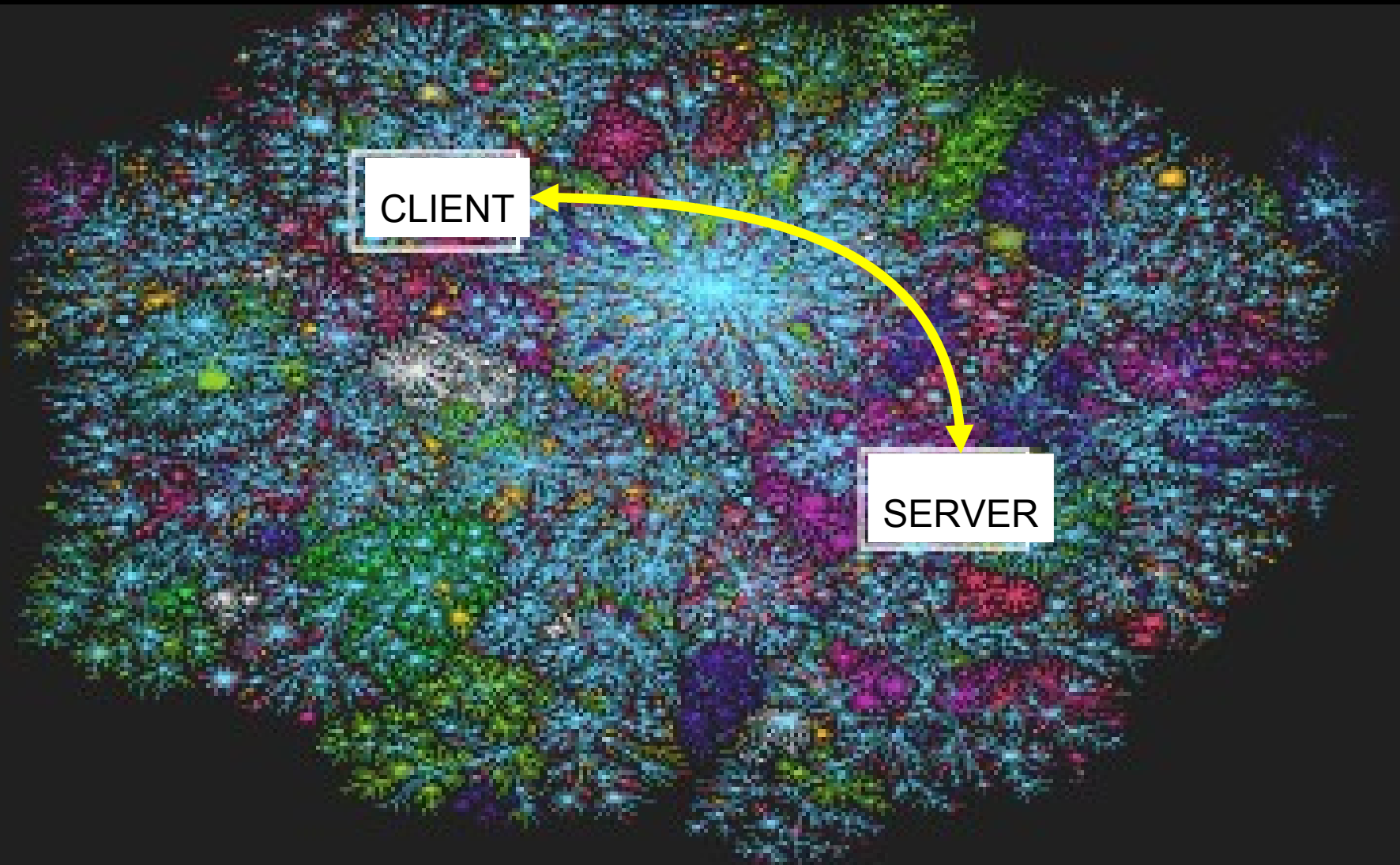
August 1999

Modulo 7: Architettura di Internet

Ma cos'è Internet?

Ma cos'è INTERNET (PdV utente)?

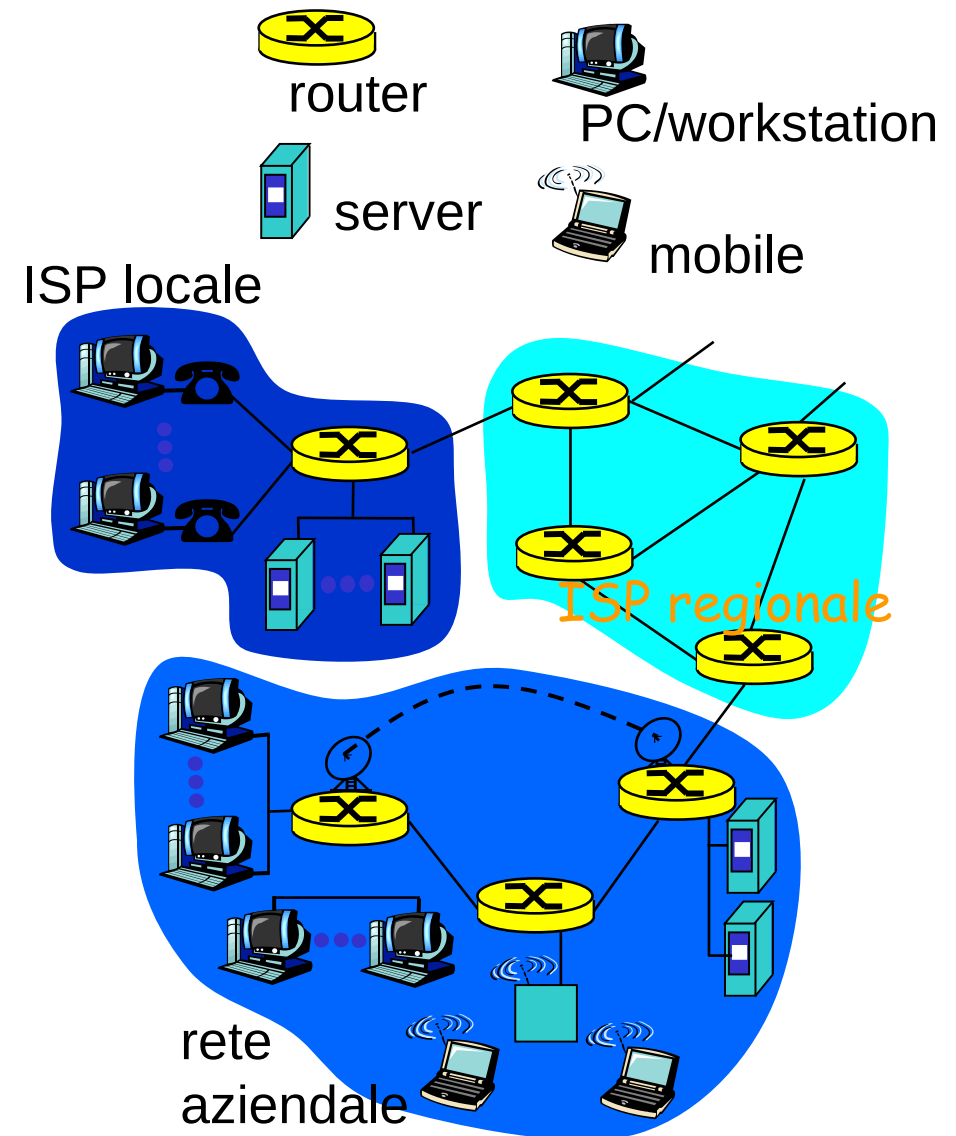
Un entità trasparente per Client/Server



Ma cos'è **INTERNET** (PdV Struttura)?

Un insieme di componenti interni

- Host
- Link di comunicazione
- Router



Obiettivi dell'infrastruttura di Internet

- **Obiettivo globale:**
 - Connettere un qualsiasi numero di reti indipendenti ed eterogenee
- **Scelte fondamentali del progetto:**
 - Multiplexing ottenuto mediante rete packet switched invece che circuit switched
 - Componenti (router) con funzionalità di store and forward tra le reti

Principî di progetto

- **Survivability**

- Se tra i due host esiste un qualsiasi percorso, la comunicazione deve poter continuare (in modo trasparente per i livelli superiori)

- **Forma a clessidra**

- IP effettua minime assunzioni sui mezzi di trasporto sottostanti e deve funzionare per tutti i tipi di applicazioni di rete

Principi di progetto

- **Mancanza di “stato”**
 - La “intelligenza” è mantenuta ai bordi della rete (host)
 - Facilita la survivability
- **Autonomous systems**
 - Ogni rete è posseduta e gestita da un ente diverso

L'organizzazione “interna” di Internet

Architettura lascamente gerarchica

- **Gli host terminali sono connessi ad Internet Service Provider (ISP) locali**
- **Gli ISP locali sono collegati a ISP regionali (tipicamente nazionali)**
- **Gli ISP regionali sono collegati a ISP internazionali, detti National Backbone Provider (NBP) o National Service Provider (NSP)**

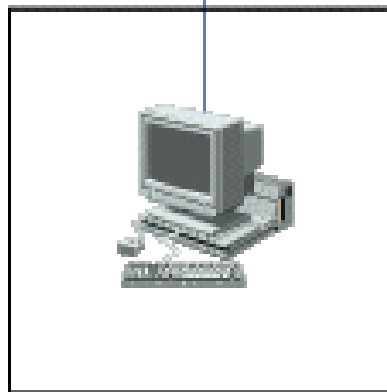
Gestori accessi e trasmissioni Internet

Gestori dei backbone nazionali:
GARR, InterBusiness, ...

Gestori dei backbone internazionali:
EBone, SEABone, UUnet,...

Fornitori di accesso (Local ISP):
Mclink, Tin, Libero, ...

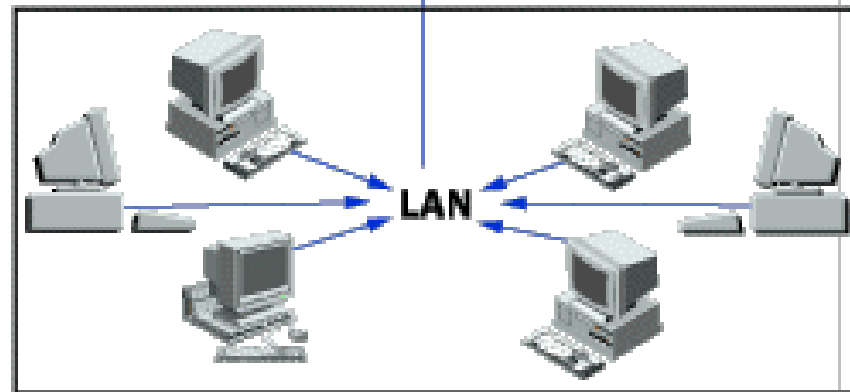
Conventional Phone,
Digital Subscriber,
or Cable Modem Line



