Fondamenti di Internet e Reti

Antonio Capone, Matteo Cesana,
Ilario Filippini, Guido Maier

POLITECNICO
MILANO 1863

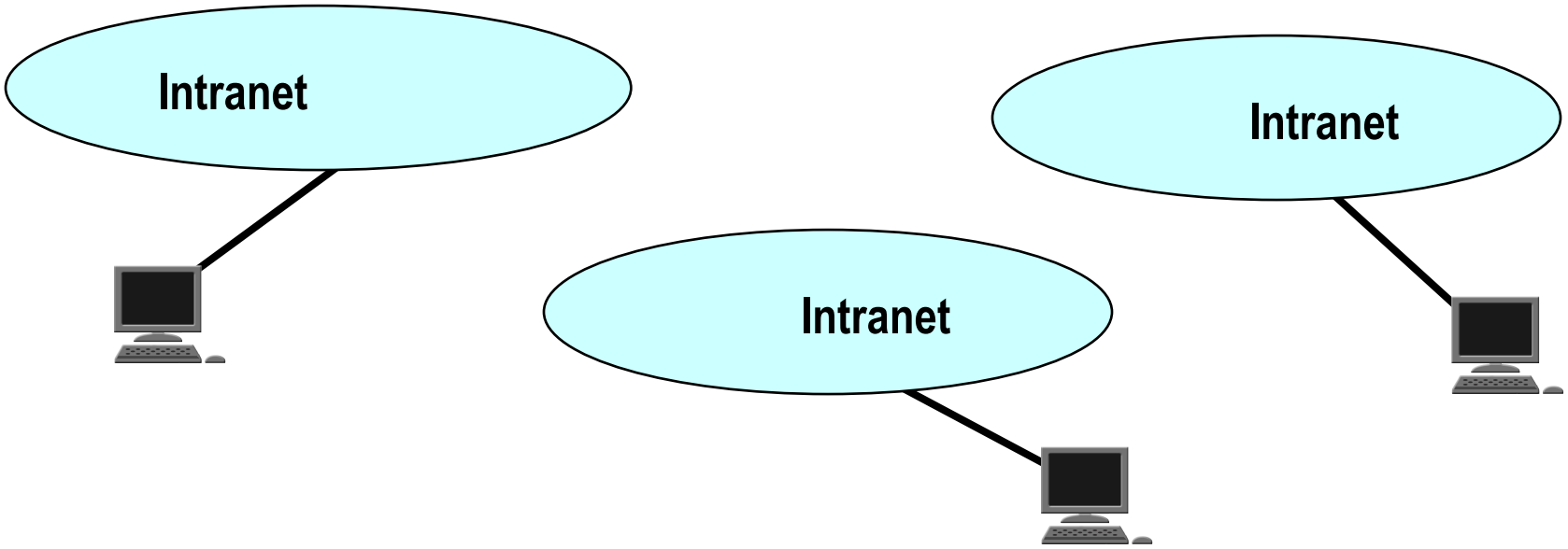
6 – Evoluzioni (VPN, IPv6, MPLS)

Antonio Capone, Matteo Cesana,
Ilario Filippini, Guido Maier

VPN

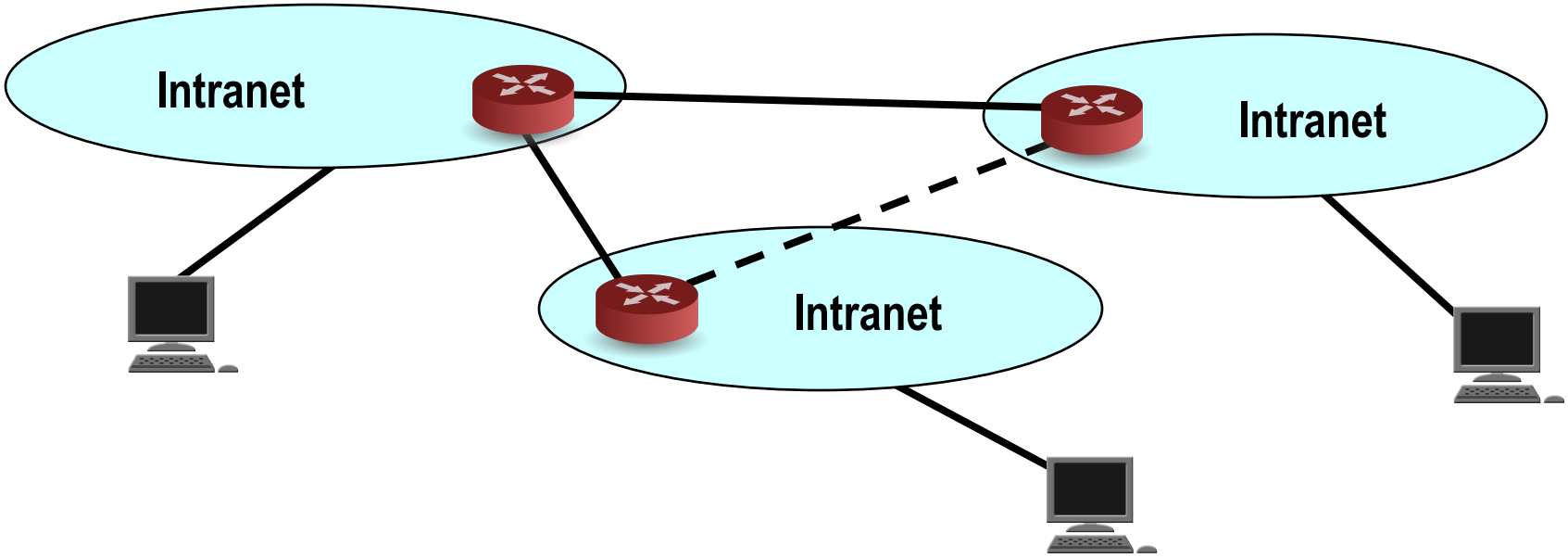
Connessione di intranet remote

- Abbiamo discusso di Intranet e di indirizzamento privato
- Una volta create le Intranet può sorgere il problema di **collegarle tra loro** (ad es. sedi diverse di una stessa azienda)



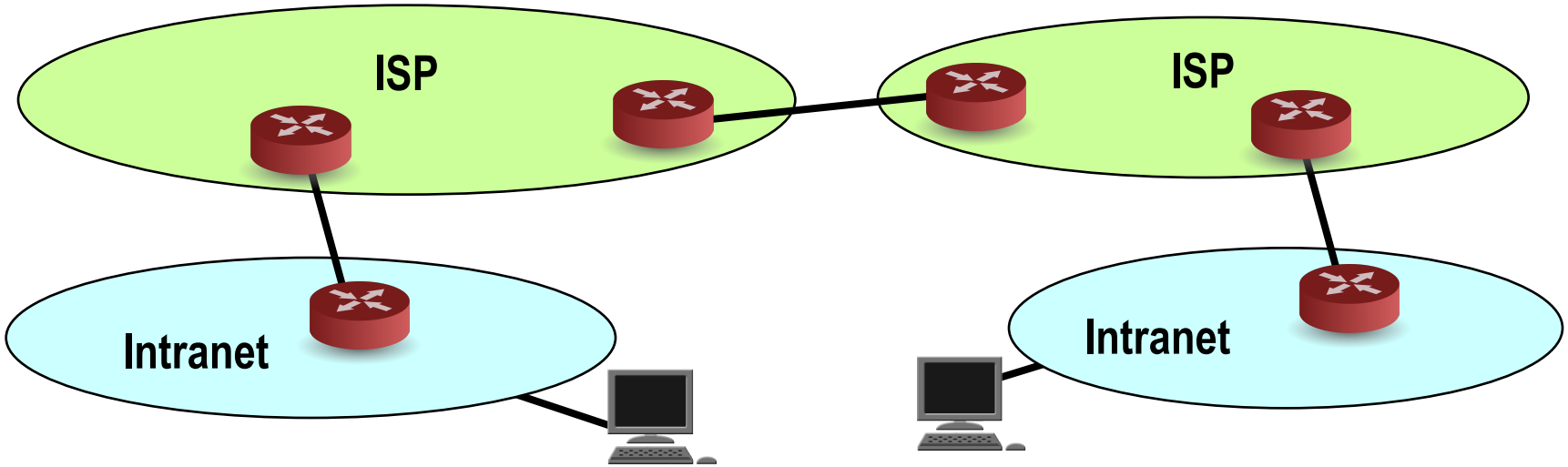
Connessione di intranet remote

- **Possibile soluzione: Uso di canali dedicati**
- **Problemi:**
  - l'uso può non giustificare il costo elevato



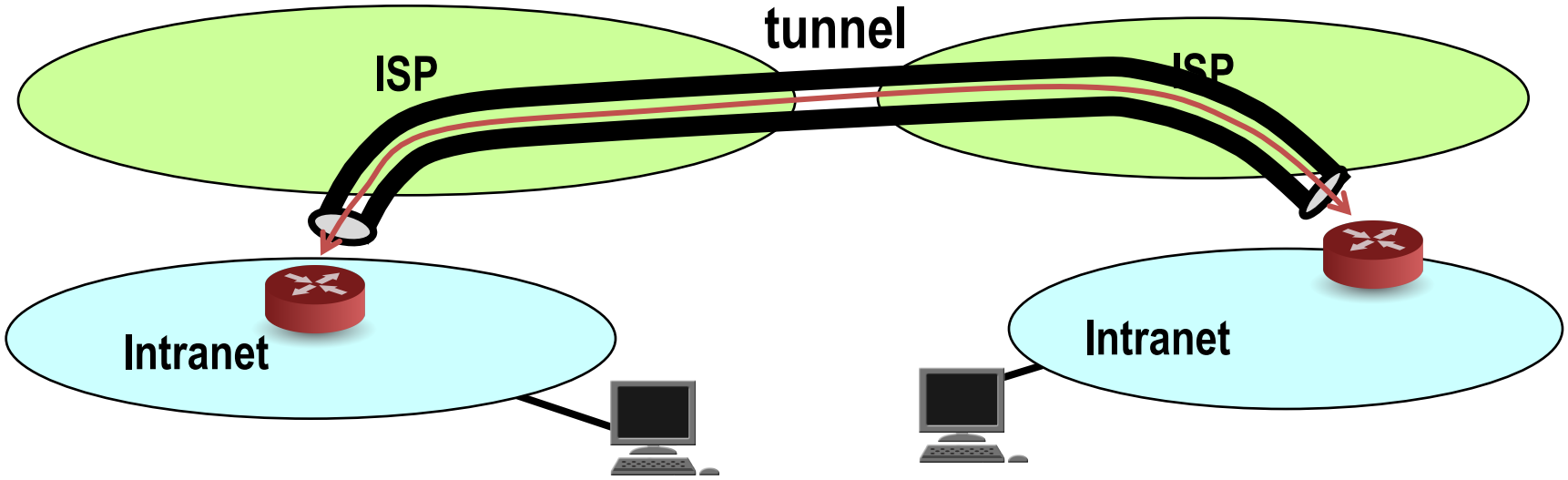
Connessione di intranet remote

- **Uso di INTERNET (Virtual Private Network - VPN)**
- **Problemi:**
  - uso di indirizzi privati
  - sicurezza
  - prestazioni