Home



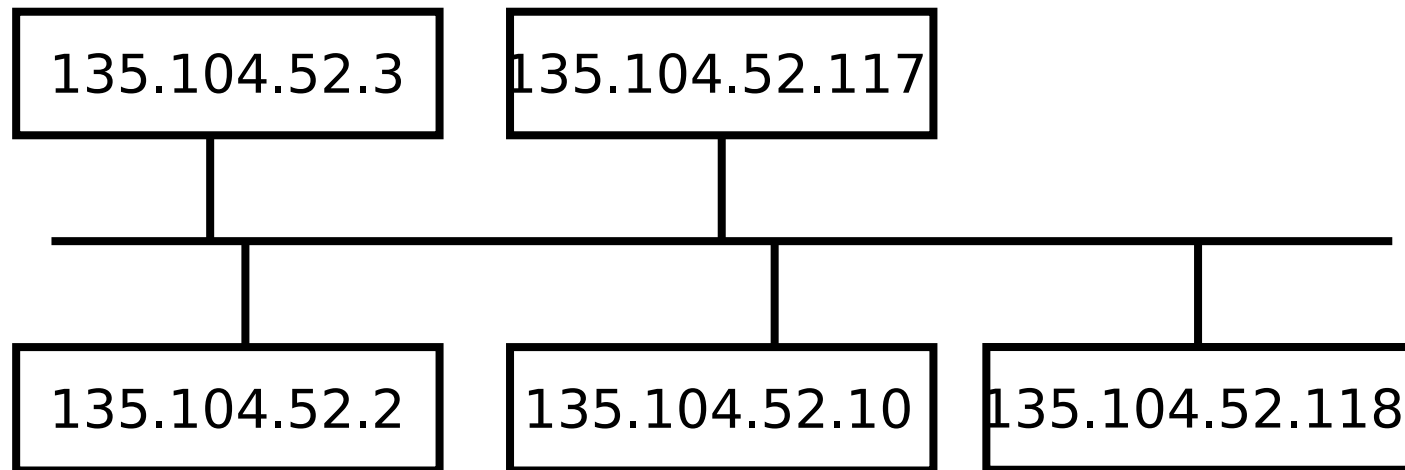
T1
Line



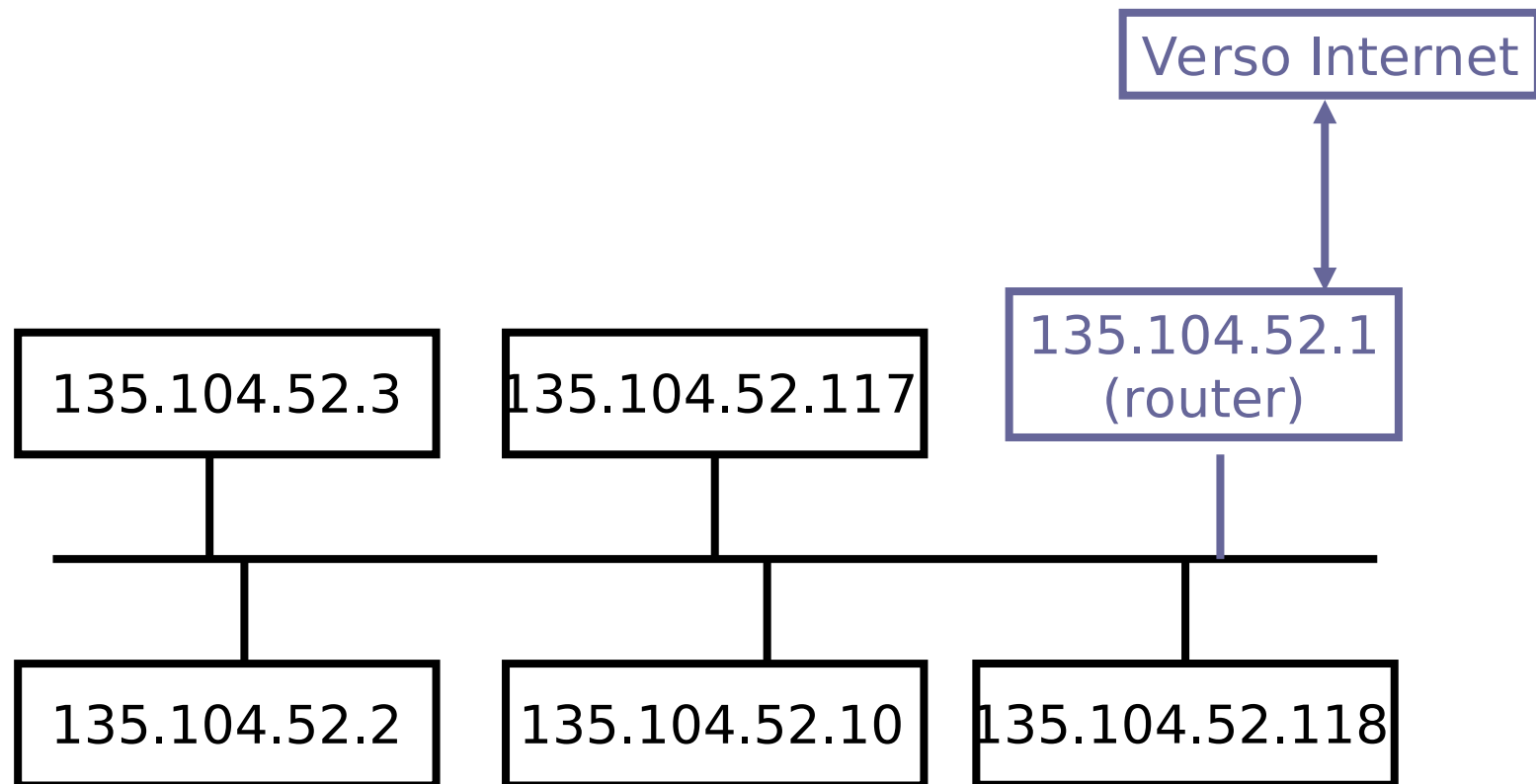
Business

World
ISP

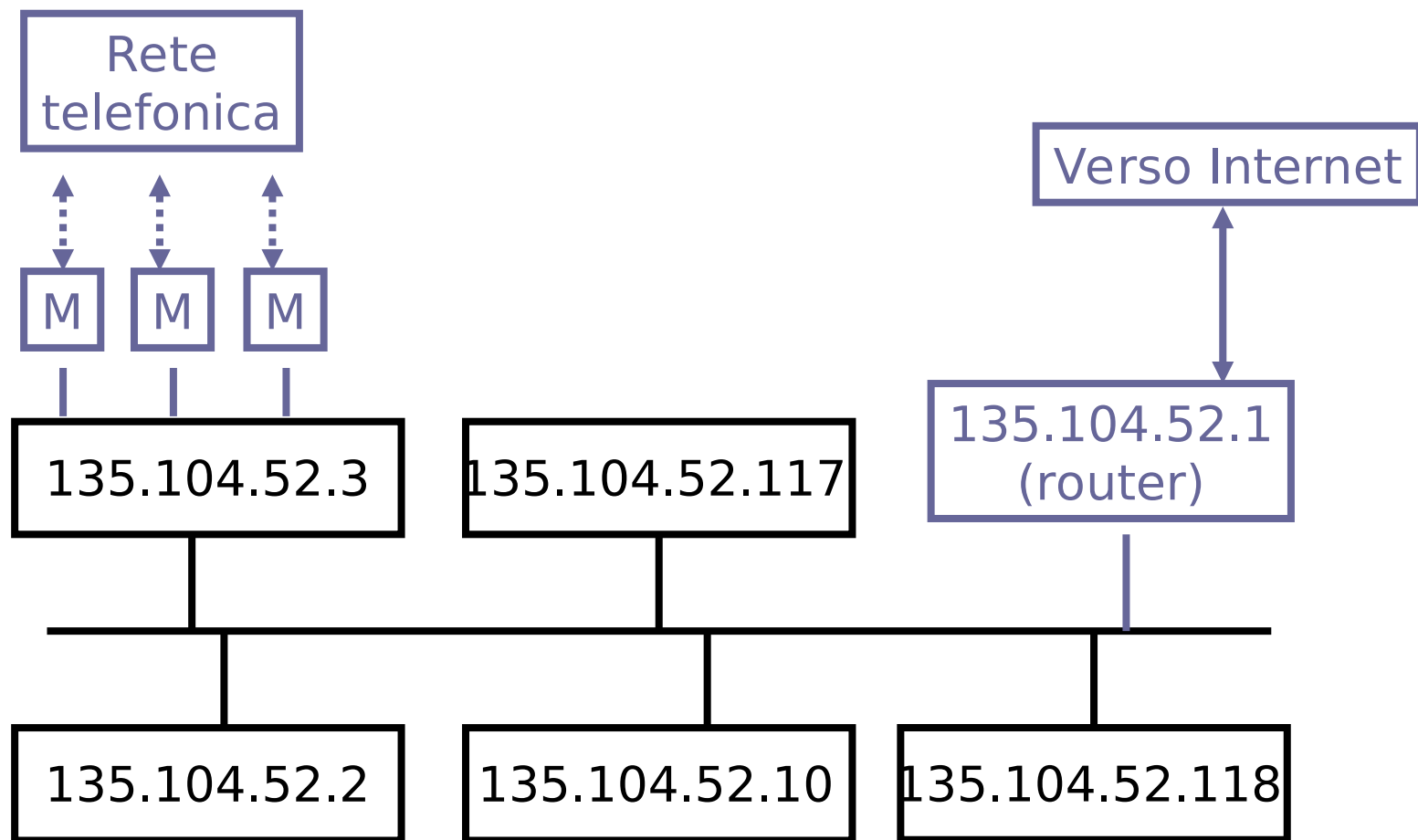
Local area network



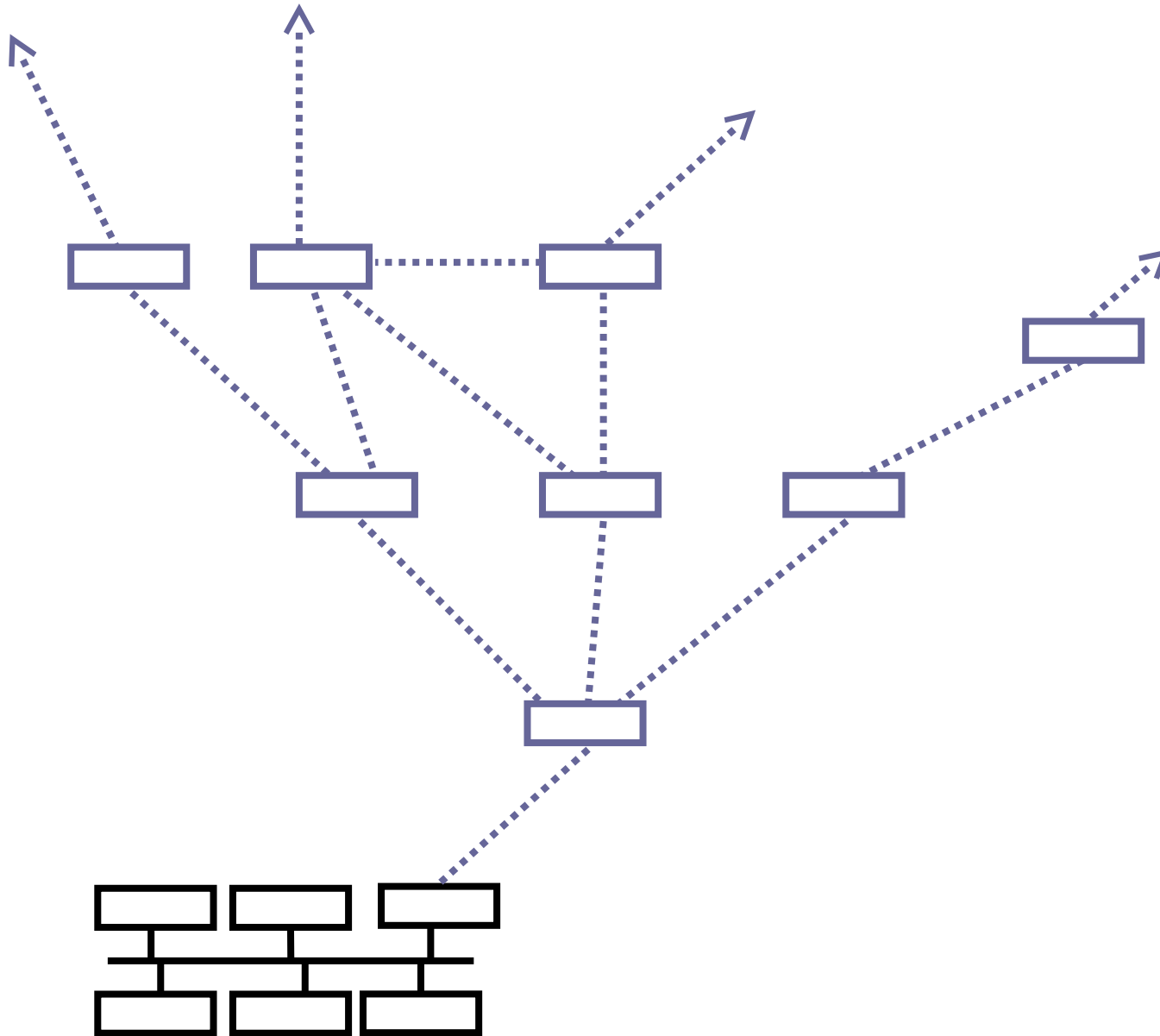
Local area network connessa a Internet mediante router



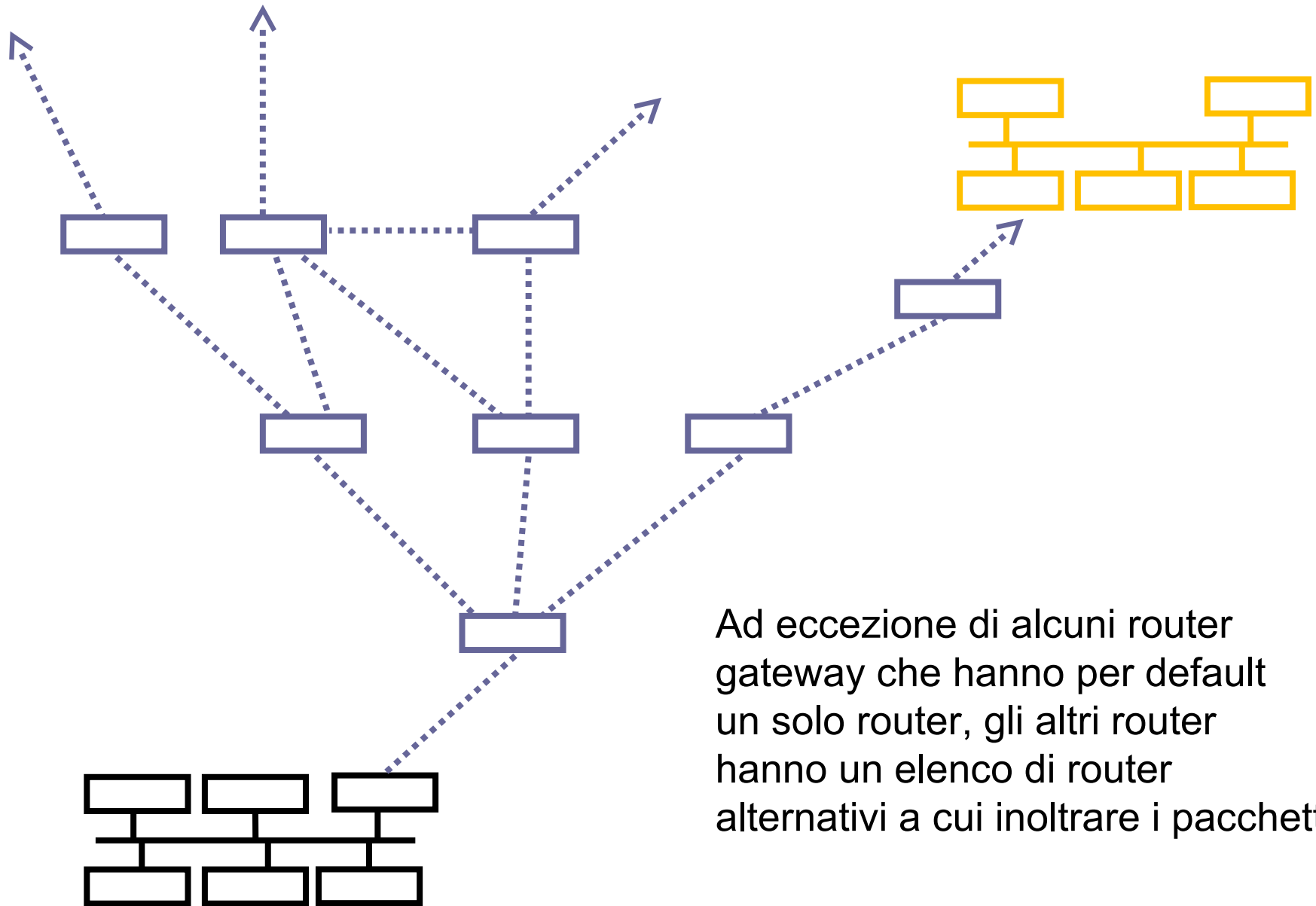
Local area network connessa a Internet mediante modem



Router interconnessioni



Router che collegano LAN



Ad eccezione di alcuni router gateway che hanno per default un solo router, gli altri router hanno un elenco di router alternativi a cui inoltrare i pacchetti

Infrastruttura di Internet

- **ISP locali**

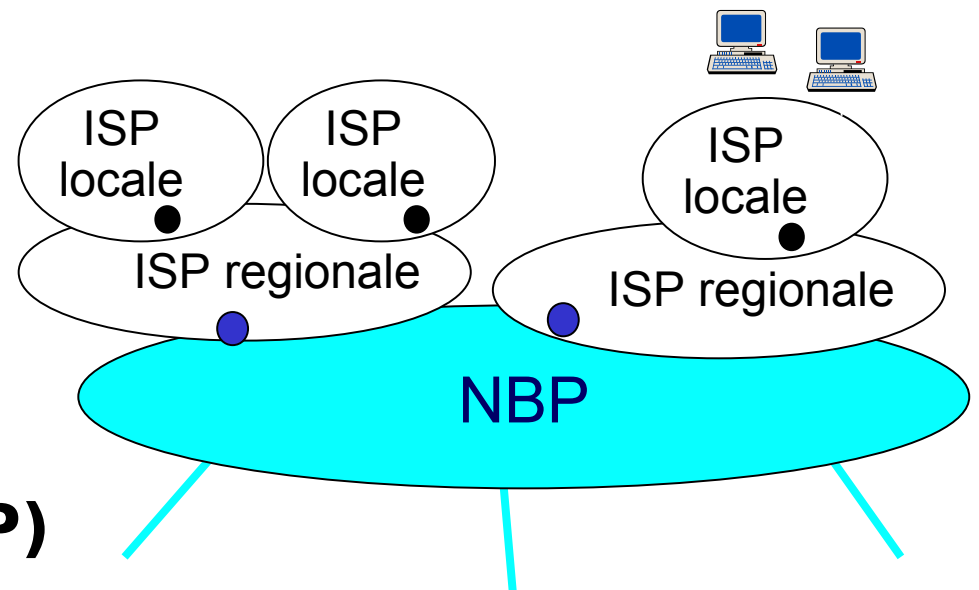
- Ciascun Internet Service Provider (ISP) ha dei Points-Of-Presence (POP) tramite cui si collegano gli utenti privati o aziendali
- A loro volta gli ISP locali si connettono agli ISP regionali (nazionali) mediante linee (almeno T3) tramite i Network Access Points (NAP), gestiti da ISP regionali

- **ISP regionali**

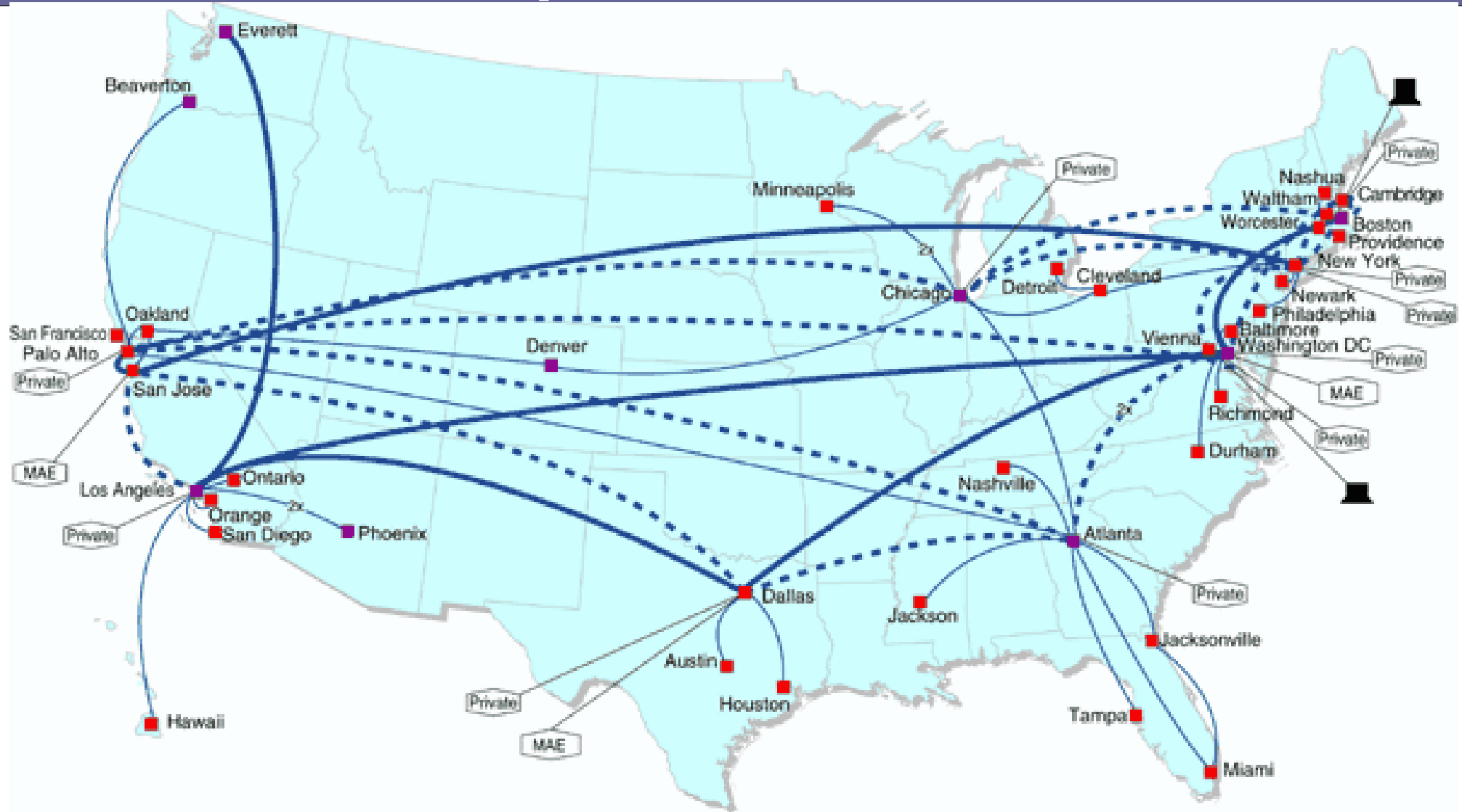
- Noleggiano accesso ai NBP ovvero provider intercontinentali

- **National/international backbone provider (NBP)**

- Es., BBN/GTE, Sprint, AT&T, Verizon, UUNet



National Backbone Provider (es., BBN/GTE provider US)