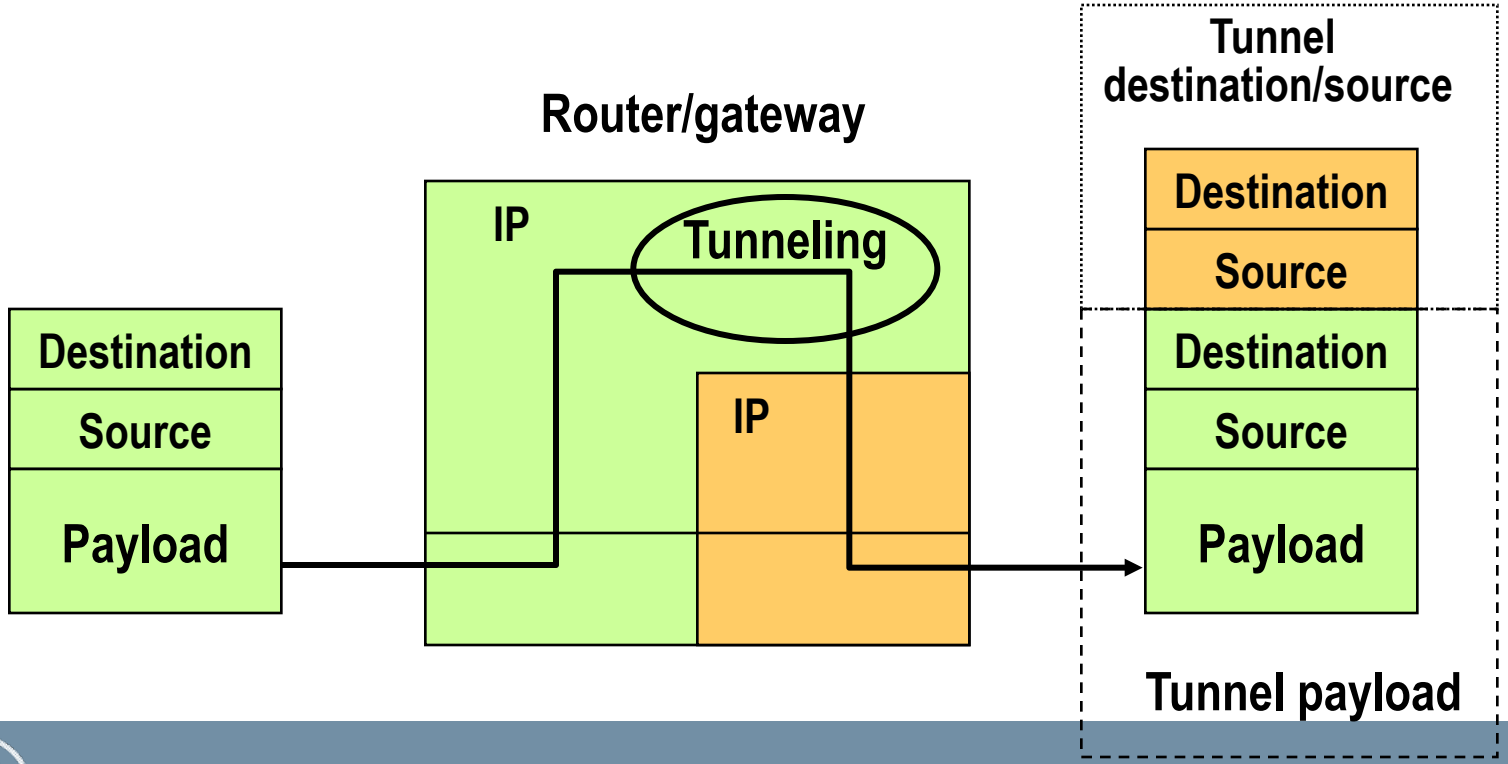
Virtual Private Networks: Tunnel

- **Tunnel di collegamento**

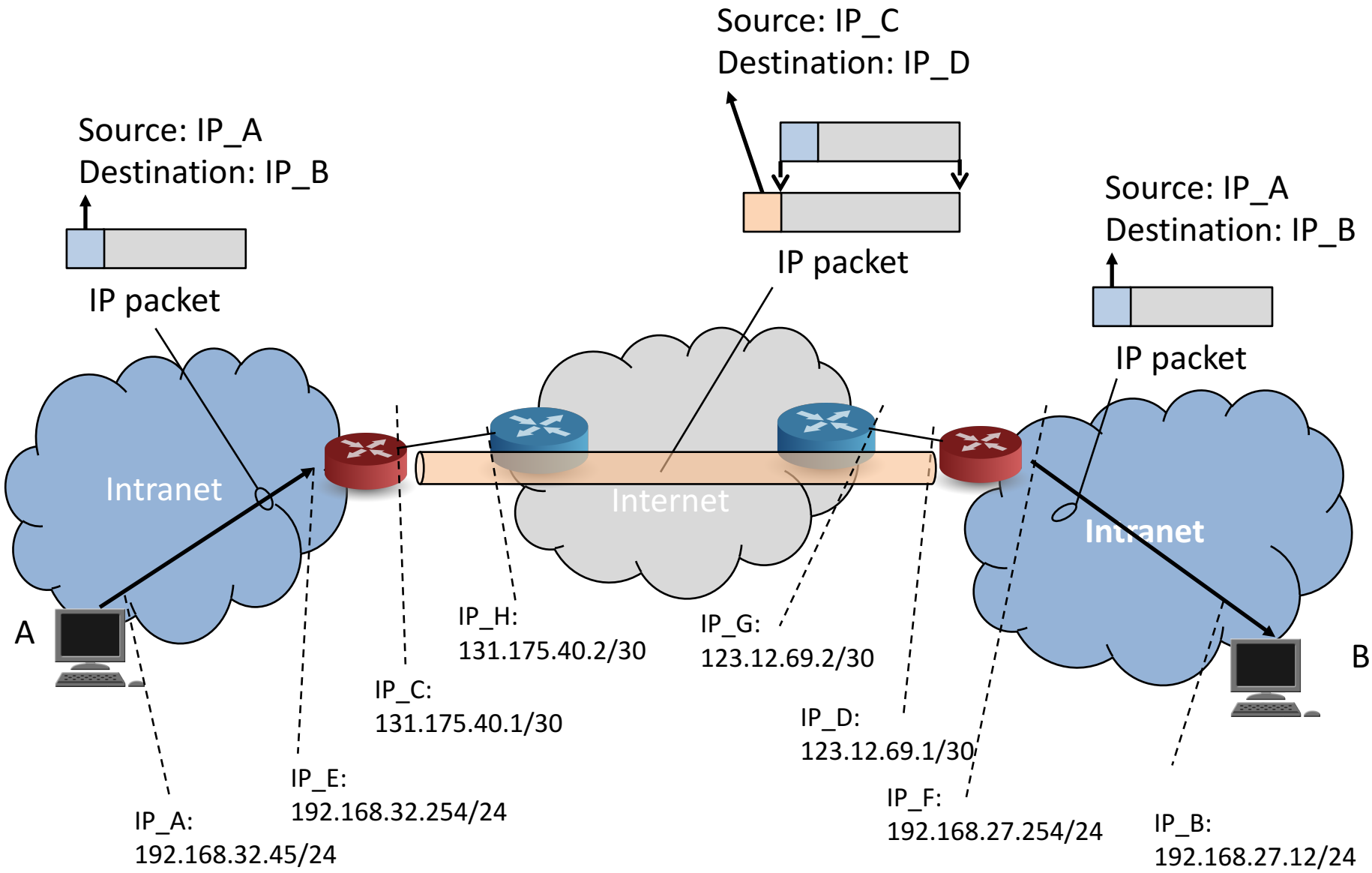


IP tunneling

- Il tunnel si costruisce incapsulando trame IP in altre trame IP
- Il payload che viaggia nel segmento pubblico può essere criptato
- Gli indirizzi A e B possono essere privati



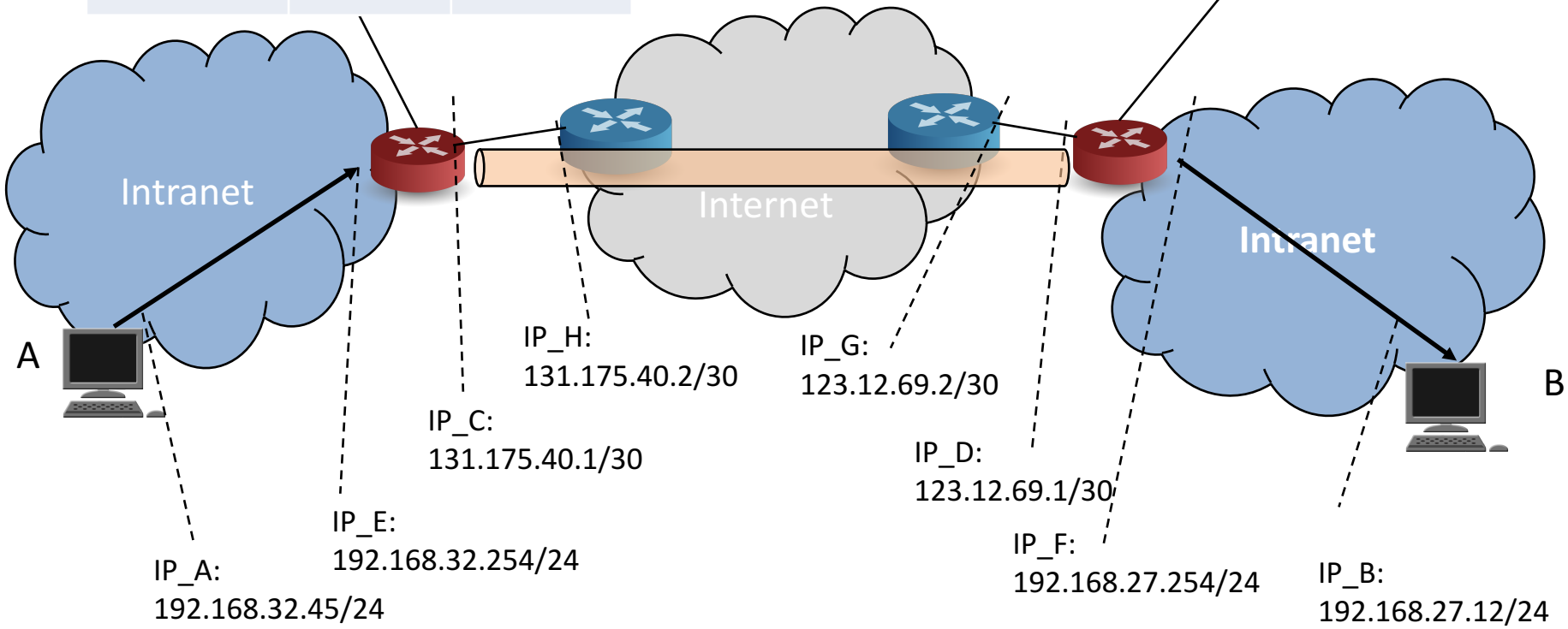
IP tunneling: esempio



IP tunneling: esempio

Network	Next hop	interface
192.168.32.0/24	local	ethernet0
131.175.40.0/30	local	serial0
192.168.27.0/24	123.12.69.1	tunnel0
0.0.0.0/0	131.175.40.2	serial0

Network	Next hop	interface
192.168.27.0/24	local	ethernet0
123.12.69.0/30	local	serial0
192.168.32.0/24	131.175.40.1	tunnel0
0.0.0.0/0	123.12.69.2	serial0



Tunneling & encapsulation

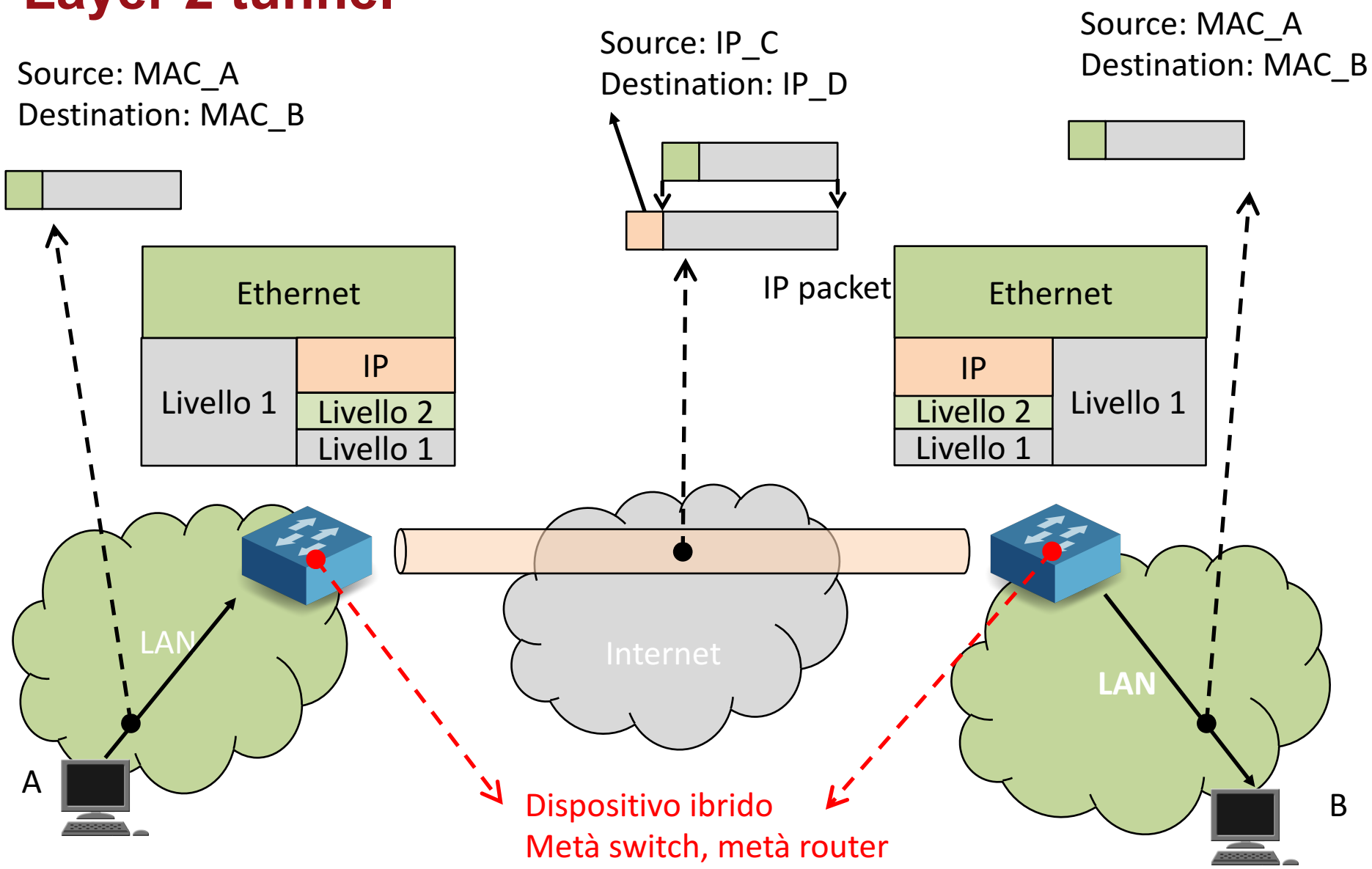
- In realtà però i tunnel sono uno strumento più generale del caso IP-tunneling appena descritto
- Un tunnel è costituito da:
  - **Protocollo passeggero:** è il protocollo che viene trasportato all'interno del tunnel da un estremo all'altro
  - **Protocollo trasportatore:** è il protocollo che trasporta il passeggero
  - **Protocollo di incapsulamento:** è un protocollo supplementare in mezzo tra passeggero e trasportatore
- Il protocollo di incapsulamento svolge funzioni principalmente di sicurezza (autenticazione, cifratura, integrità), ma anche di gestione del tunnel (setup, tear-down)

Passeggeri

- I casi più comuni per il mondo Internet di protocolli passeggeri sono
  - IP (come nell'esempio precedente)
  - Ethernet (Layer 2)

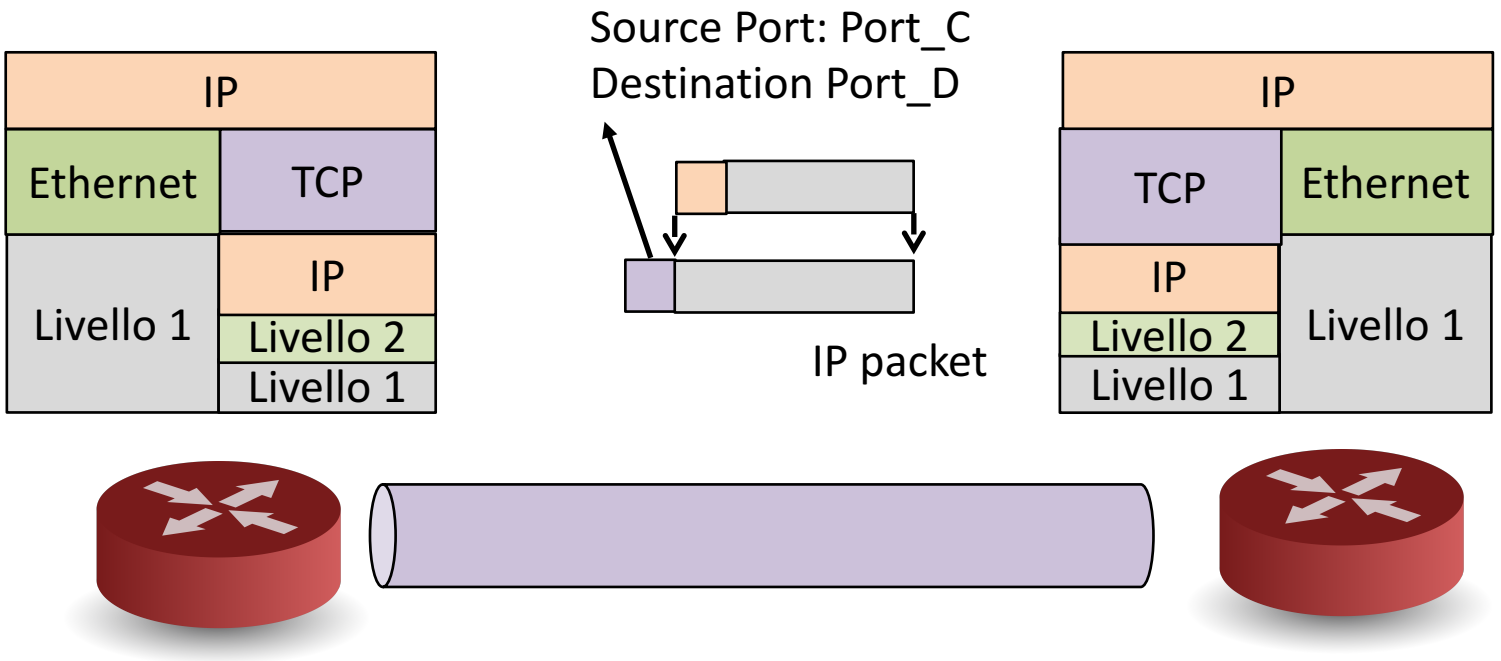
- Nel caso di tunnel di livello 2 (Ethernet) il tunnel si comporta come un collegamento tra due switch ethernet, e la rete diventa un unico dominio di broadcast

Layer 2 tunnel



Trasportatori

- Il protocollo trasportatore può essere IP, ma in alcuni casi anche un protocollo di livello 4 come TCP o UDP

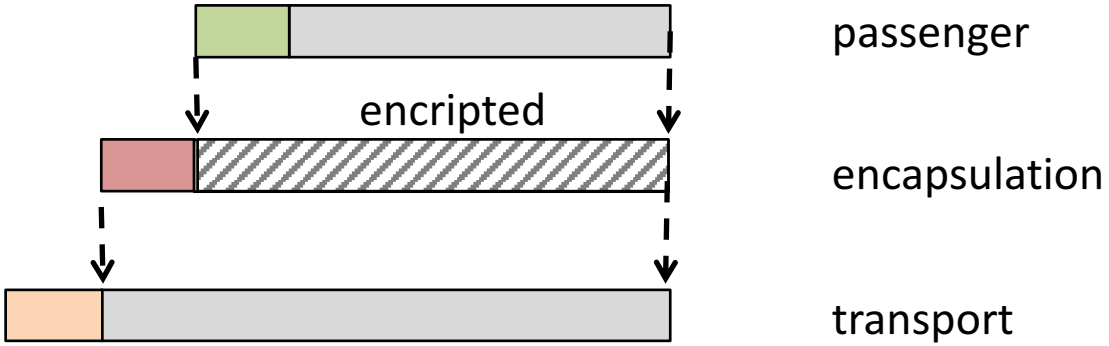


Encapsulation

- Il protocollo di incapsulamento fornisce principalmente servizi di sicurezza e gestione del tunnel
- Tra i pricipali:
  - **IPSec**: IP security protocol
  - **L2TP**: Layer 2 Tunneling Protocol
  - **PPTP**: Point-to-Point Tunneling Protocol
  - **GTP**: GPRS Tunneling Protocol