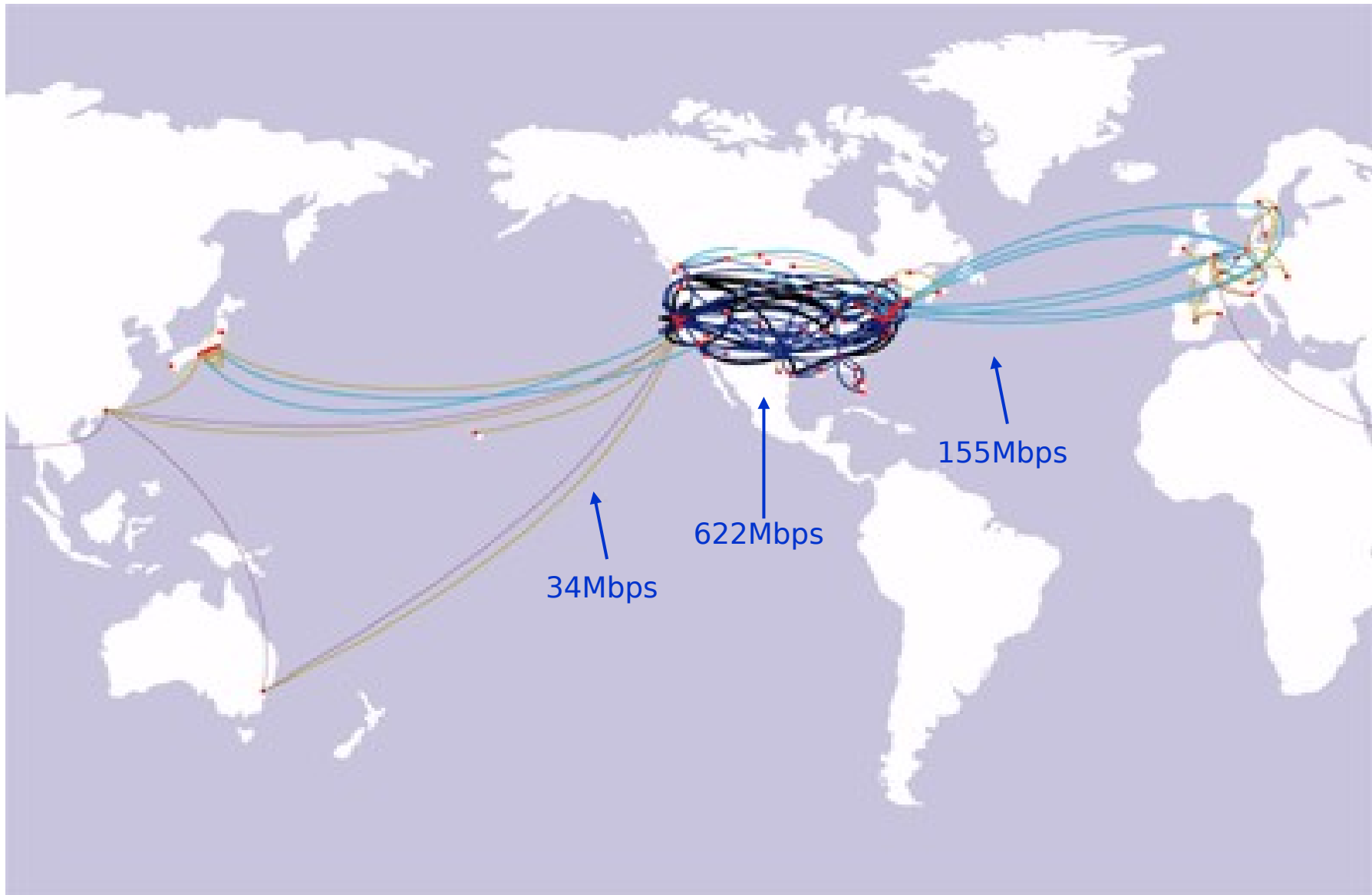
Copyright © GTE Internetworking 1999. All rights reserved. 0399/Version 4

3 Van de Graaff Drive P.O. Box 3073 Burlington, MA 01803

800.472.4565 Web: <http://www.bbn.com> E-mail: net-info@bbn.com

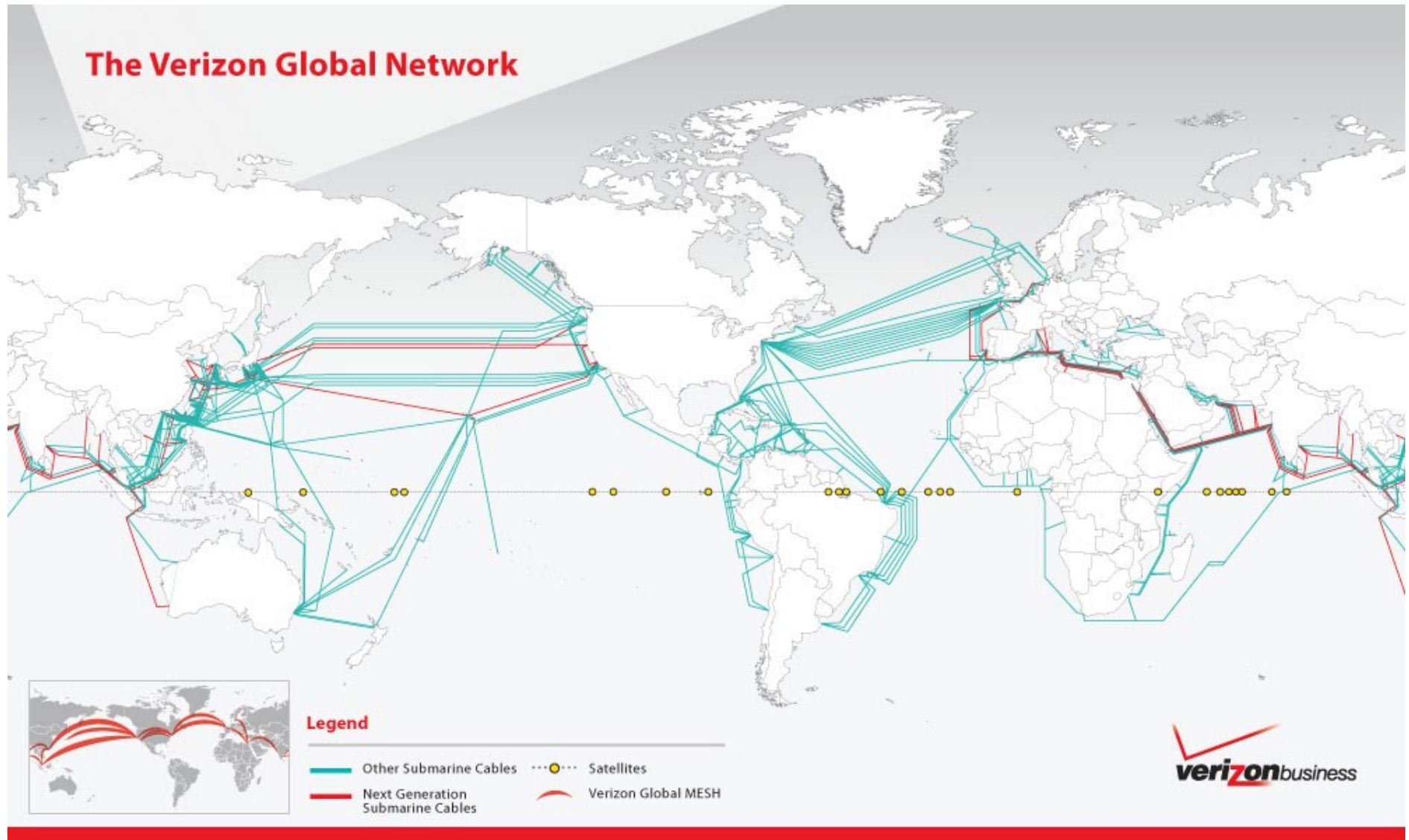
UUNET Backbones (MCI)

(Backbone continentali e intercontinentali)



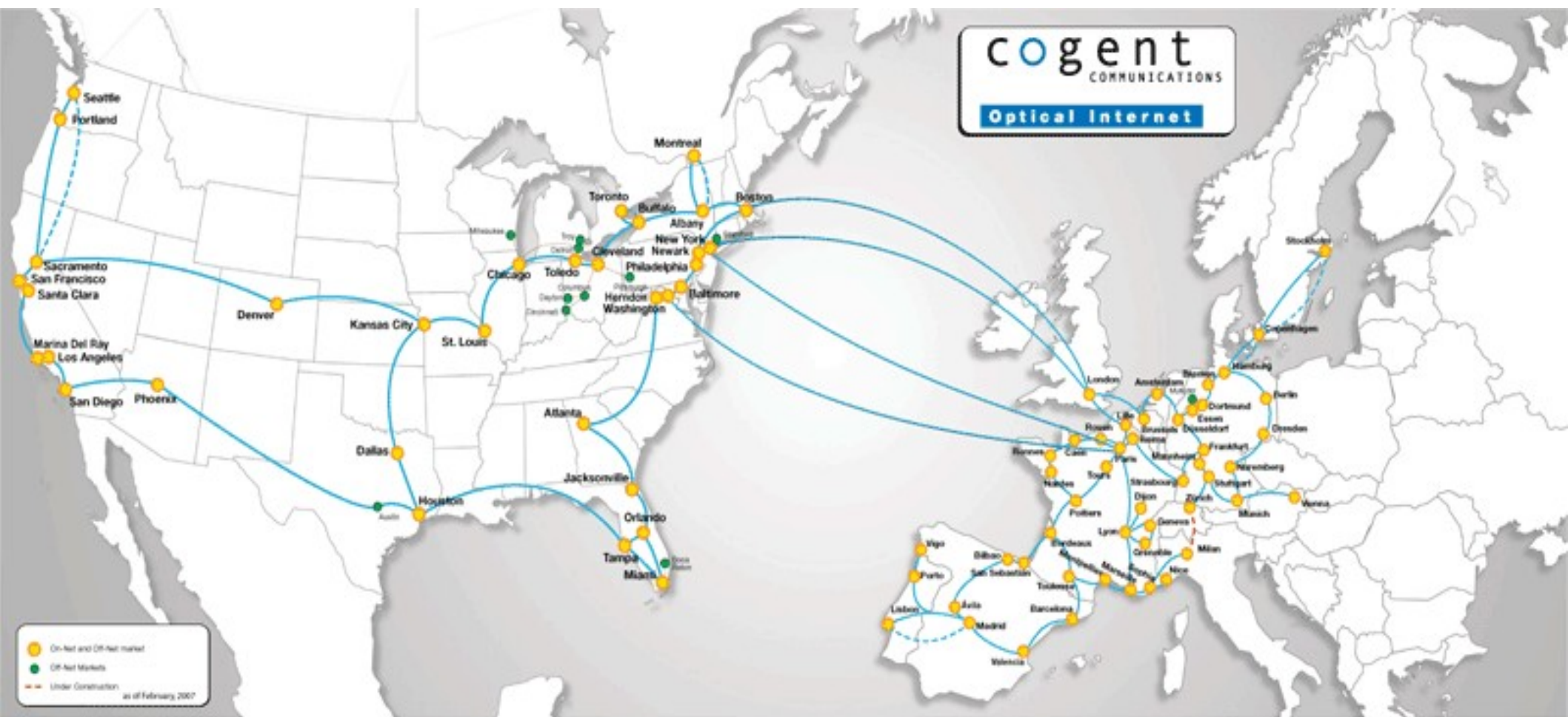
Courtesy of UUNET, 2000

Verizon Backbones (Backbone intercontinentali)



Courtesy of Verizon, 2009

Cogent Communications



Bande di alcune tecnologie trasmissive

• GPRS	56-114 Kbps
• ISDN	64-128 Kbps
• IDSL	128 Kbps
• Satellite	382 Kbps
• Frame relay	56 Kbps – 1.544 Mbps
• T-1	1.544 Mbps
• UMTS	fino a 2 Mbps
• IBM Token Ring	4 – 16 Mbps
• T-2	6.312 Mbps
• DSL	512 Kbps – 8 Mbps
• Modem via cavo	512 Kbps – 52 Mbps
• Ethernet	10 Mbps
• T-3	44.736 Mbps
• OC-1 (<i>ottica</i>)	51.84 Mbps
• Fast Ethernet	100 Mbps
• FDDI	100 Mbps
• OC-3	155.52 Mbps
• OC-12	622.08 Mbps
• Gigabit Ethernet	1 Gbps
• OC-198	10 Gbps

NOTA: bande di picco teoriche

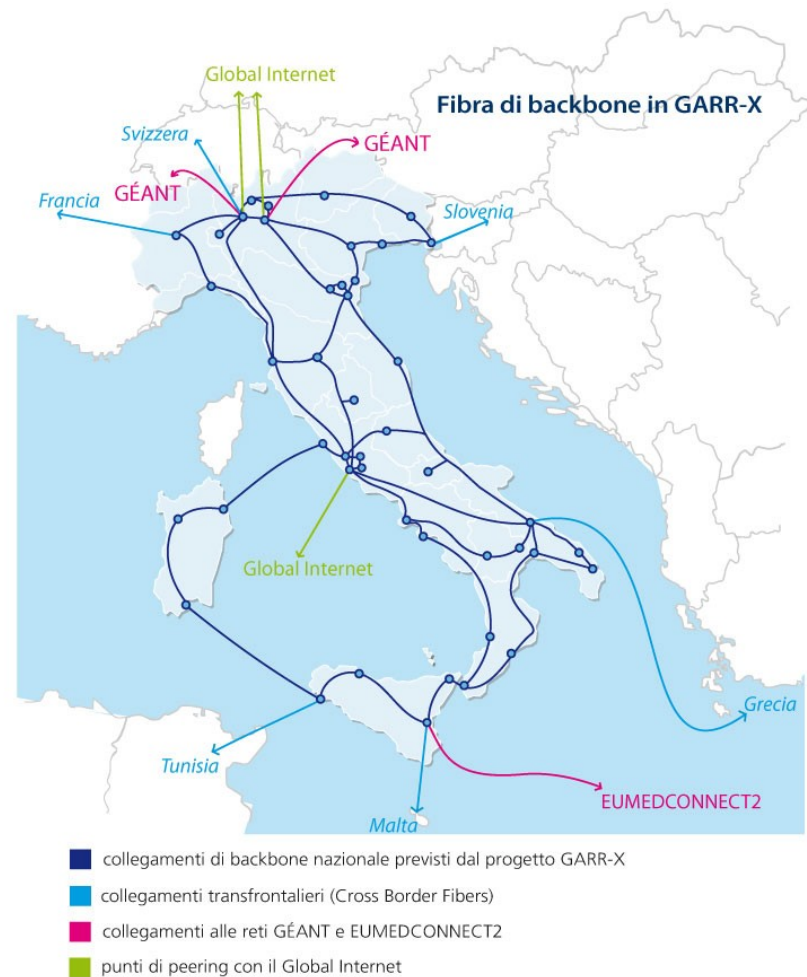
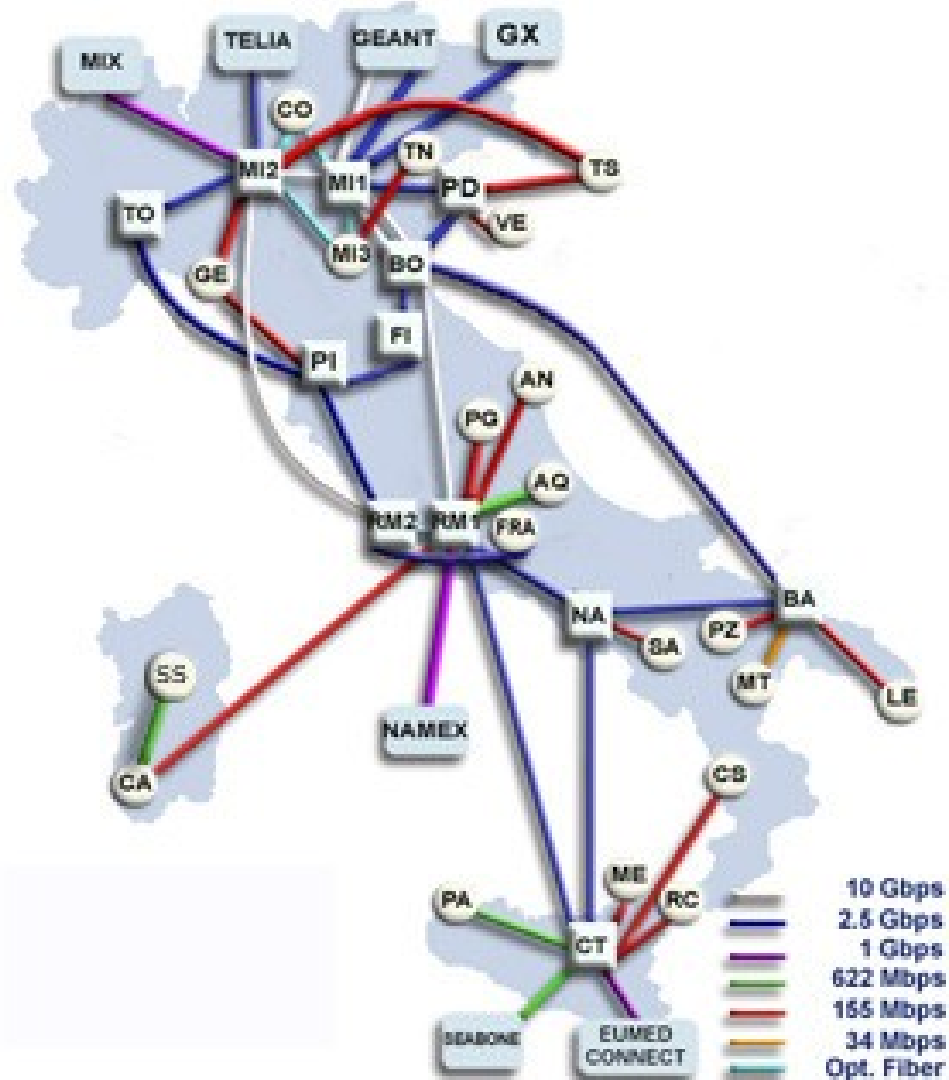
Due storiche dorsali nazionali



La dorsale INTERBUSINESS

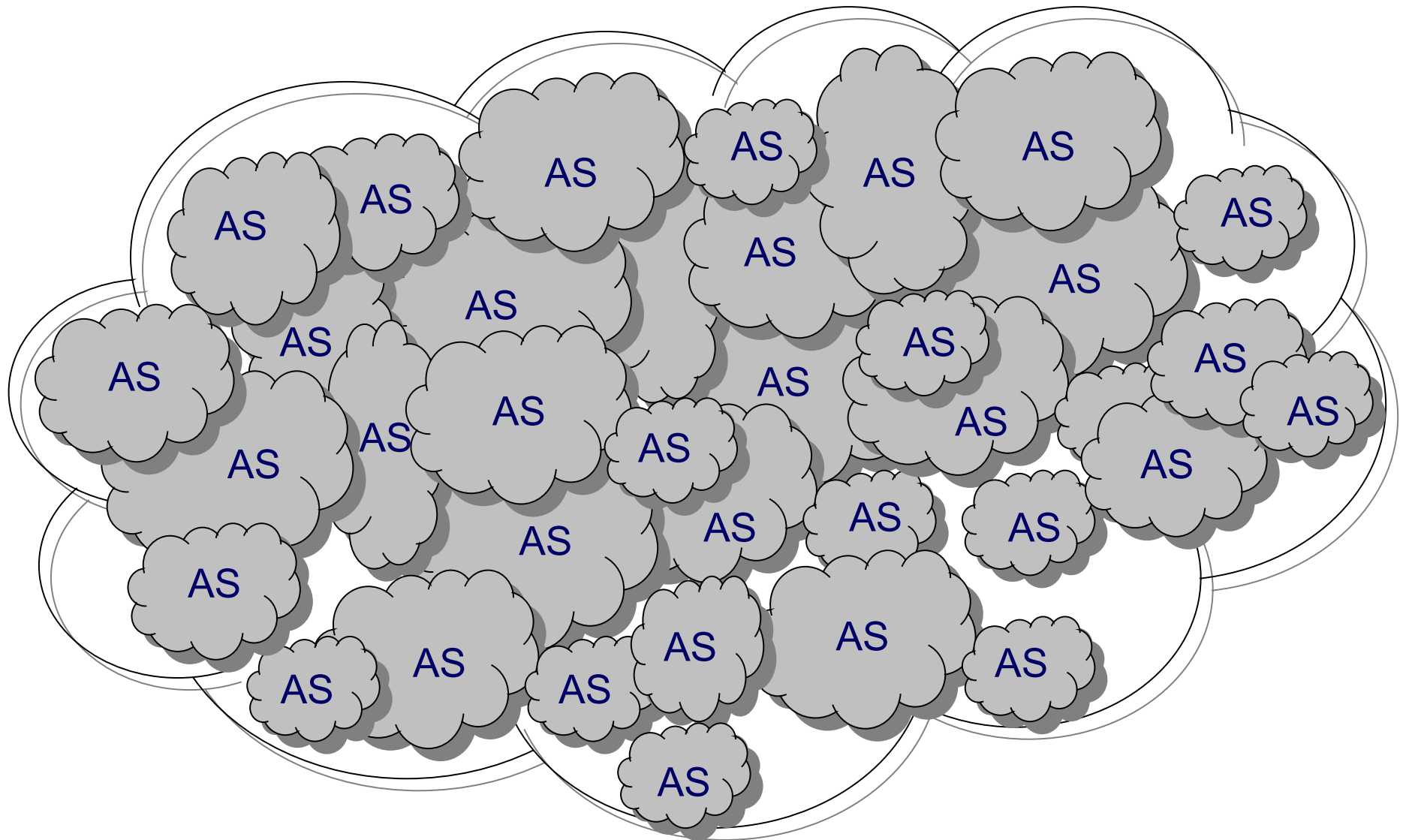


Mappa reti e NAP principali



Cos'è **INTERNET** (PdV Organizzativo)?

Insieme 20000+ Autonomous Systems



Autonomous Systems

- **Internet non è un insieme di router “sparsi” casualmente nel mondo che vengono interconnessi tra di loro
→ I router sono aggregati in regioni, chiamate Autonomous Systems (AS)**

**“Un insieme di reti IP (network prefix) e di router sotto il controllo di una organizzazione (o consorzio di) nell’ambito del quale si utilizza una politica di interior routing. Gli AS sono le unità delle politiche di exterior routing, come nel caso del BGP”
[RFC 1930]**

Autonomous Systems

- **Non tutti i router sono uguali per potenza, per configurazione e modalità di azione**
- **Tuttavia, tutti i router all'interno dello stesso AS usano lo stesso algoritmo di instradamento dei messaggi (routing) e si scambiano continue informazioni con gli altri router**
- **Gli Autonomous Systems dall'esterno vengono visti come un'unica entità**
→ **Gerarchia architettura Internet: 2 livelli**