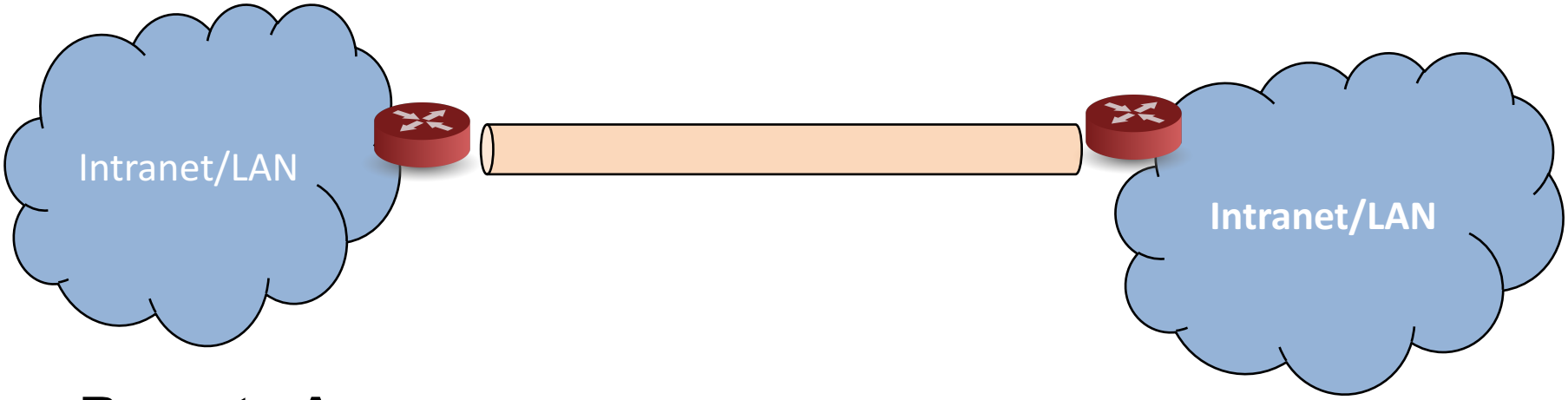
Encapsulation Header:

- Encription
- Autentication
- Integrity

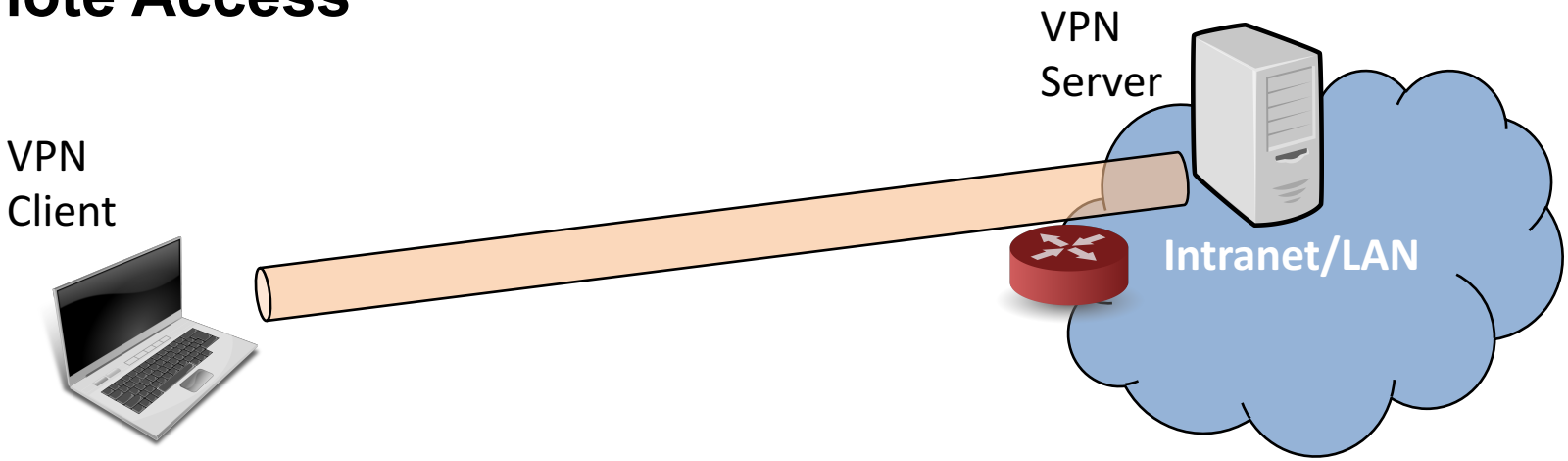


Tipi di VPN

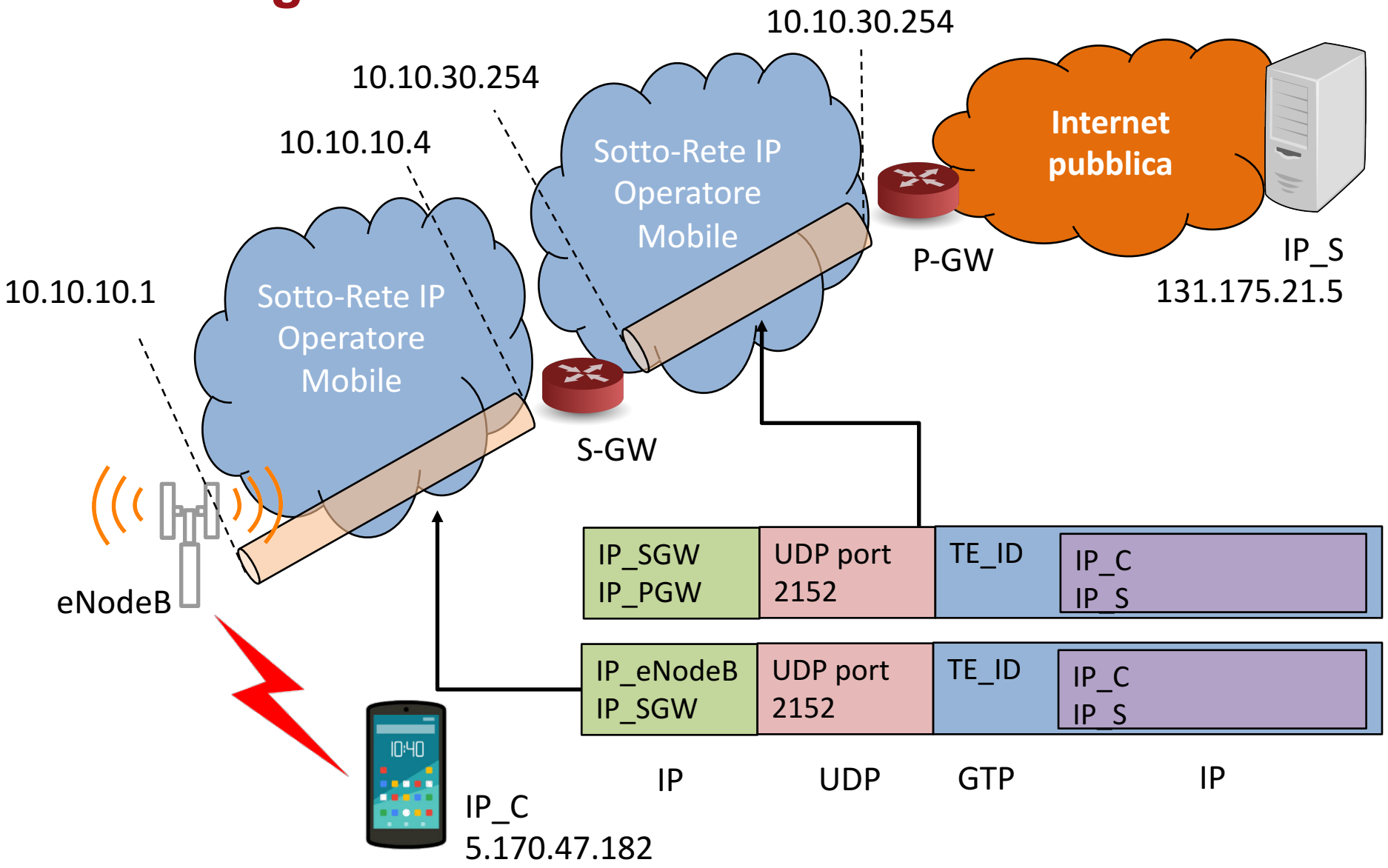
- **Site-to-Site**



- **Remote Access**

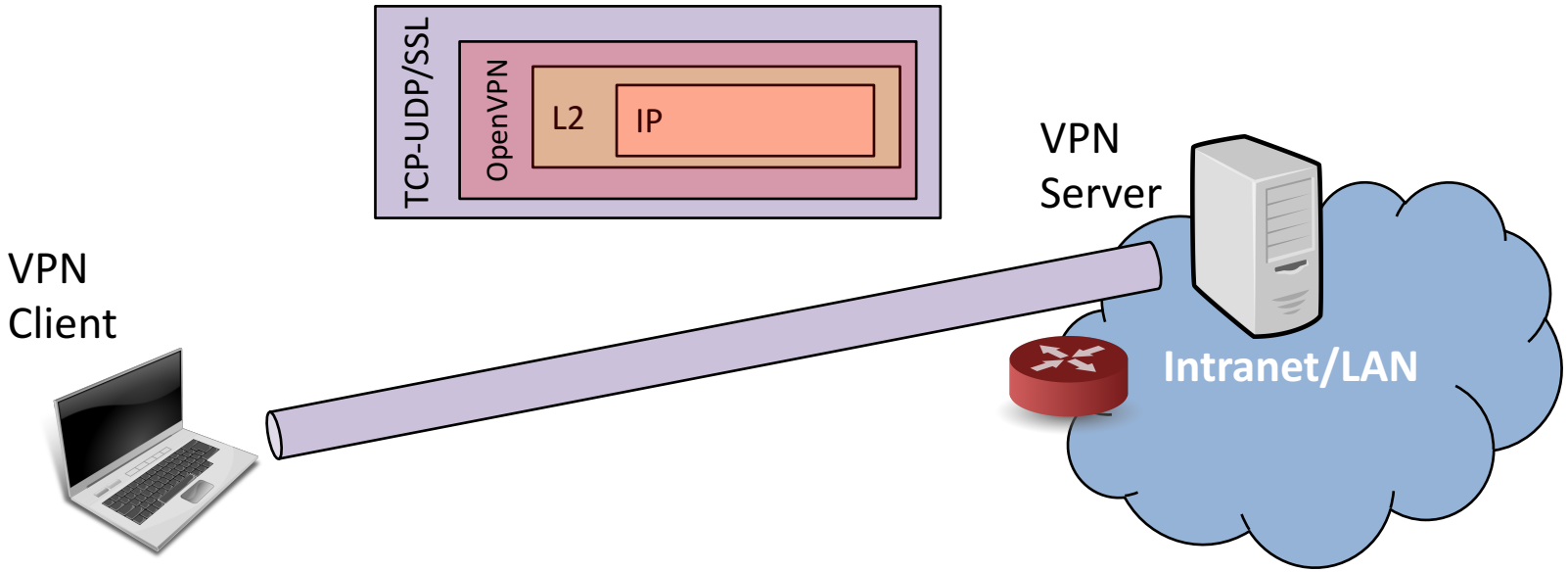


Tunneling nelle reti mobili: GTP



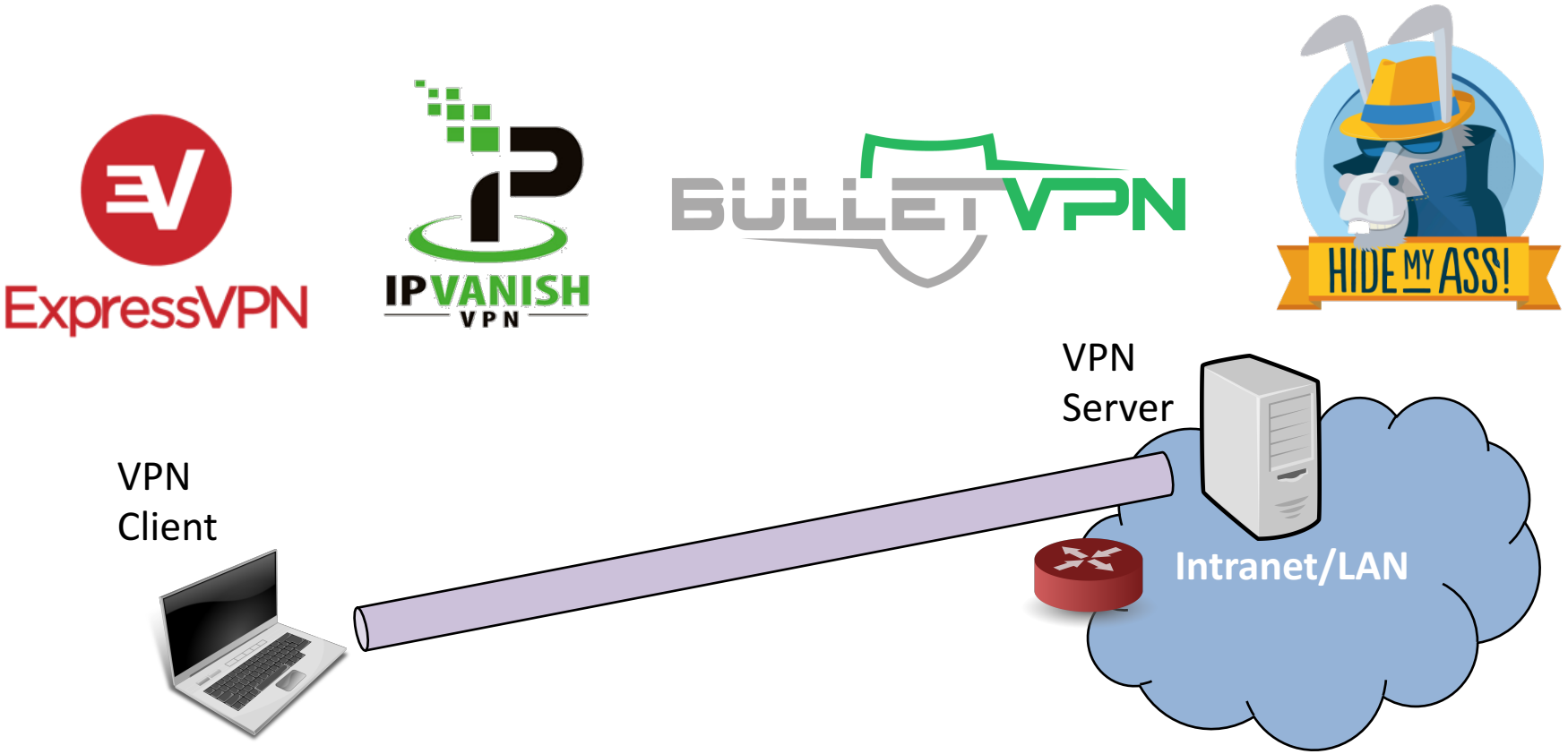
User-space VPN: OpenVPN

- **OpenVPN** è la soluzione più usata per Remote Access VPN
- Trasporta IP (o livello 2) in segmenti TCP o UDP
- Come incapsulamento usa SSL/TLS
- E' anche nota come **User-space VPN** perché di fatto crea una interfaccia virtuale collegandolo allo user-space delle applicazioni dove un interfaccia socket sicura trasporta le trame



Servizi VPN

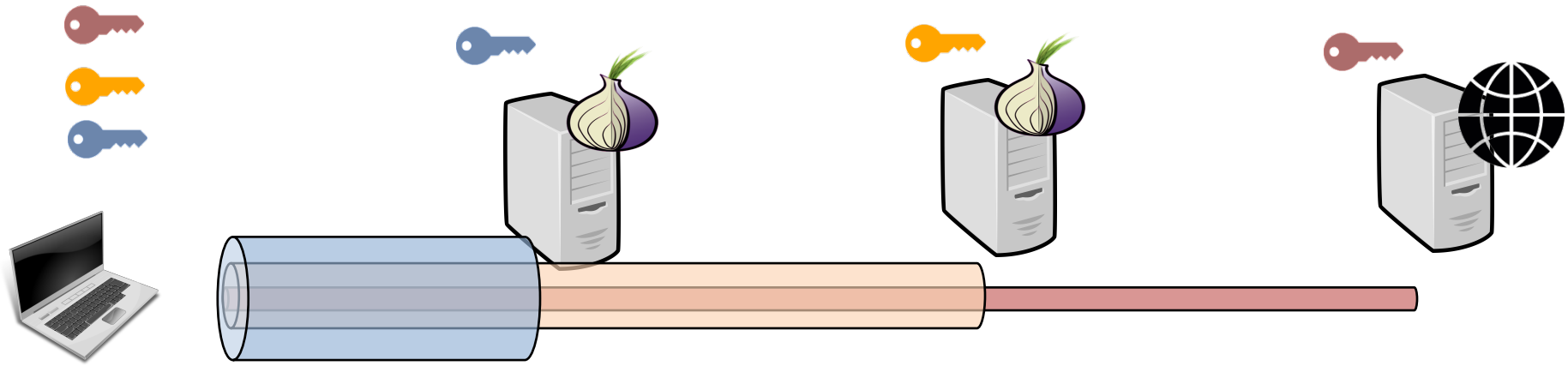
- **OpenVPN** è lanche la soluzione più utilizzata dai servizi VPN offerti da una serie di provider
- L'utilizzo di VPN ha vari obiettivi: evitare il blocco di alcuni servizi in vari paesi, nascondere il proprio indirizzo IP, ecc.