Situazione degli AS

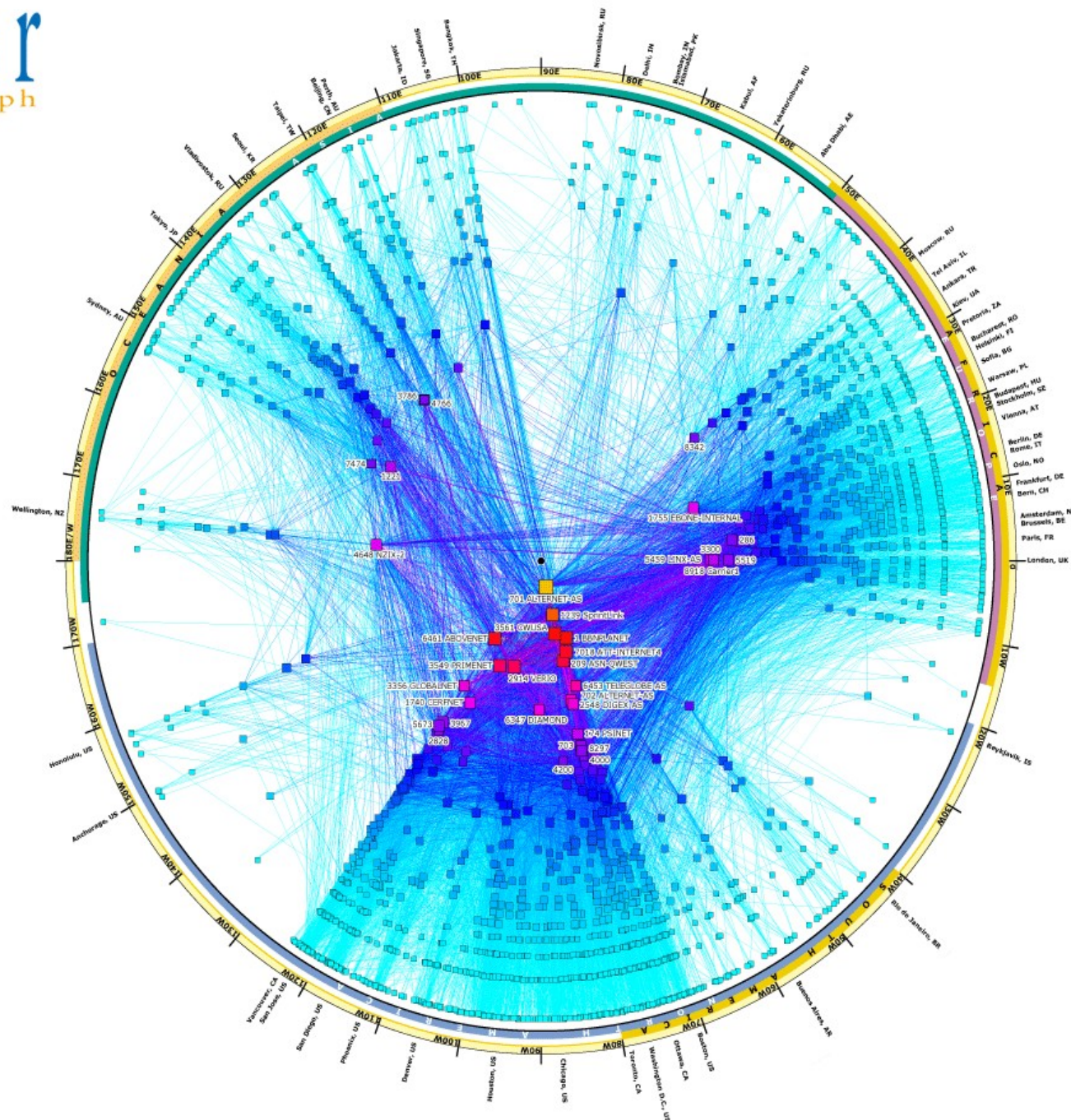
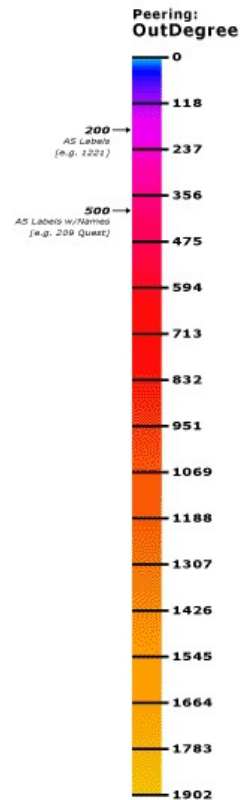
- **Il traffico Internet si distribuisce tra più di 20000 Autonomous Systems (AT&T, UUNET, @Home, BBN Planet, Sprint, Earthlink, RoadRunner, ...)**
- **Ciascun Autonomous System è caratterizzato da:**
 - un numero identificativo su 2 byte ($2^{16}=65536$), in realtà compreso fra 1 e 64511 perché alcuni sono riservati, assegnato da IANA in fase di di registrazione (es. GARR → AS173)
 - uno o più network ID o network prefix (es., 120.240.0.0 nel caso di indirizzo di classe B)

NOTA IMPORTANTE:

- **Nessun AS gestisce più del 5% del traffico**
- **La stragrande maggioranza degli AS gestisce molto meno dell'1% del traffico**

skitter

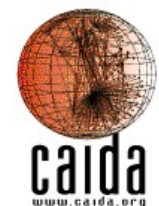
AS internet graph



cooperative association for internet data analysis ○ san diego supercomputer center ○ university of california, san diego
9500 gilman drive, mc0505 ○ la jolla, ca 92093-0505 ○ tel. 858-534-5000 ○ <http://www.caida.org>

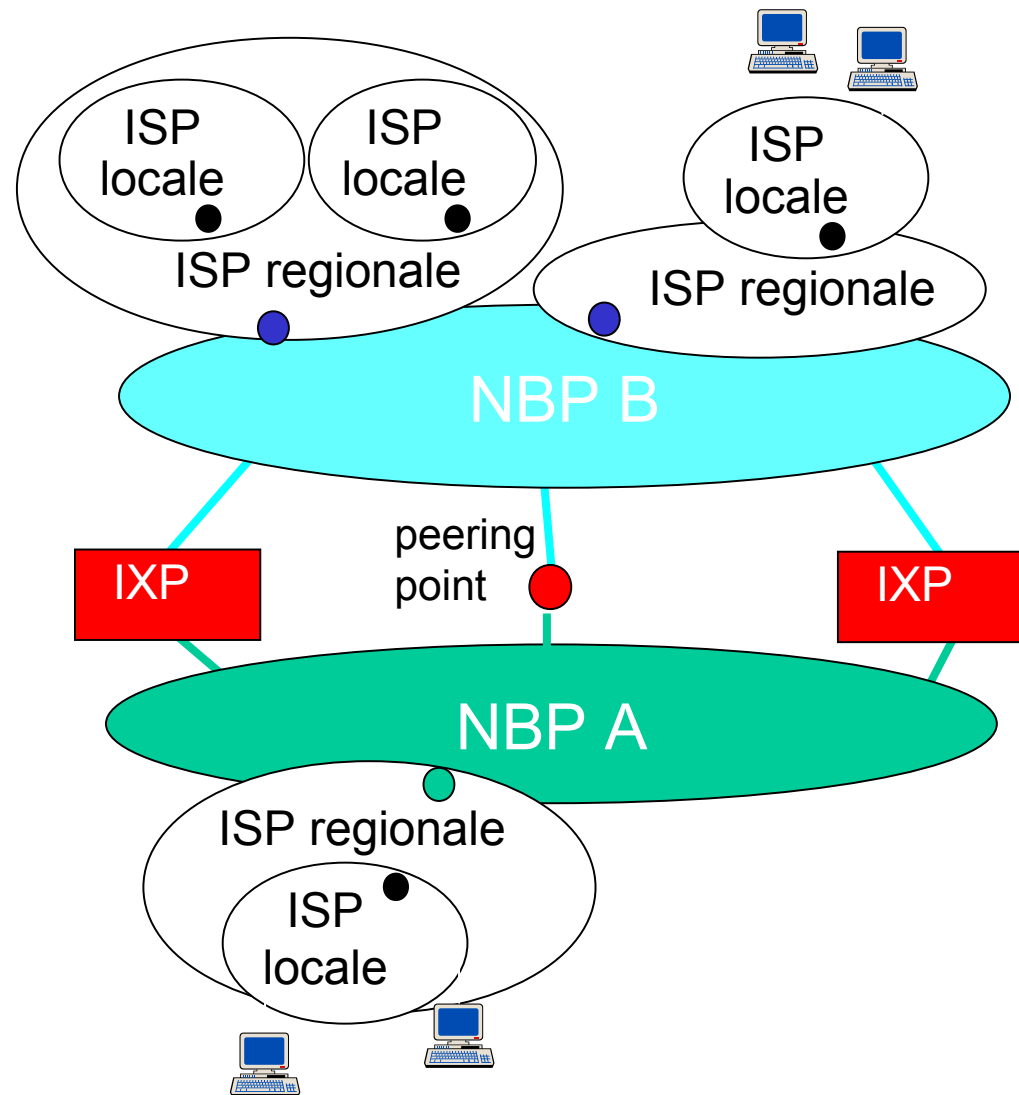
CAIDA is a program of the University of California's San Diego Supercomputer Center (UCSD/SDSC)

skitter is supported by DARPA NGI Cooperative Agreement N66001-98-2-8922, NSF ANIR Grant NCR-9711092 and CAIDA members



Interconnessioni tra AS

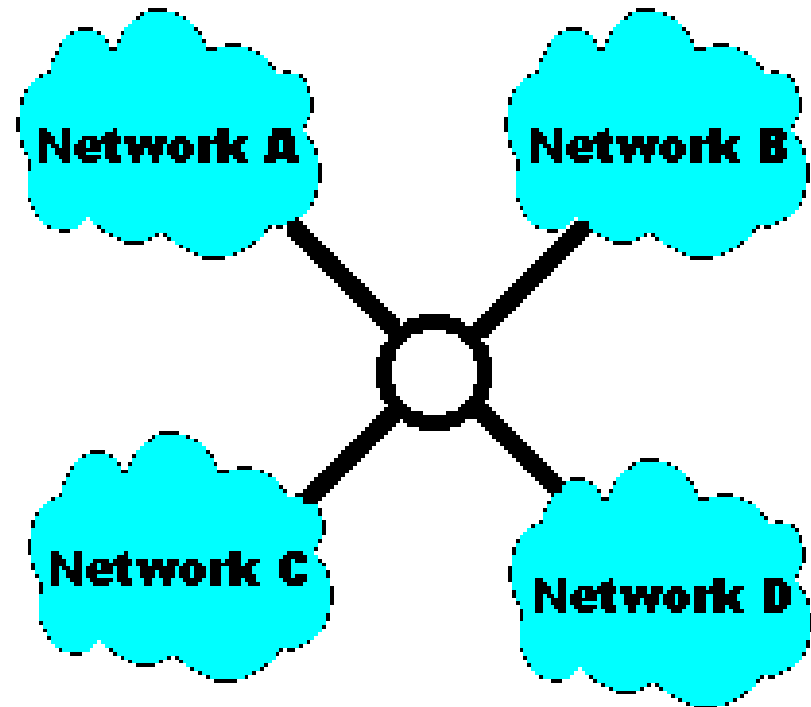
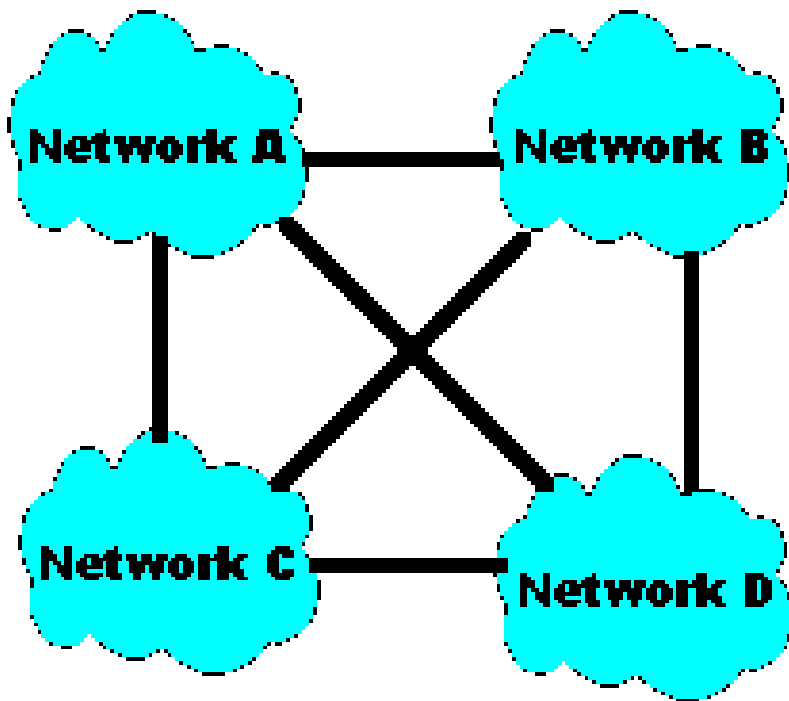
Gli ISP “regionali” (nazionali) e internazionali sono collegati tra di loro al più alto livello della gerarchia, mediante peering point (privati) oppure mediante Internet Exchange Point (IXP o IX), una volta chiamati Network Access Point (NAP)



Interconnessioni tra AS

- **Gli AS sono collegati tra di loro mediante due tipi di “centri di interscambio” traffico:**
 - Peering point (privati) oppure
 - Internet Exchange Point (IXP), una volta chiamati Network Access Point (NAP)
- **Peering è una interconnessione stabilita tra peer (in questo caso, AS) con lo scopo di scambiarsi il traffico dei relativi utenti**
- **Inizialmente era definizione implicita che nessuno dei due contraenti pagava l'altro (“sender keeps all”, inteso pagato dai propri utenti)**
- **Attualmente, è più opportuno definire “settlement-free peering” quando ci si vuole riferire ad una situazione di peering senza pagamenti**