TOR

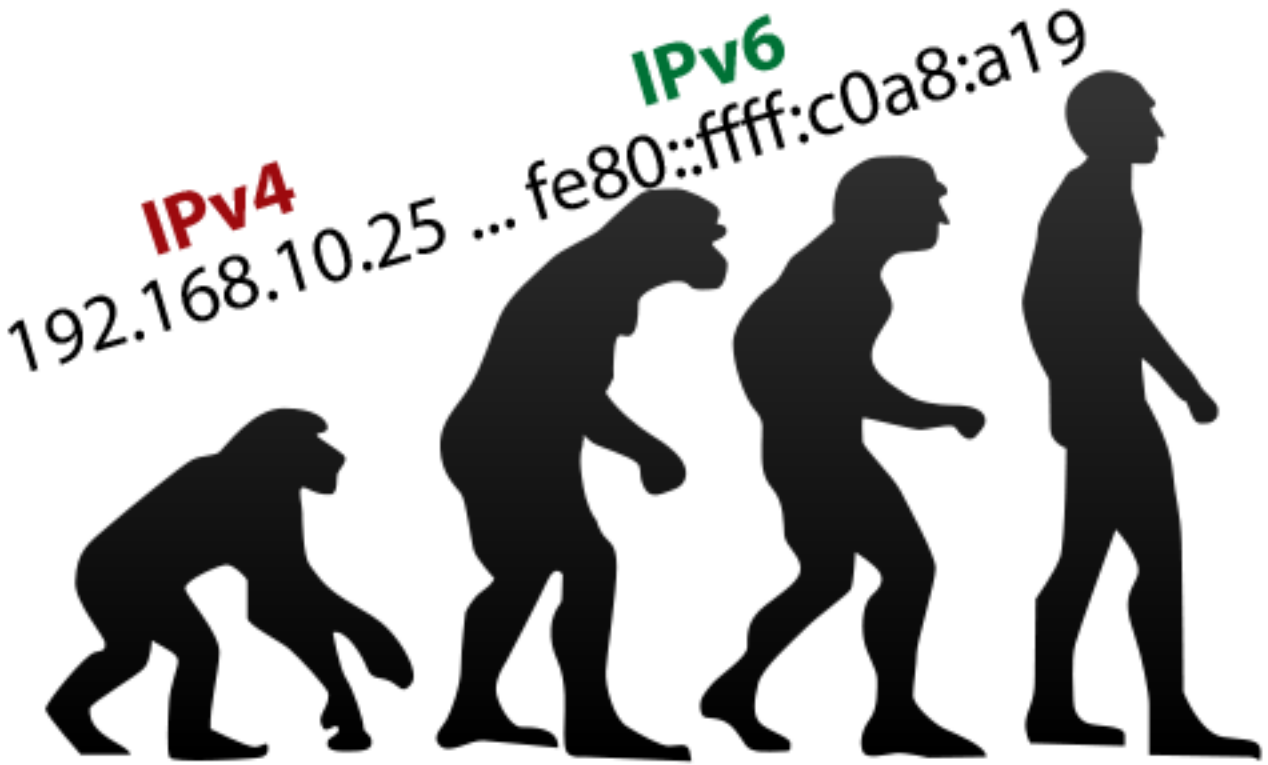
TorProject.org

- **TOR** è la soluzione più nota per la gestione distribuita ed anonima dell'accesso a servizi su internet (e il deep web)
- Utilizza Onion Routing con tunnel innestati, cifrati e anonimizzati

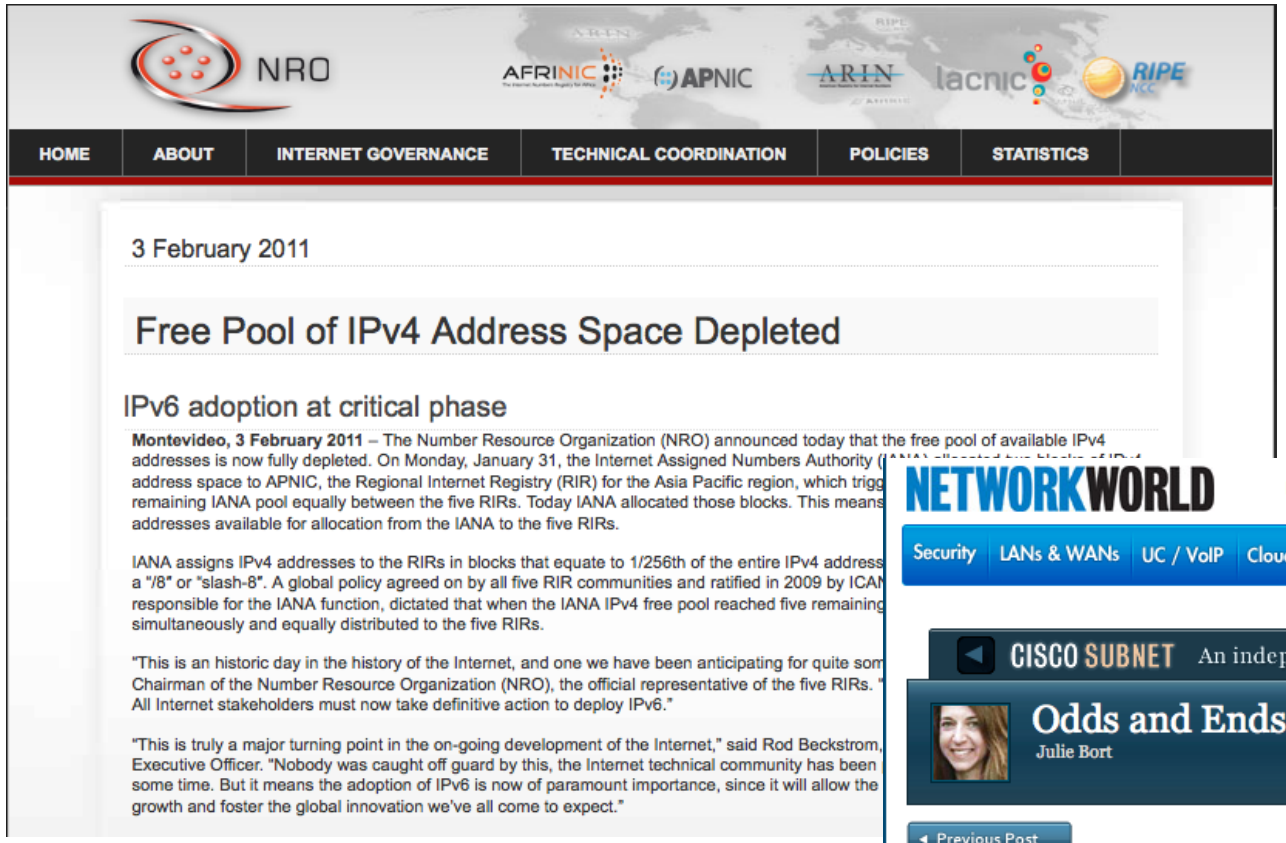


TOR
Client

IPv6



Esaurimento indirizzi IPv4



Esaurimento indirizzi IPv4

RIPE NCC RIPE NETWORK COORDINATION CENTRE

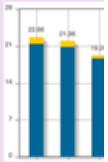
News | Press Centre | Internet Governance | IPv6 | IPv4 Exhaustion | IPv6 Act Now

FAQ: IPv4 and Reaching the last /8 • Information for Press and Media • Reaching the Last /8 • Last /8 Phases

You are here: Home > Internet Coordination > IPv4 Exhaustion

IPv4 Exhaustion

On 14 September 2012, the RIPE NCC began to allocate IPv4 address space from the last /8 of IPv4 address space it holds.

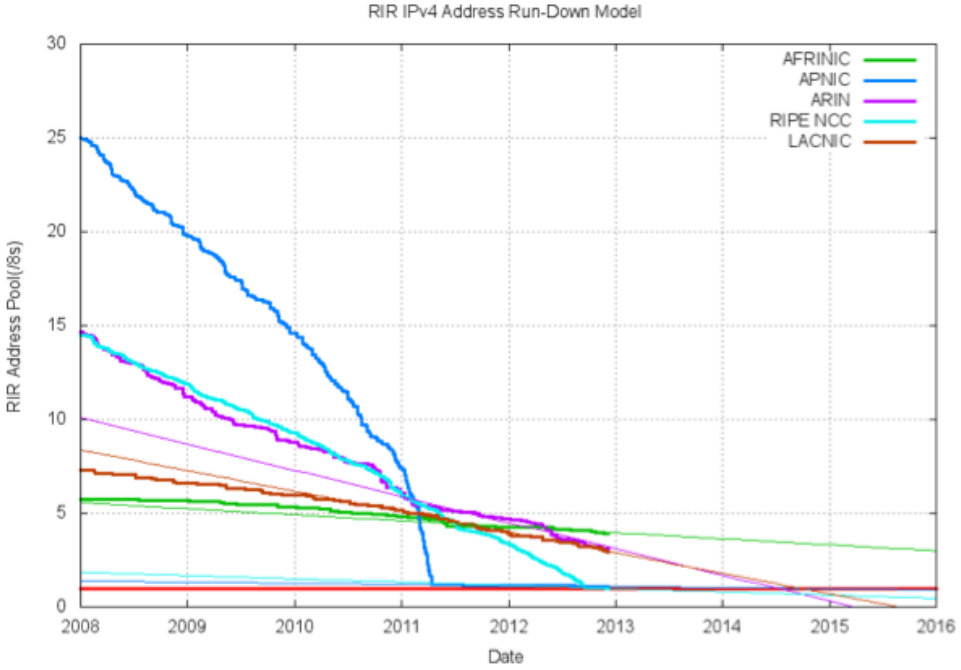


RIPE NCC I

This graph s
addresses ir

What does this mean?

The RIPE NCC now allocates the IPv4 address space it holds according to section 5.6 of "IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region", which states that RIPE NCC members can request a one time /22 allocation (1,024 IPv4 addresses) if they already have an IPv6 allocation. No new IPv4 Provider Independent (PI) space will be assigned.



Projection of consumption of Remaining RIR Address Pools

IPv6

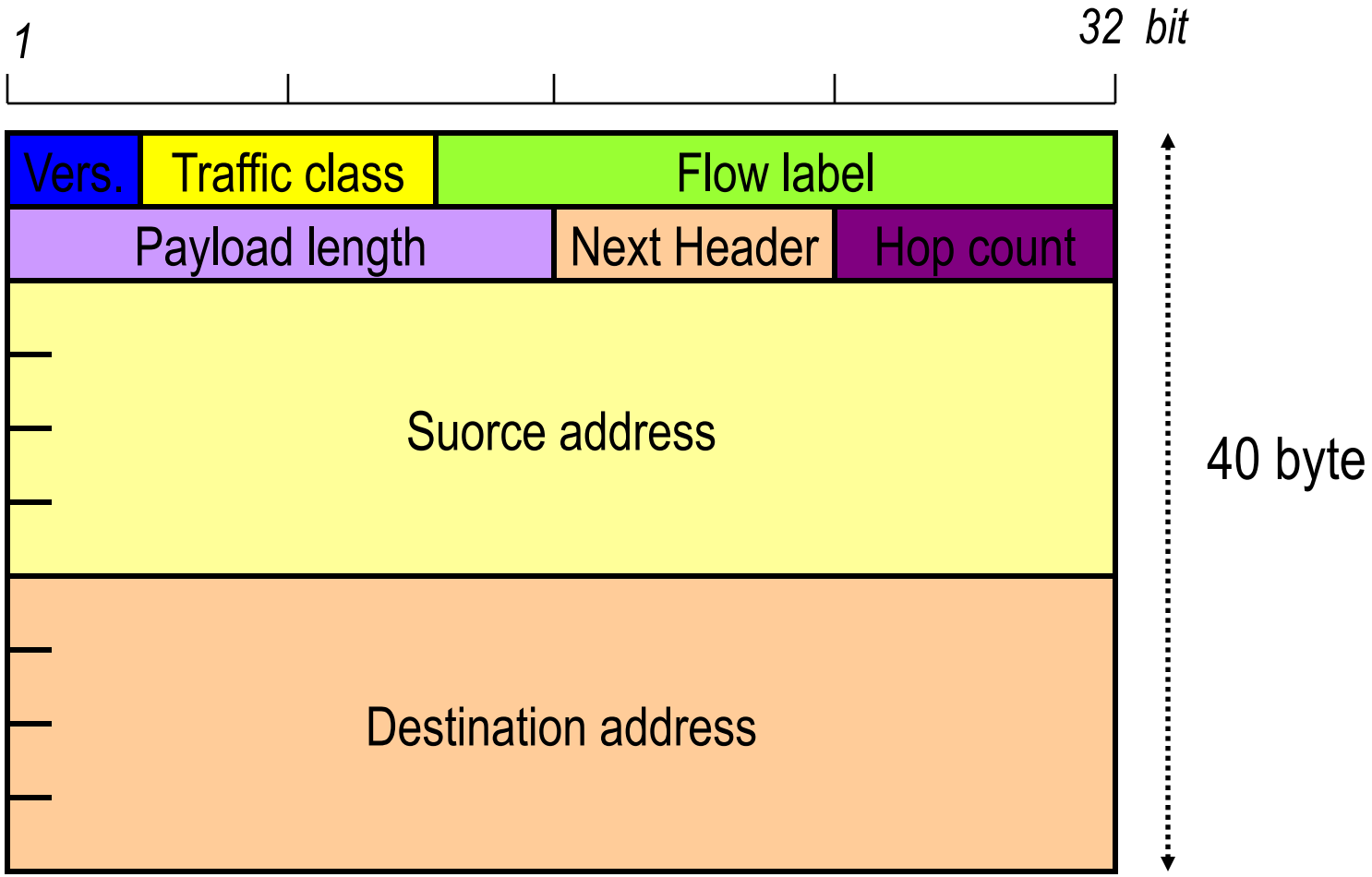
- **IP versione 6 è la nuova versione dell'Internet Protocol il cui processo di standardizzazione è iniziato negli anni '90**
- **Mantiene l'impostazione fondamentale di IPv4 ma cambia molti aspetti**
- **… e soprattutto aumenta la lunghezza degli indirizzi da 32 a 128 bit**

IPv6: le novità principali

- **IPv6**
  - Indirizzi, gestione delle opzioni, gestione della frammentazione, identificazione flussi, classi di traffico, niente header checksum, ecc.
- **ICMPv6:**
  - Nuova versione di ICMP con funzionalità aggiuntive
- **ARP:**
  - Eliminato e sostituito da ICMPv6
- **DHCPv6**
  - Modificato per il nuovo protocollo (alcune funzioni sono svolte da ICMPv6)
- **Routing**
  - RIPng e OSPFv6

Header IPv6

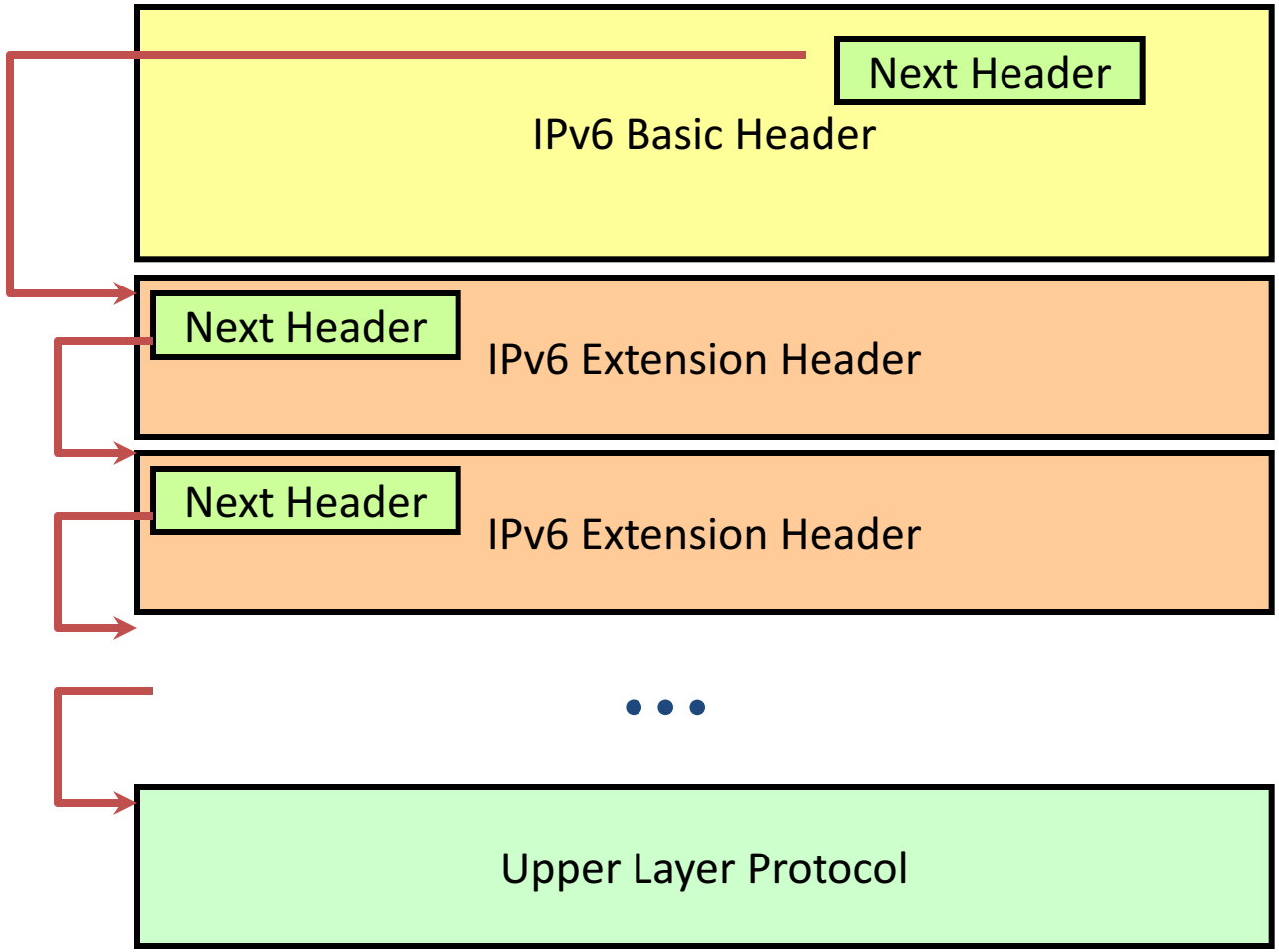
Basic Header



Header IPv6

Campo	Lung. (bit)	Descrizione
Version	***4***	*Versione del Protocollo (6)*
Traffic Class	***8***	*Campo utilizzabile per distinguere diversi tipi di traffico nelle reti Differentiated Services*
Flow Label	***20***	*Campo utilizzabile per identificare un flusso di pacchetti (stessa lunghezza di MPLS)*
Payload Length	***16***	*Lunghezza del pacchetto (eccetto basic header)*
Next Header	***8***	*Identifica il tipo di header che segue il basic header (può essere di livello superiore come TCP o un extension header)*
Hop Limit	***8***	*Stessa funzione del TTL di IPv4*
Source Address	***128***	*Indirizzo di sorgente*
Destination Add	***128***	*Indirizzo di destinazione*

Next Header


Next Header
IPv6 Basic Header
Next Header
IPv6 Extension Header
Next Header
IPv6 Extension Header
Upper Layer Protocol

IPv6 Extension Headers

- **Hop-by-hop option:**
  - deve essere interpretato dai router
  - Ha varie opzioni per pacchetti lunghi e gestione di allineamenti a 32 bit
- **Source Routing:**
  - Serve a obbligare i router a seguire un particolare percorso per il pacchetto
- **Fragmentation:**
  - Implementa la frammentazione, ma questa può essere eseguita solo dal mittente che deve conoscere la massima MTU del path (la ottiene mediante i messaggi di MTU Path discovery di ICMPv6)
- **Autenticazione**
  - Serve per l'autenticazione del mittente
- **Encrypted security payload**
  - Serve per crittare il payload (altro pacchetto IP o livelli superiori)

Indirizzi IPv6

notazioni sintetiche:

- **a gruppi di 2 byte in esadecimale:**

  8000:0000:0000:0000:8965:0678:A45C:87D3

- **gli zeri possono essere omessi:**

  8000::8965:678:A45C:87D3

- **notazione speciale per IPv4**

  ::131.175.21.173

- **numero di indirizzi per metro quadro di superficie terrestre:**

  7×10^{23}

  (maggiore del numero di Avogadro)

Tipi di indirizzi IPv6

- **IPv6 prevede un ricca varietà di indirizzi e assume che normalmente una interfaccia abbia più di un indirizzo associato**
- **Destinatario**
  - Unicast (*uno*)
  - Anycast (*almeno uno di un gruppo*)
  - Multicast (*tutti quelli di un gruppo*)
- **Uso**
  - Globale
  - Locale (stesso link, stesso site)

Prefissi IPv6

- Così come IPv4 anche IPv6 assume i prefissi per una individuazione del campo che identifica l'interfaccia
- La notazione è la stessa (ad. Es. /60)
- I tipi diversi di indirizzi sono individuati dalla prima parte del prefisso (*format prefix - FP*)

Tipi di indirizzi IPv6

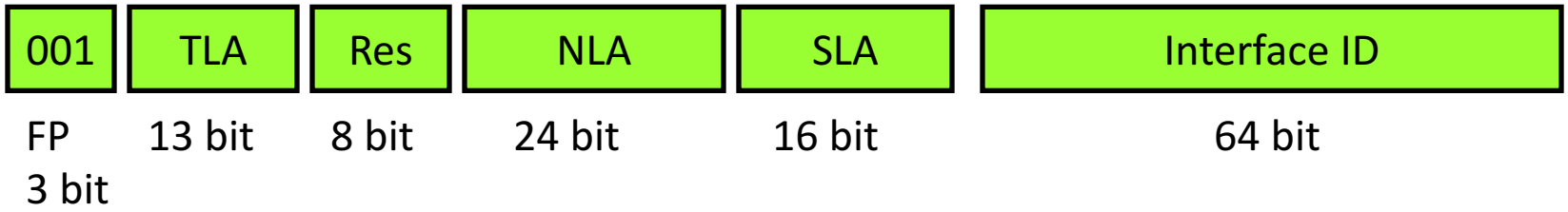
prefix (binary)	usage	fraction
0000 0000	Reserved for IPv4 addresses	1/256
0000 0001	Unassigned	1/256
0000 001	OSI NSAP addresses	1/128
0000 010	Novell Netware IPX addresses	1/128
0000 011	Unassigned	1/128
0000 1	Unassigned	1/32
0001	Unassigned	1/16
001	Aggregatable Global Unicast add.	1/8
010	Unassigned	1/8
011	Unassigned	1/8
100	Unassigned	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1/16
1111 0	Unassigned	1/32
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
1111 1110 0	Unassigned	1/512
1111 1110 10	Link local use addresses	1/1024
1111 1110 11	Site local use addresses	1/1024
1111 1111	Multicast	1/256

Indirizzi speciali

- **Unspecified address (0:0:0:0:0:0:0:0)**
  - Usato come indirizzo di sorgente quando il nodo non conosce altri suoi indirizzi
  - Non può essere usato come indirizzo di destinazione
- **Loopback address (0:0:0:0:0:0:0:1)**
  - Indirizzo di loopback analogo al 127.x.y.z di IPv4
- **IPv4-compatible IPv6 address (::IPv4_addr)**
  - Utilizzato per far comunicare host IPv6 quando occorre attraversare una rete IPv4 (96 zero + 32 bit IPv4_addr)
- **IPv4-mapper IPv6 address (::FFFF:IPv4_addr)**
  - Utilizzati per far comunicare host IPv6 con host IPv4 (80 zero + 16 uno + IPv4_addr)

Aggregatable Global Unicast Address

- Formato unicast globale
- Struttura gerarchica per ridurre i problemi di scalabilità delle tabelle di routing
- 3 macrolivelli: Public Topology, Site Topology, Interface_ID



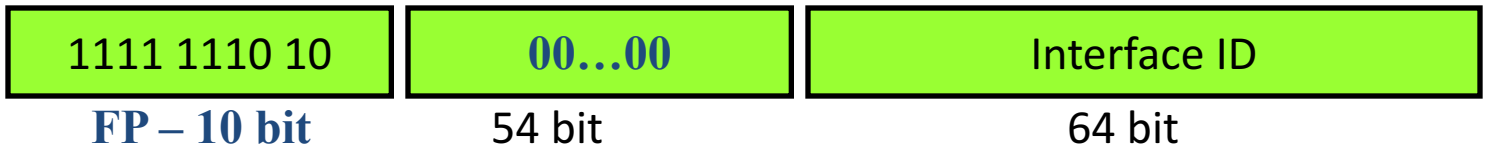
Aggregatable Global Unicast Address

- **TLA (Top Level Aggregation)**
  - *Livello gerarchico più elevato normalmente assegnato su base geografica o agli ISP di backbone*
- **Res (Reserved) – future espansioni**
- **NLA (Next Level Aggregation)**
  - *Ogni ISP con un TLA può strutturare gerarchicamente le sue reti con diversi NLA*
- **SLA (Site Level Aggregation)**
  - *Livello legato al singolo site (sottorete)*
- **Interface ID**
  - *64 bit con formato derivato da IEEE EUI-64*

I livelli NLA e SLA possono essere ulteriormenti divisi gerarchicamente

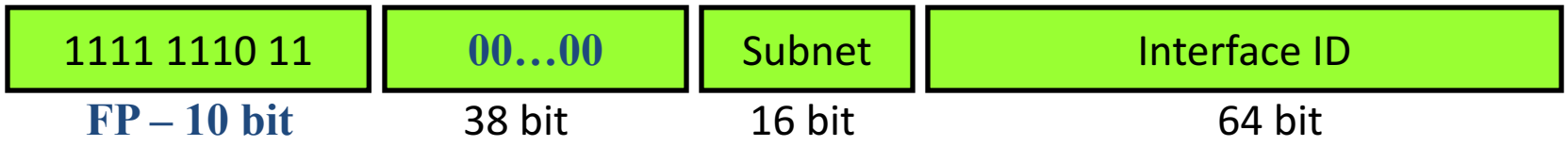
Link-Local Unicast Address

- **FP = 1111 1110 10**
- Sono indirizzi utilizzabili sono per l'indirizzamente su un singolo link (sottorete)
- IPv6 prevede che ogni interfaccia disponga di almeno un link-local unicast address
  - che viene normalmente assegnato per autoconfigurazione a partire dall'indirizzo fisico di interfaccia (IEEE EUI-64)
- Questi indirizzi sono fondamentali nel processo di Neighbor Discovery



Site-Local Unicast Address

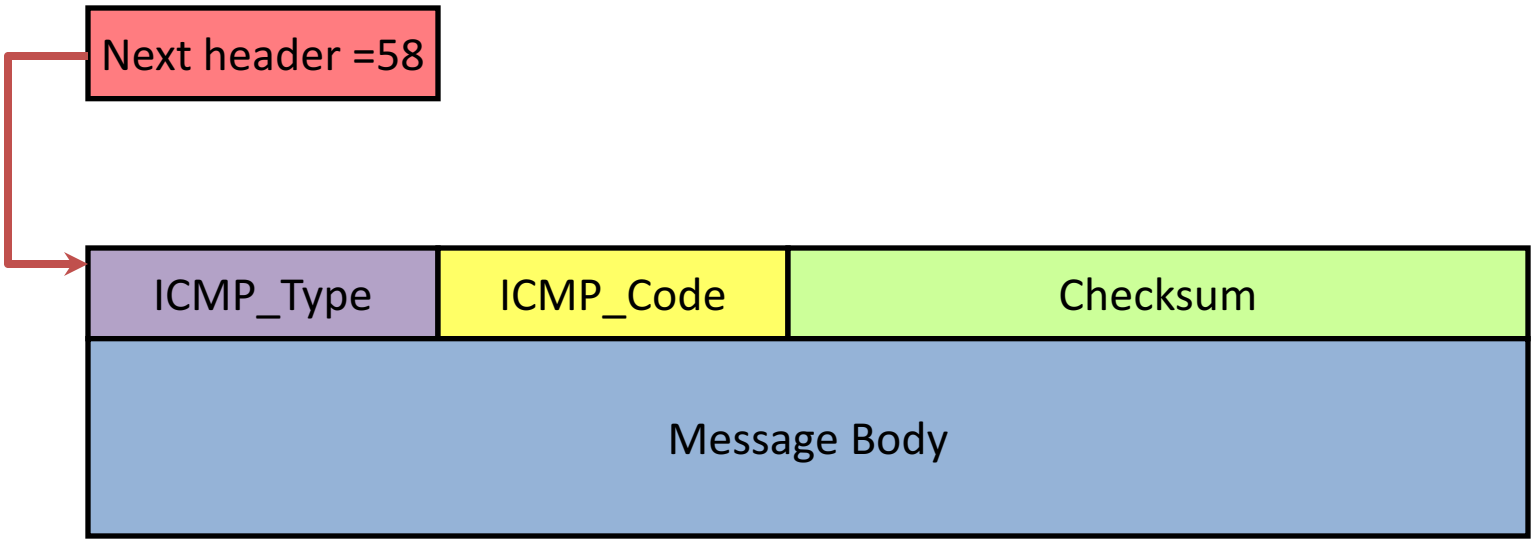
- **FP = 1111 1110 11**
- Anche questi destinati ad uso locale
- Definiscono una spazio di indirizzamento privato



ICMP version 6

- **ICMP ha un importanza molto maggiore con IPv6**
- **Vengono svolte molte funzioni:**
  - Error reporting e diagnostica di rete
  - Risoluzione degli indirizzi di livello link
  - Individuazione del router corretto
  - Controllo degli indirizzi IPv6 assegnati
  - Autoconfigurazione degli indirizzi IPv6
  - Calcolo del PATH-MTU per la frammentazione

ICMPv6: struttura dei messaggi



Alcuni tipi comuni

- **Type=1 – destination unreachable**
- **Type=2 – Packet too big**
- **Type=3 – Time excedeed**
- **Type=4 – Parameter problem,**
- **Type=128 – Echo request**
- **Type=129 – Echo reply**

ICMPv6 Neighbors Discovery

- **Sono previste diverse procedure di *ND***
  - Address Resolution
    - Funzione analoga a quella di ARP per IPv4
  - Router Discovery
    - Segnalare e scoprire presenza di router sul link
  - Redirection
    - Simile all'opzione redirect di IPv4
  - Neighbor Unreachability Detection
    - Scopre irragiungilità di host noti