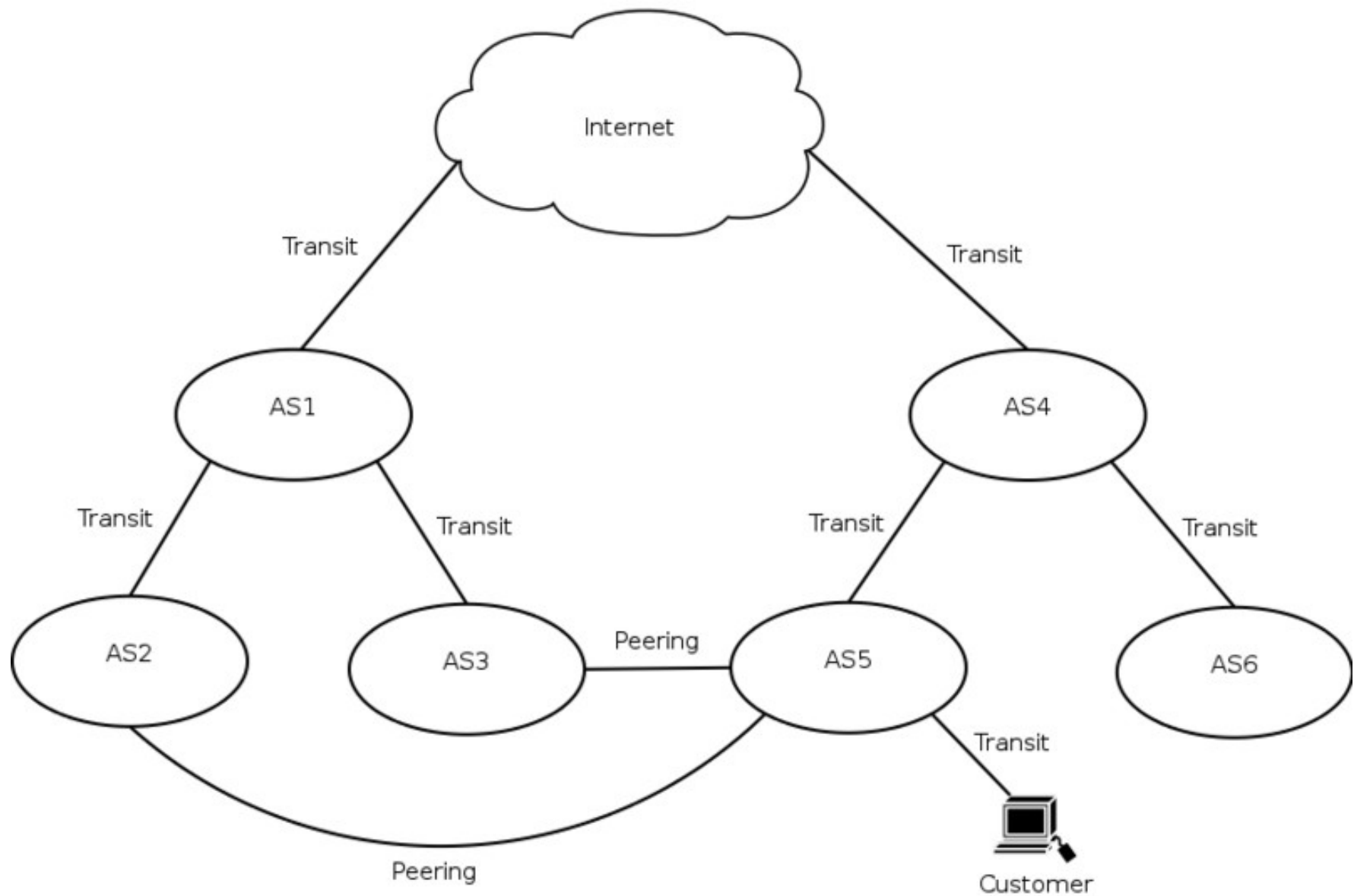
Peering e IXP



Peering point (oggi)

- **Transit (o pay):** tu AS paghi un altro AS per avere accesso o transito su Internet; si accetta chiaramente traffico interno ma anche traffico esterno in transito
- **Peering (o swap):** Due AS si scambiano il traffico dei rispettivi utenti senza costi, per reciproco interesse:
 - non solo per evitare costi,
 - ma anche per aumentare affidabilità creando strade alternative,
 - e per diminuire la lunghezza dei percorsi creandone uno diretto
- **Customer (o sell):** Un altro AS paga te AS per avere accesso a Internet

Esempio



Internet Exchange Point (IXP o IX)

- **Tipicamente consorzi indipendenti senza scopo di lucro**
- **Creati fra AS, talvolta supportati da finanziamenti pubblici**
- **Spesso sono Metropolitan Area Exchange (MAE)**
- **Offrono servizio tra gli associati, ma anche ad altri**

Internet Exchange Point (IXP o IX)

- **Elenco (non completo) dei principali IXP mondiali:**
 - Amsterdam Internet Exchange (AMS-IX) – 259 partner, 218 Gbps di banda massima
 - London Internet Exchange (LINX) – 221 partner, 221 Gbps di banda massima
 - Deutscher Commercial Internet Exchange (DE-CIX) – 189 partner, 189 Gbps di banda massima
 - New York International Internet Exchange (NYIIX) – 98 partner, 21 Gbps di banda
 - Milan Internet Exchange (MIX) – 59 partner, 21 Gbps di banda
 - Athens Internet Exchange (AIX) – 14 partner, 2 Gbps di banda
 - Nautilus Mediterranean Exchange (NAMEX) – 32 partner, 32 Gbps di banda

Alcuni IX



LINX (Londra)



AMS-IX
(Amsterdam)

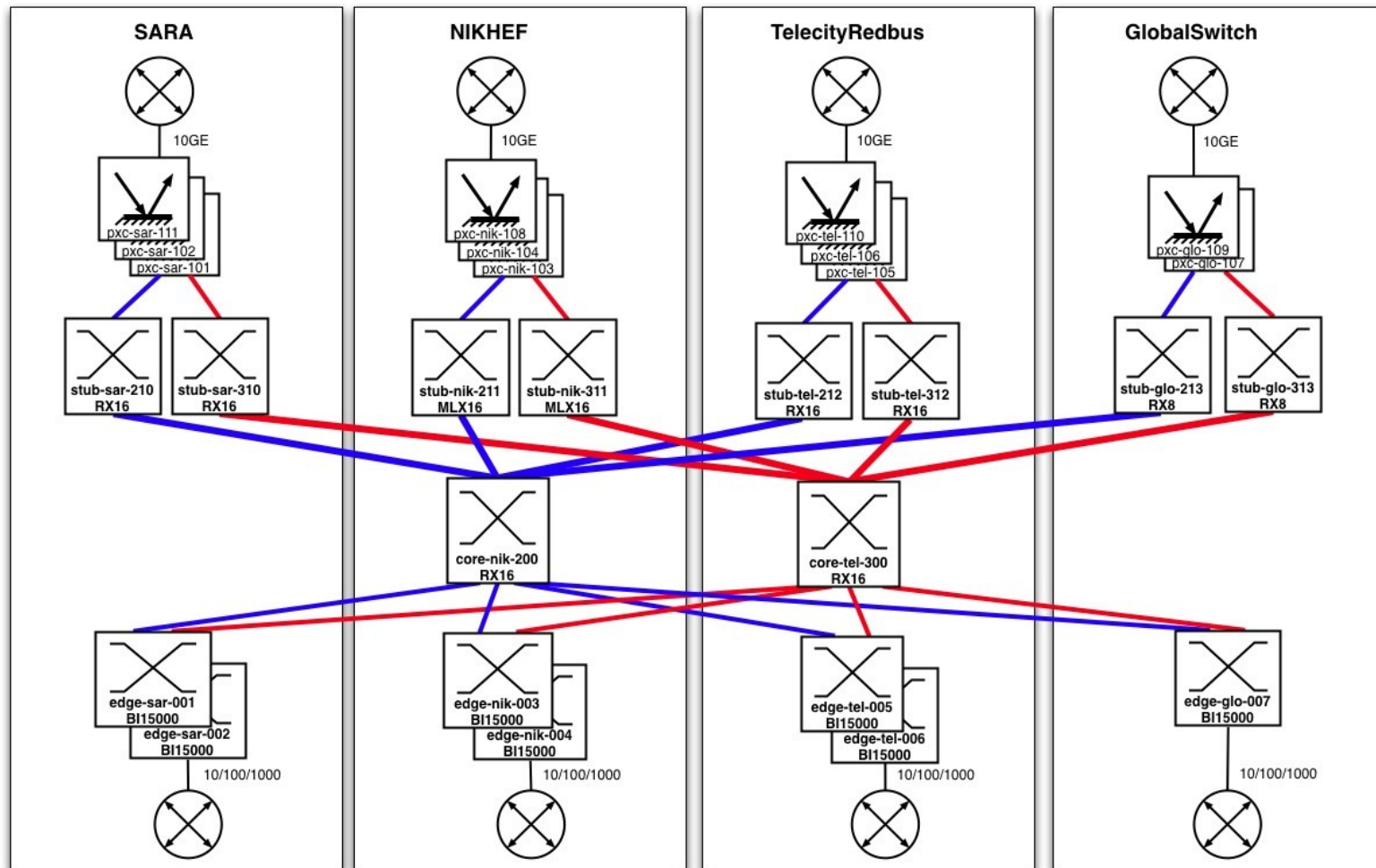


NYIIX (New York)

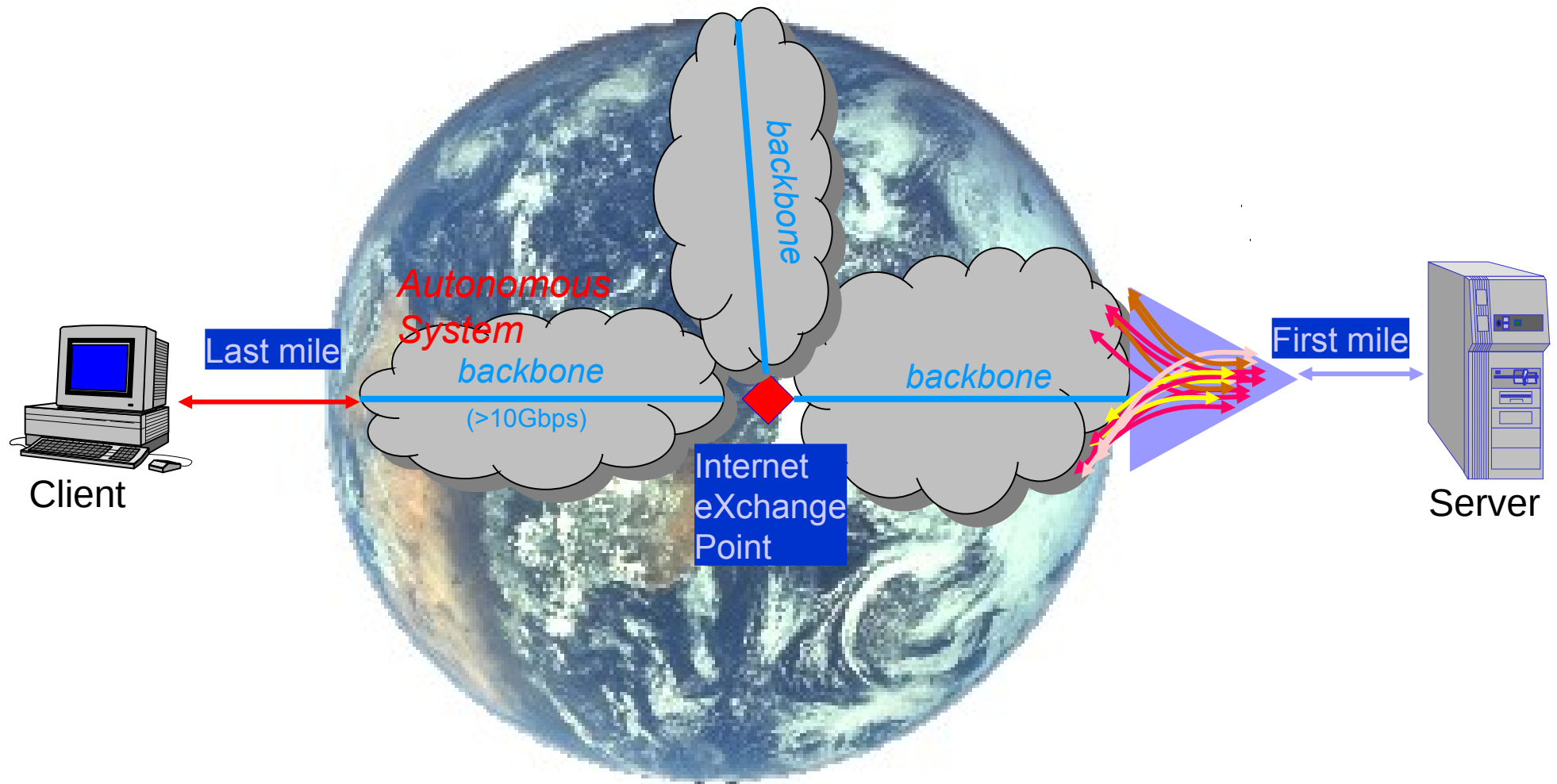
Tecnologia dei centri di interscambio

- **Poiché trasferiscono enormi quantità di traffico Internet, i centri di interscambio sono costituiti da elementi di switching molto potenti e replicati**
- **La tecnologia tipica di un centro di interscambio (peering o IX) consiste di uno o più centri stella ai quali vengono collegati i router dei vari partecipanti → shared switch fabric**
- **Si stabiliscono così dei peering tra i router che consentono agli AS di scambiarsi traffico mediante protocollo BGP [si studierà in seguito]**
- **La tecnologia di switching più utilizzata nei punti di interscambio è passata da ATM a Gigabit Ethernet**