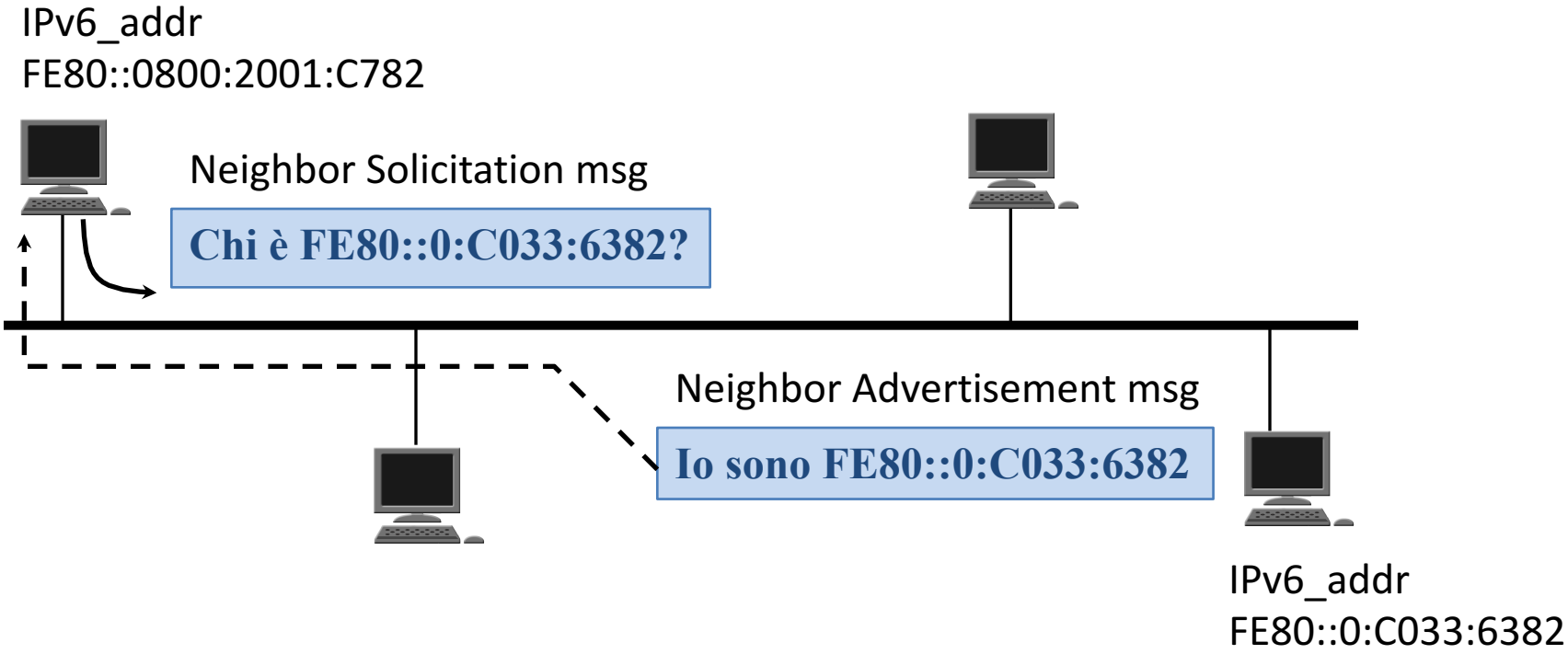
ICMPv6 Neighbor Discovery

- **E sono introdotti 5 nuovi tipi di messaggio:**
  - Router Solicitation message: type=133
  - Router Advertisement message: type=134
  - Neighbor Solicitation message: type=135
  - Neighbor Advertisement message: type=136
  - Redirect message: type=137
- **Sono utilizzati molti indirizzi speciali (link-scope):**
  - All-systems Multicast Address (FF02::1)
  - All-Routers Multicast Address (FF02::1)
  - Solicited-node Multicast Address
  - Unicast Link-Local Address
  - Unspecified Address (0::0)

ICMPv6 Address Resolution

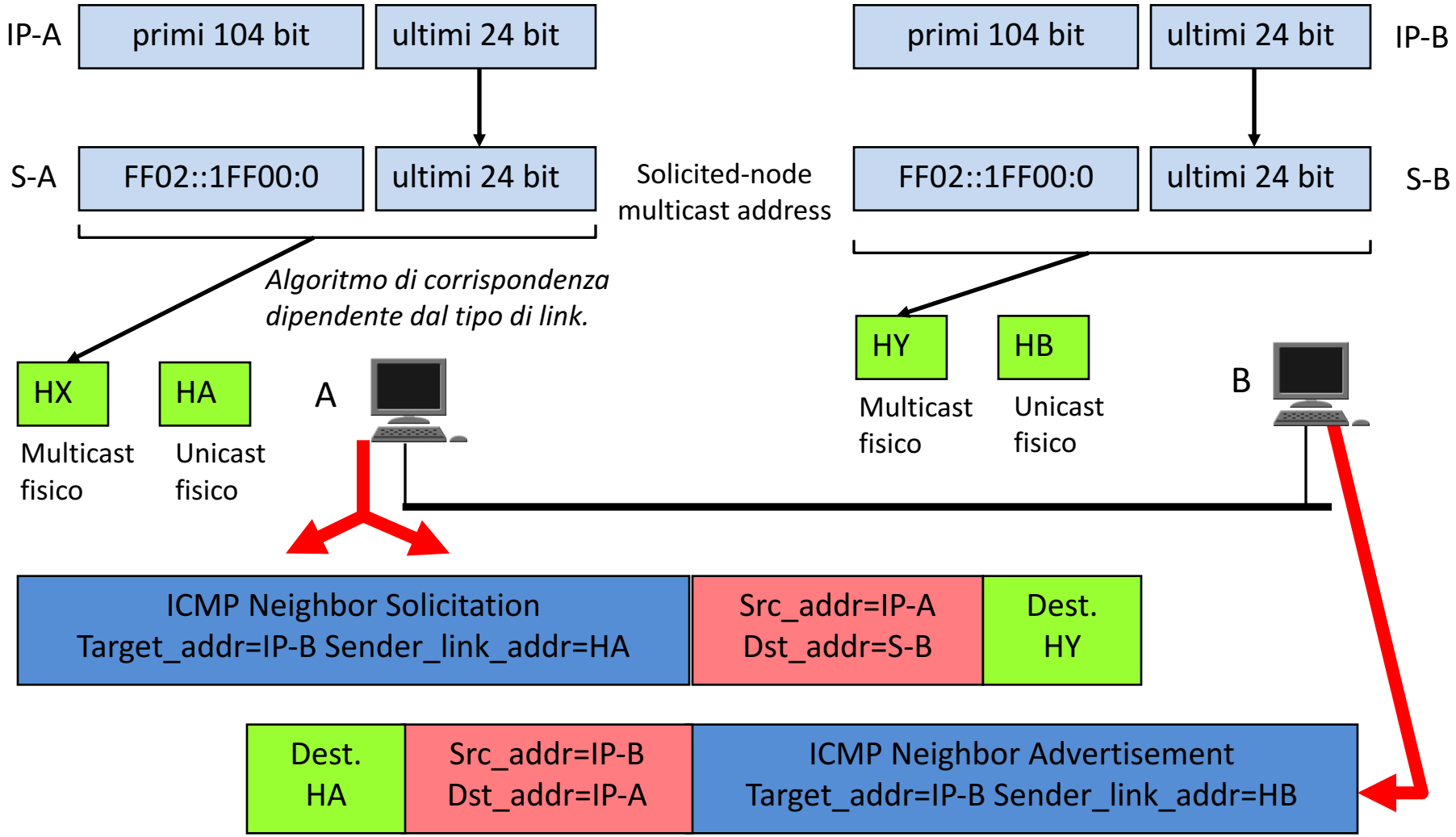
- **Stessa funzione di ARP**
- **Servono indirizzi multicast/broadcast sul livello inferiore**
  - Si suppone l'esistenza di un mappaggio tra indirizzi multicast IPv6 e multicast/broadcast a livello link
- **Si fa uso dei messaggi di "Neighbor Solicitation" e Neighbor Advertisement"**

ICMPv6 Address Resolution

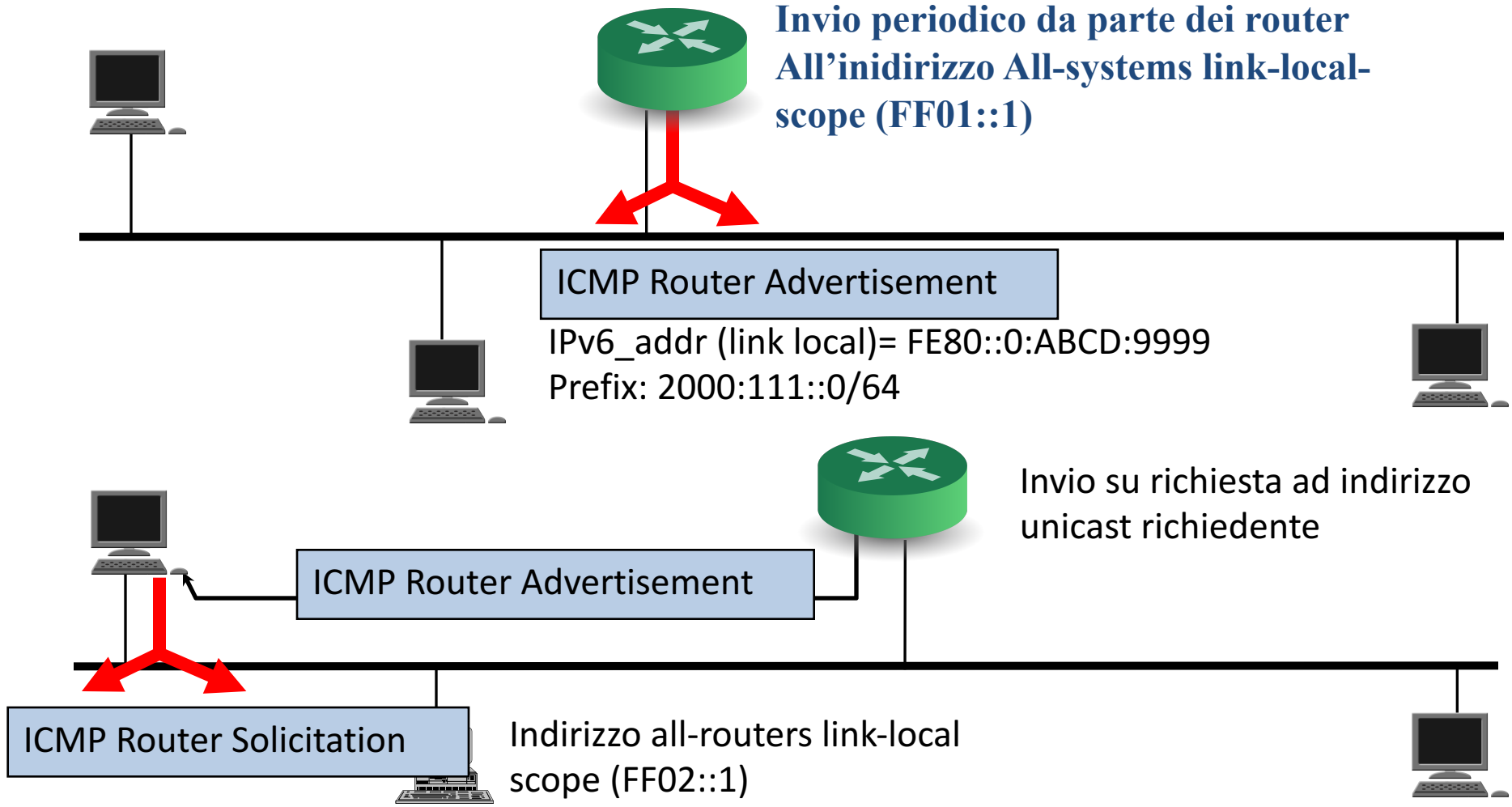


- Il messaggio di ***Neighbor Solicitation*** viene inviato all'indirizzo node-solicited multicast address che può essere ricavato anche dal richiedente
- Il messaggio di ***Neighbor Advertisement*** viene inviato all'indirizzo IPv6 di sorgente del pacchetto di richiesta

ICMPv6 Address Resolution



Router Discovery



Autoconfigurazione Indirizzi

- **Oltre agli indirizzi Link-local si possono autoconfigurare indirizzi globali**
  - Stateful configuration (tramite DHCPv6)
  - Stateless configuration (tramite ICMP)
    - Noto il prefisso annunciato dai router
    - Si può ricavare l'indirizzi a partire dall'indirizzo fisico a 64 bit

MTU Path Discovery

- Il mittente deve sapere la MTU più piccola sul percorso
- Invia 1 pacchetto con pacchetto lungo quanto MTU primo link
- Se arriva messaggio ICMP errore “Packet too big” ridurre MTU
- Fino a che non arrivano più messaggi di errore

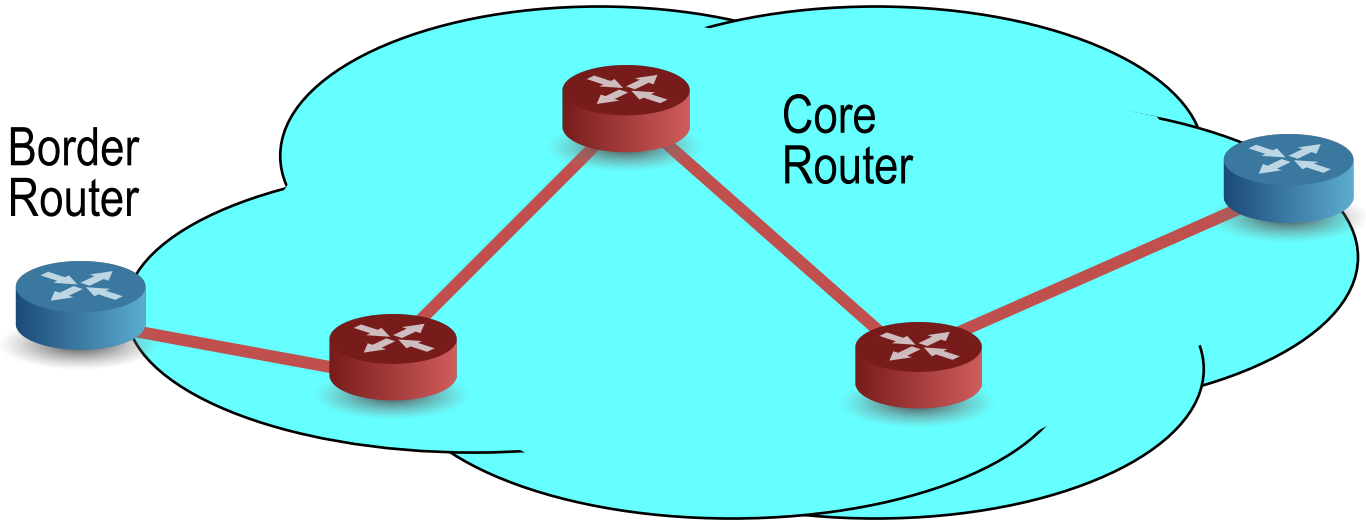
Migrazione IPv4 – IPv6

- **Si basa sull'uso di queste conponenti:**
  - Dual stack:
    - Sistemi con doppio stack IPv4 e IPv6
  - Tunneling:
    - Attraversamento di porzioni di rete IPv4 mediante tunneling
  - Header translation:
    - Traduzione degli header dei due formati

MPLS
Multi Protocol Label Switching

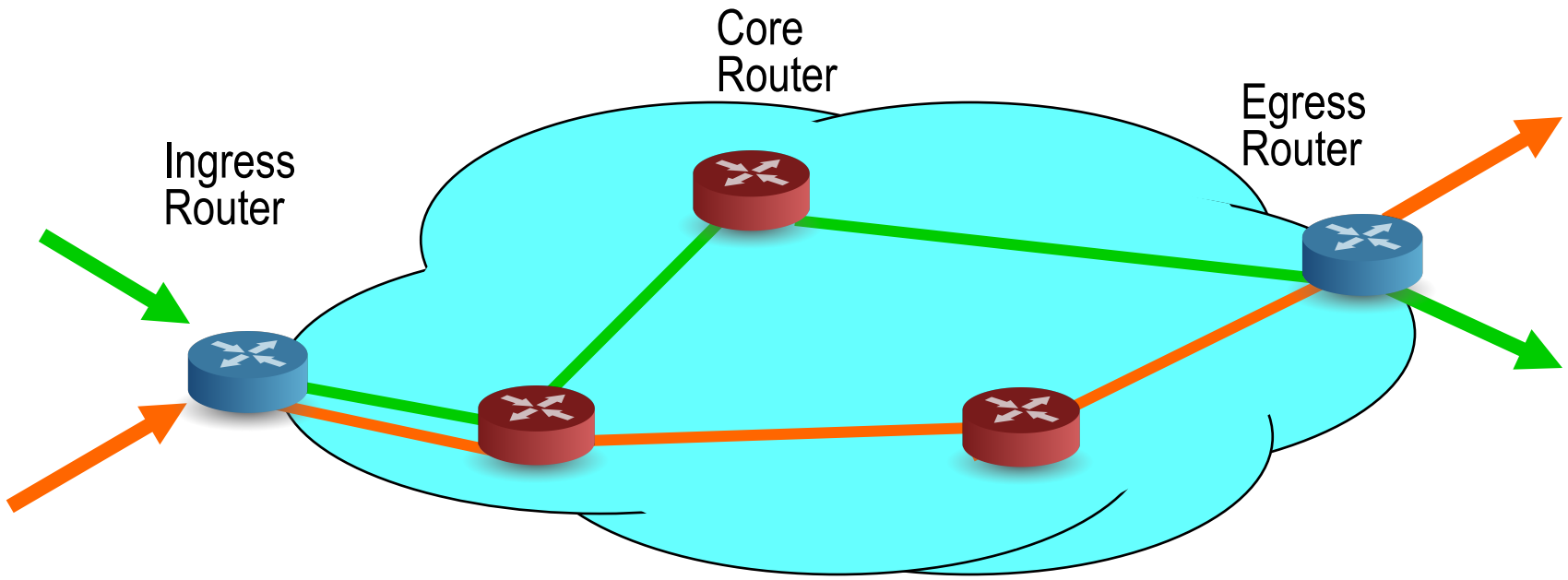
Architettura Generale

- **Trasporta pacchetti IP (tunnel MPLS)**
- **Gestisce inoltro mediante circuiti virtuali**
- **che sono:**
  - predeterminati dal gestore o su
  - richiesta esplicita degli utenti
  - meccanismo di “set up”
  - prenotazione di risorse



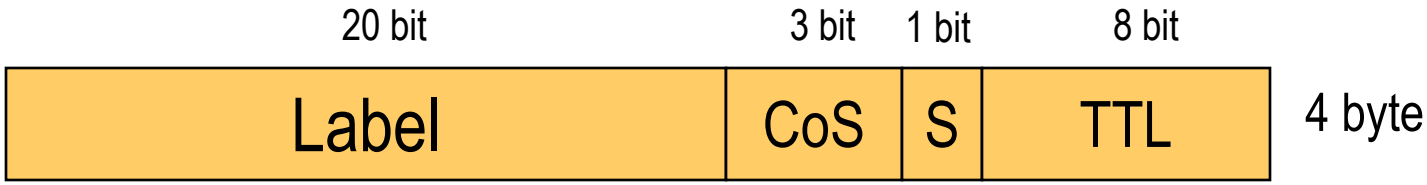
Architettura generale

- E' possibile ottimizzare l'instradamento dei flussi in base a meccanismi statici o dinamici
- E' possibile instradare in base a un ricco set di parametri (sorgenti, porte, applicazioni) in aggiunta alla destinazione



LS Forwarding

- IP è incapsulato in un LS header



- ***CoS**: Class of Service*
- ***S**: Stack (consente l'uso in cascata di più header)*
- ***TTL**: Time To Live*

LS Forwarding

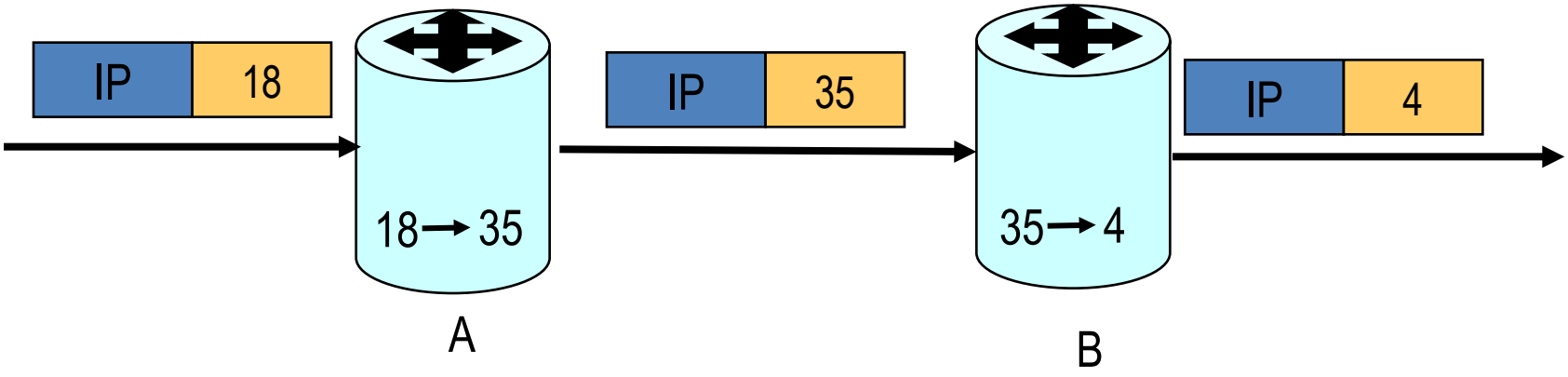
- La Label è usata per commutare - Label Swapping (circuito virtuale)

In Interface	In Label	Out Interface	Out Label
.....	.....	.....	.....
3	21	4	18
3	56	6	135
.....	.....	.....	.....

- La label ha significato locale

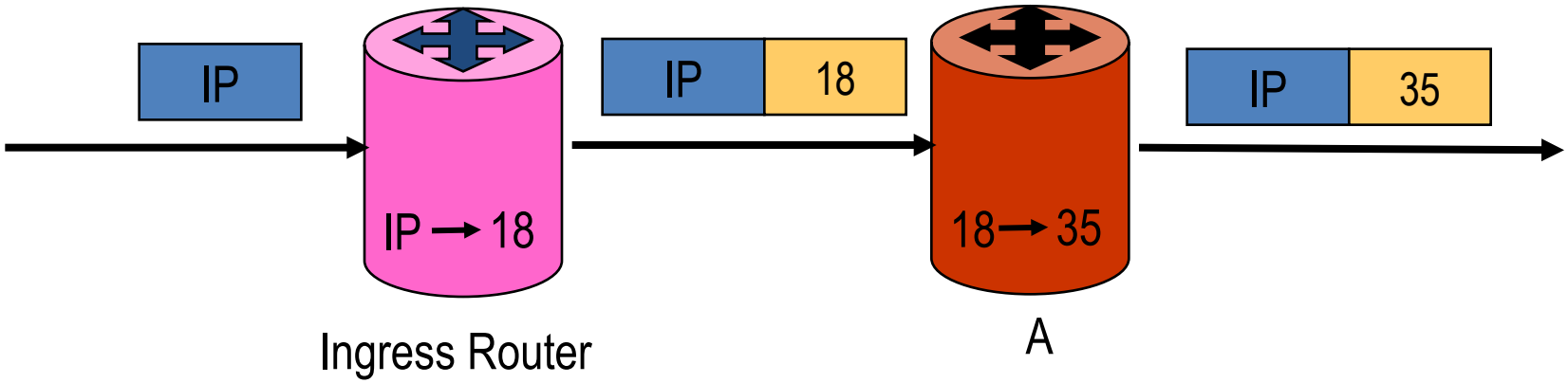
LS Forwarding

- Le Label vengono determinate e “cucite” insieme al momento del set up del cammino

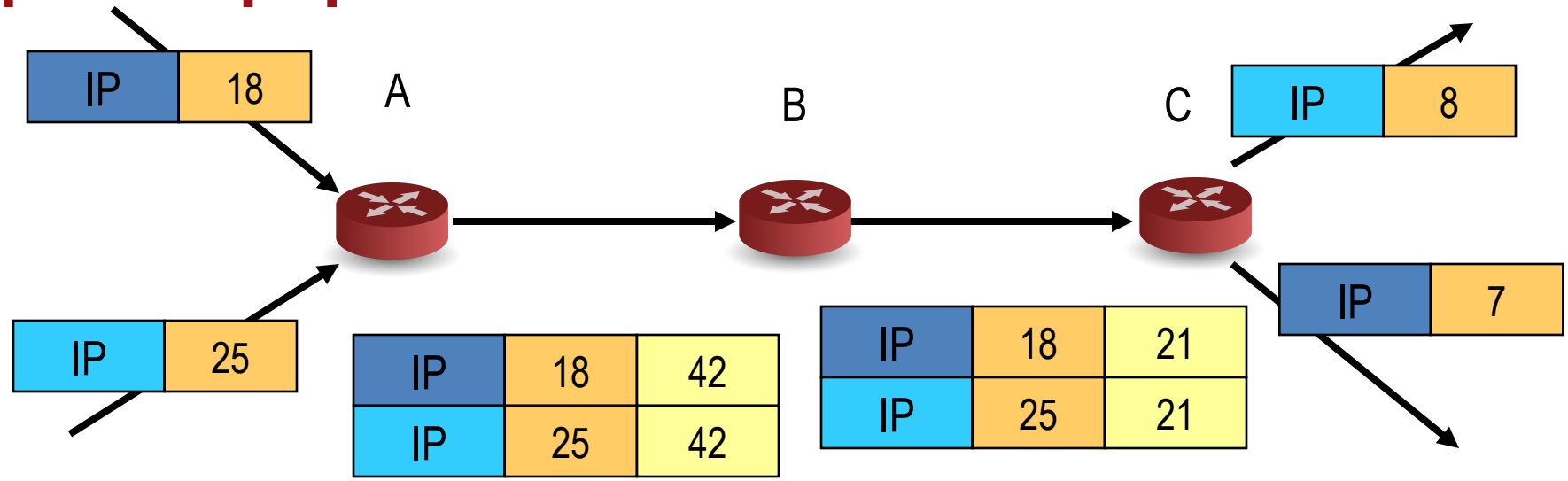


LS forwarding

- All' *Ingress Router* la corrispondenza è fra l'indirizzo IP di destinazione (e possibilmente altri parametri) e la Label del cammino scelto

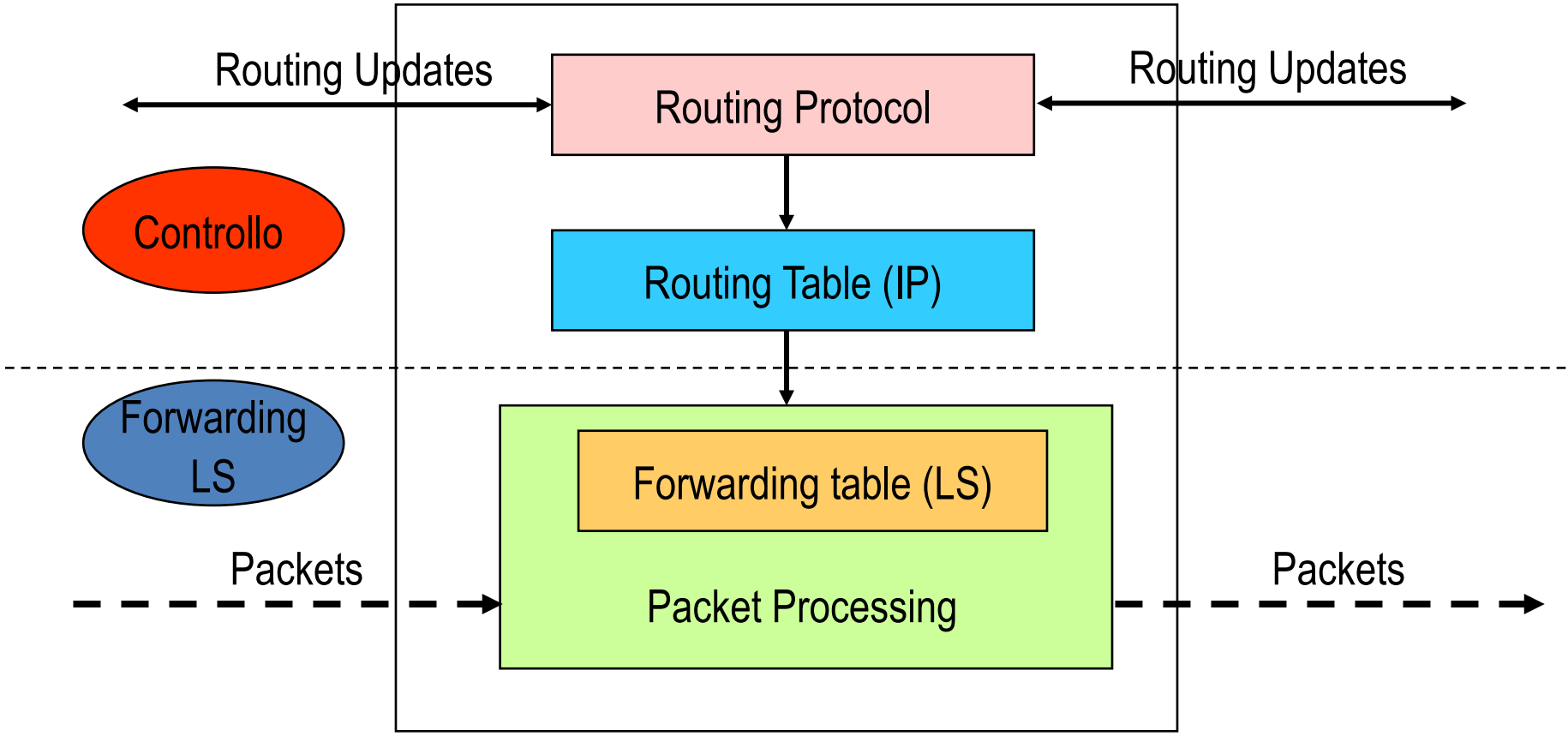


Affasciamento dei cammini: push e pop delle label



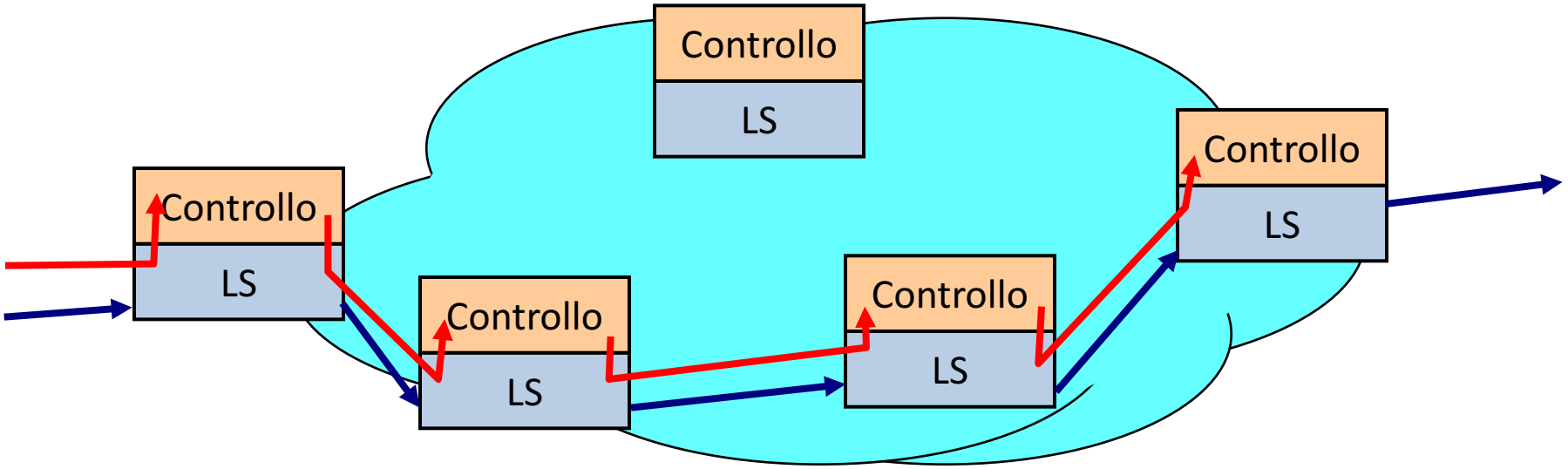
- I due flussi seguono il cammino AC in comune
- A incapsula i due flussi con identica label
- B instrada sulla label 2
- C decapsula i flussi