Esempi di architettura di AMS-IX

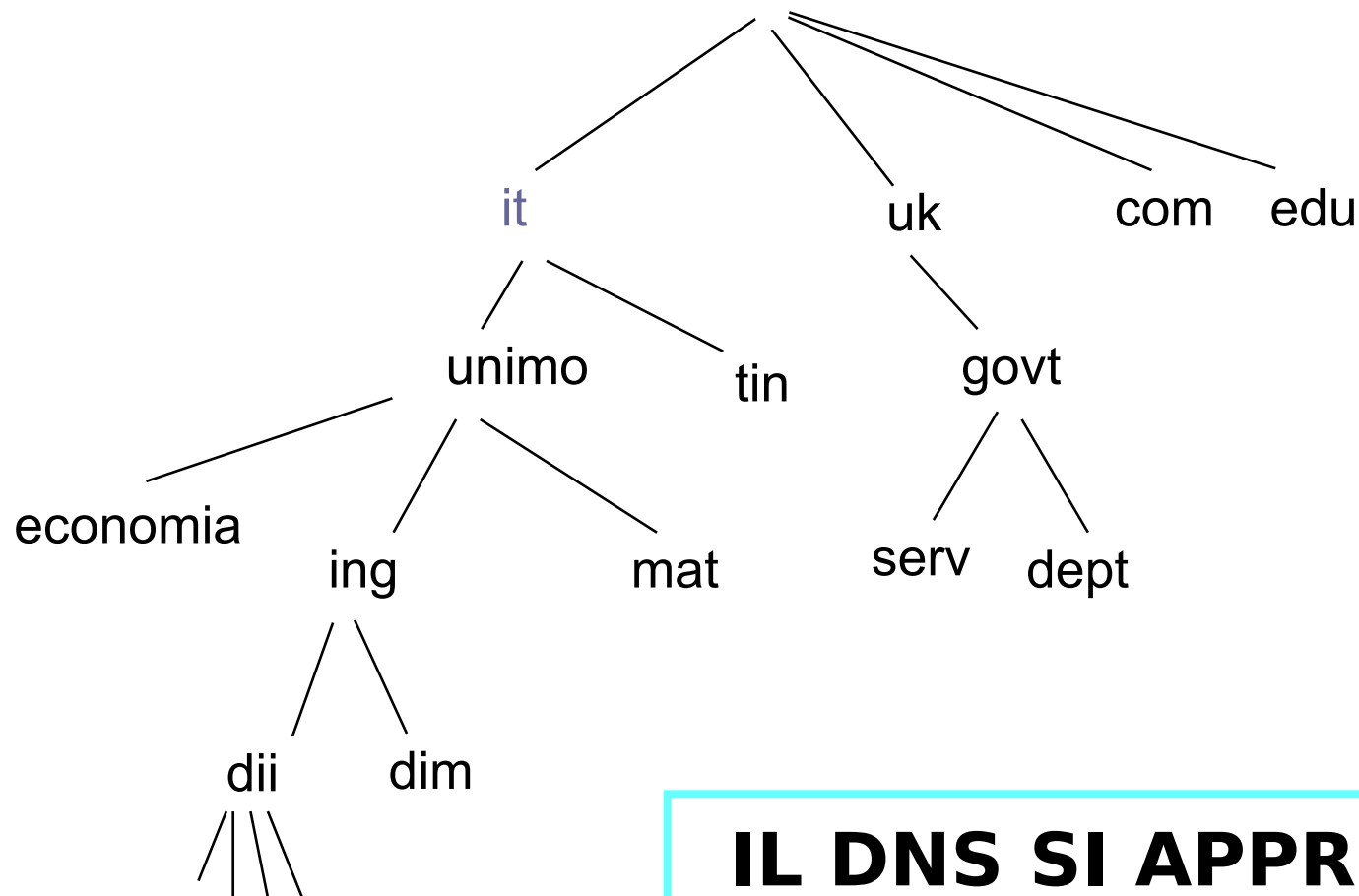


Sintesi: first mile, peering point, last mile



Ma cos'è **INTERNET** (PdV **DNS**)?

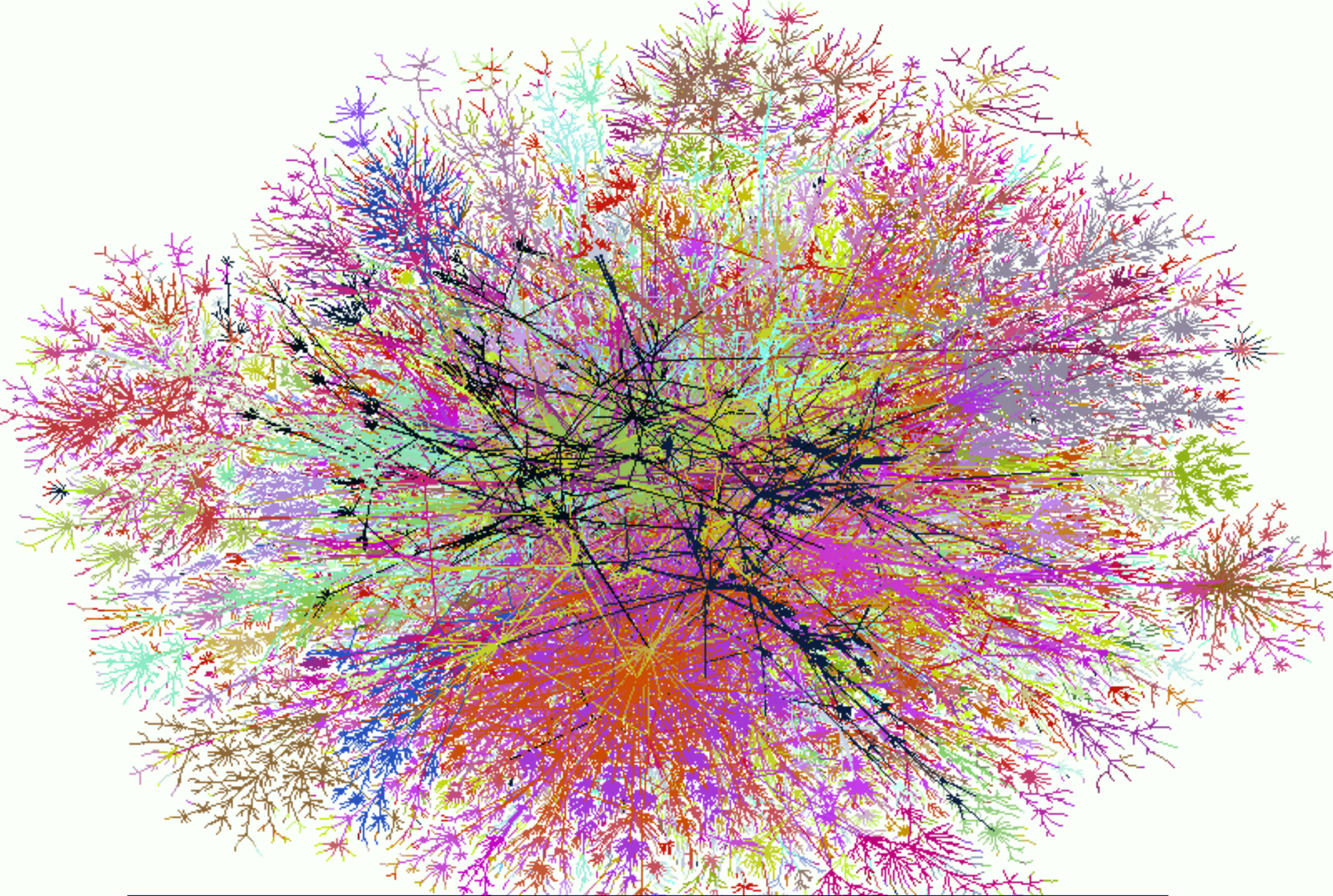
organizzazione gerarchica di nomi e di domini



**IL DNS SI APPROFONDIRA'
IN SEGUITO**

In sintesi: cos'è Internet?

- **DAL PUNTO DI VISTA DELLE APPLICAZIONI DI RETE:**
 - Un'entità trasparente, nella maggior parte dei casi
- **DAL PUNTO DI VISTA “FISICO”:**
 - Un insieme di componenti interne (host, link, router), in cui ciascun nodo è caratterizzato da un indirizzo IP strutturato in 4 byte, es.
158.24.80.57
- **DAL PUNTO DI VISTA ORGANIZZATIVO:**
 - Un insieme di Autonomous Systems (guardando ai router)
 - Un insieme di nomi e domini (guardando agli host)

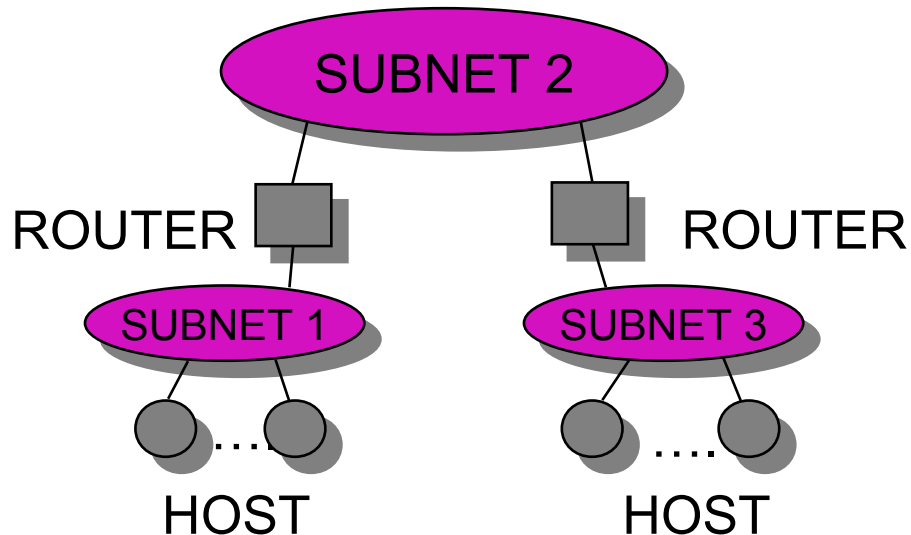


How do IP packets find their way through this mess?

Ricordare i servizi principali del livello IP

- **Indirizzamento univoco degli host**
- **Unità di trasferimento dati**
- **Architettura di Internet**
- **Funzione di routing:**
 - sceglie il percorso nella rete attraverso il quale consegnare i pacchetti
 - consegna i pacchetti da un host a un altro, ma in modo best effort, privo di connessione, e quindi non garantito

Distinguere i due casi fondamentali



Host mittente e destinatario sulla stessa sottorete
(*netid uguali*)

Host mittente e destinatario su sottoreti differenti
(*netid differenti*)