Inoltro e Controllo



Inoltro e Controllo

- I pacchetti di controllo seguono un inoltro hop-by-hop simile a quello IP tradizionale
- I pacchetti di controllo creano un nuovo label switched path (circuito virtuale)
- I pacchetti dati per i quali è stato creato il path possono dopo inoltrati direttamente in base alla label

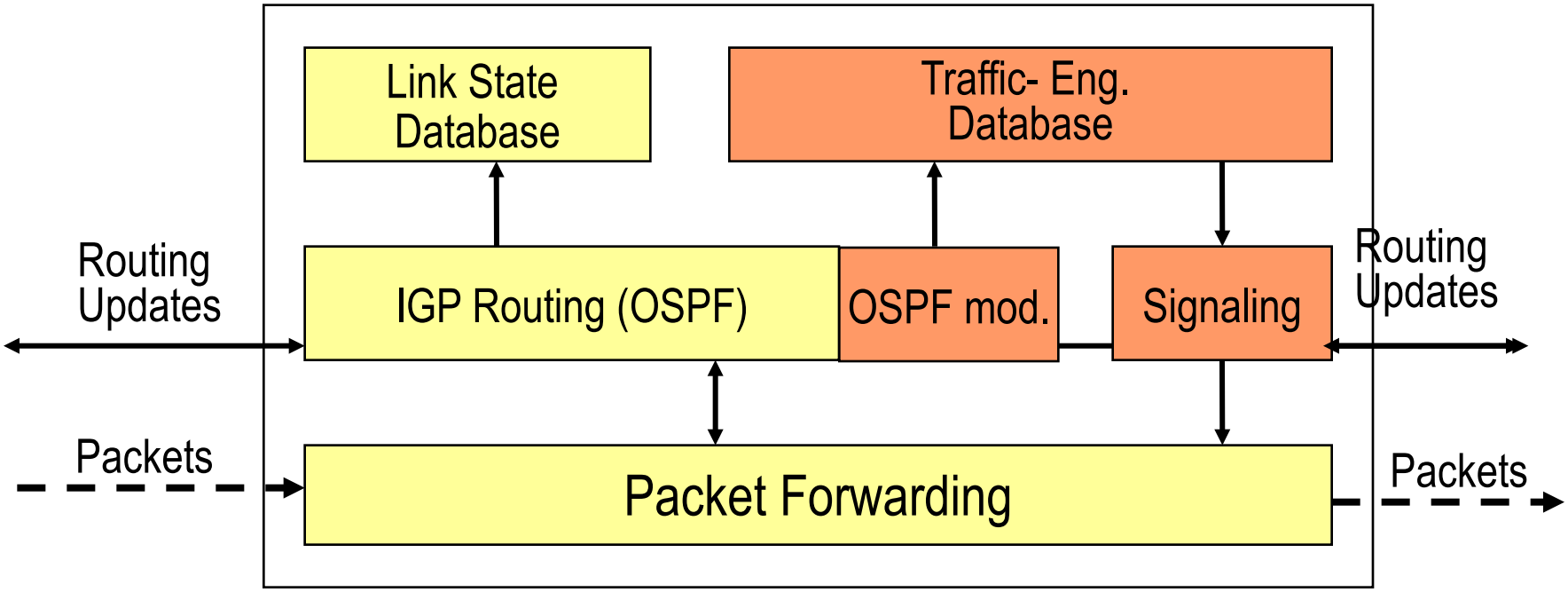


Inoltro e Controllo

- Ovviamente è possibile anche un instaurazione “manuale” dei label switched path; in questo caso il controllo non serve
- Il disaccoppiamento fra routing e forwarding consente l’evoluzione delle tecniche e dei parametri di routing
- Consente economie di scala (cammini affasciati)
- Il forwading a circuito consente la prenotazione di risorse e l’uso di tecniche di ingegneria del traffico

Controllo

- Nuovo database di traffic engineering (TED)
- Nuove procedure di segnalazione (protocolli di routing)



TED

- Contiene informazioni relative a:
- Informazioni topologiche tipo link-state
  - Derivate dai protocolli di routing
- Risorse di rete (banda dei link, banda prenotata)
  - Derivate da estensioni dei protocolli di routing (IGP)
- Dati amministrativi
  - Derivate da dati di configurazione degli utenti
- Consente ai border router di determinare un cammino

Instaurazione del cammino

- **Si determina lo *Egress Router* in base al *next hop* BGP**
- **I cammini possono essere determinati:**
  - "off line"
    - Ottimizzazione globale conoscendo i flussi
  - "on line" (Constrained based routing)
    - Tiene conto dei vincoli dell'utente
      - banda
      - inclusione/esclusione di link/nodi
      - richieste amministrative
      - riarrangiamento si/no
      - ……

Segnalazione

- Serve un **meccanismo di segnalazione** per
  - Coordinare la distribuzione delle label
  - Instaurare un cammino desiderato
  - (Explicit Route)
  - Riservare le risorse
  - Riassegnare le risorse
  - Prevenire i loop

Segnalazione

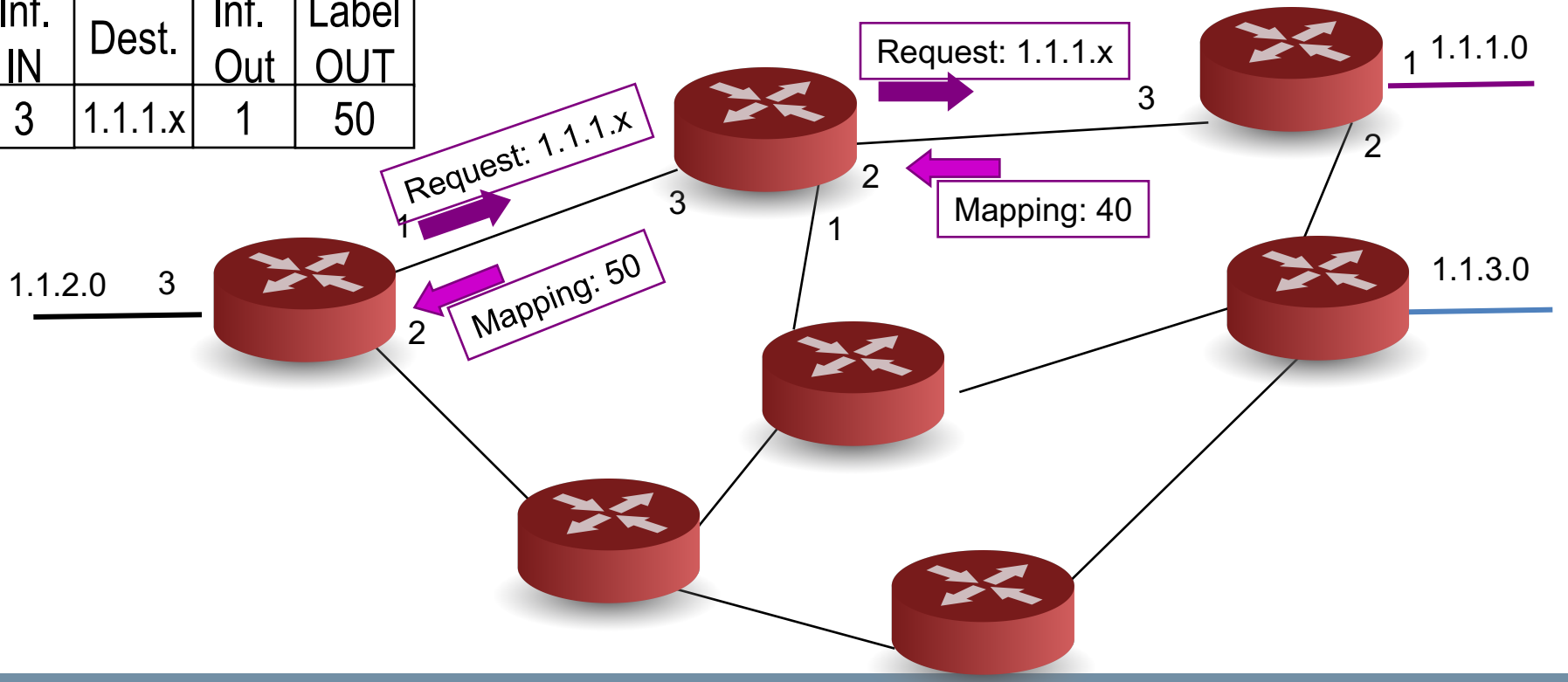
- **I meccanismi prevedono 3 possibilità**
  - *Label Distribution Protocol* (LDP)
    - Hop per Hop
    - Segue i cammini di IGP
    - Non supporta il Traffic Engineering
  - Constrained Routing LDP
    - Estende LDP a supportare le route esplicite

Label Distribution Protocol (LDP)

Inf. IN	Label IN	Dest.	Inf. Out	Label OUT
3	50	1.1.1.x	2	40

Inf. IN	Label IN	Dest.	Inf. Out
3	40	1.1.1.x	1

Inf. IN	Dest.	Inf. Out	Label OUT
3	1.1.1.x	1	50

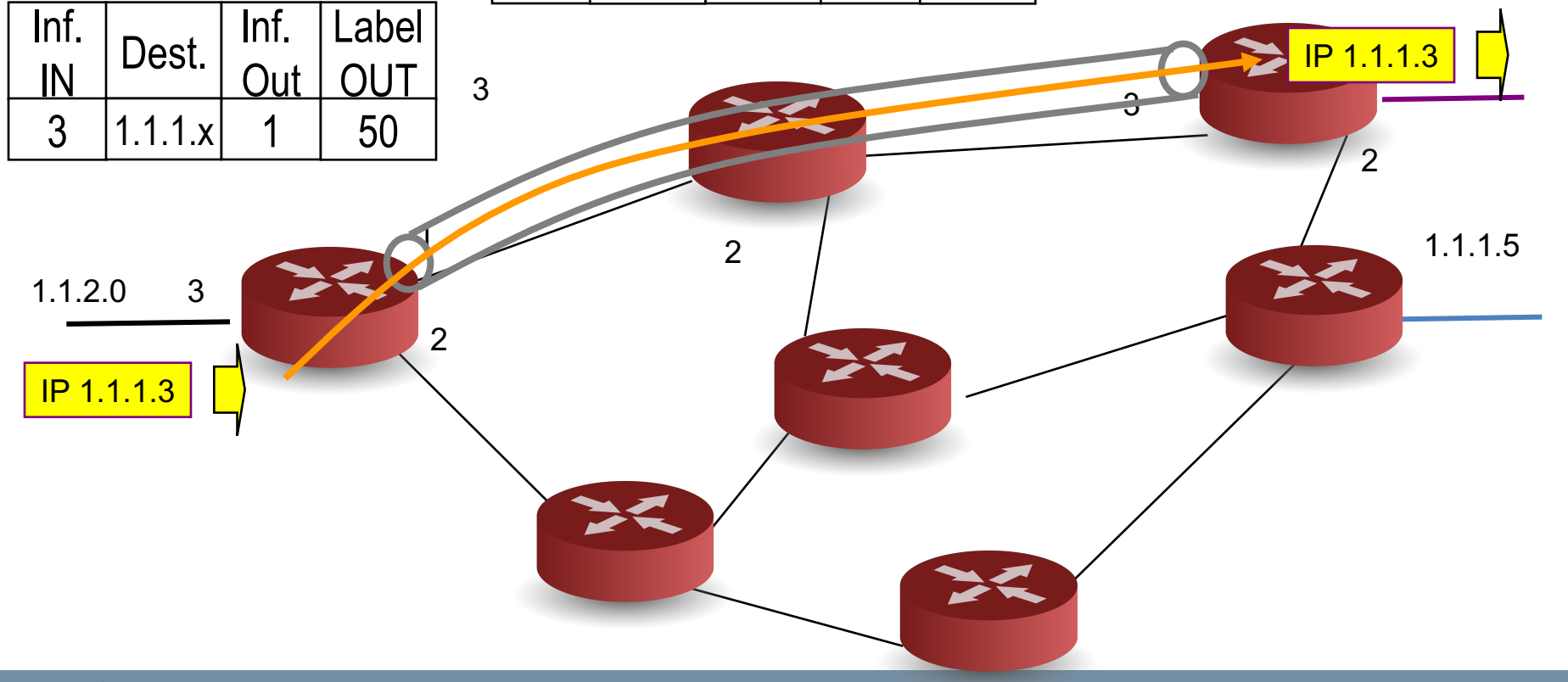


Label Switched Path (LSP)

Inf. IN	Dest.	Inf. Out	Label OUT
3	1.1.1.x	1	50

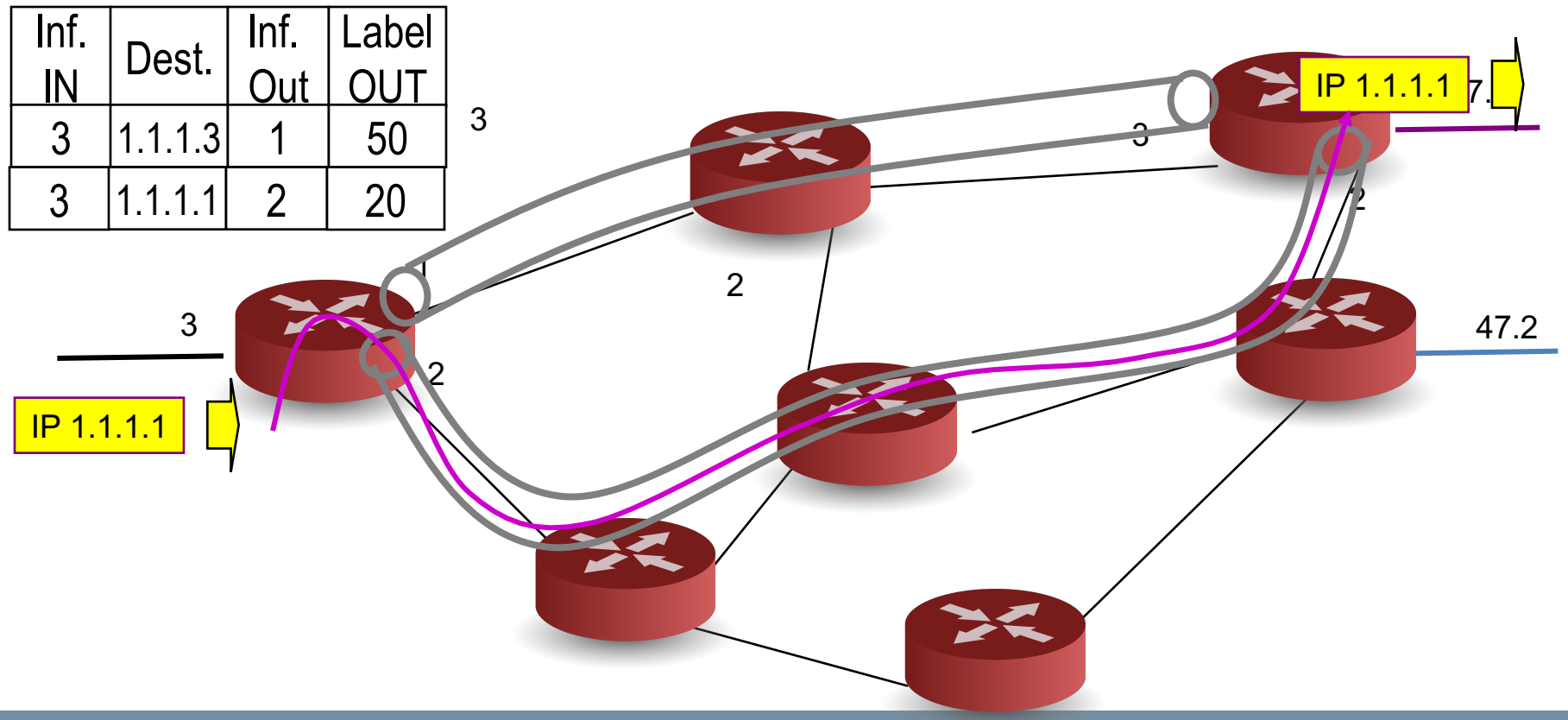
Inf. IN	Label IN	Dest.	Inf. Out	Label OUT
3	50	1.1.1.x	2	40

Inf. IN	Label IN	Dest.	Inf. Out
3	40	1.1.1.x	1

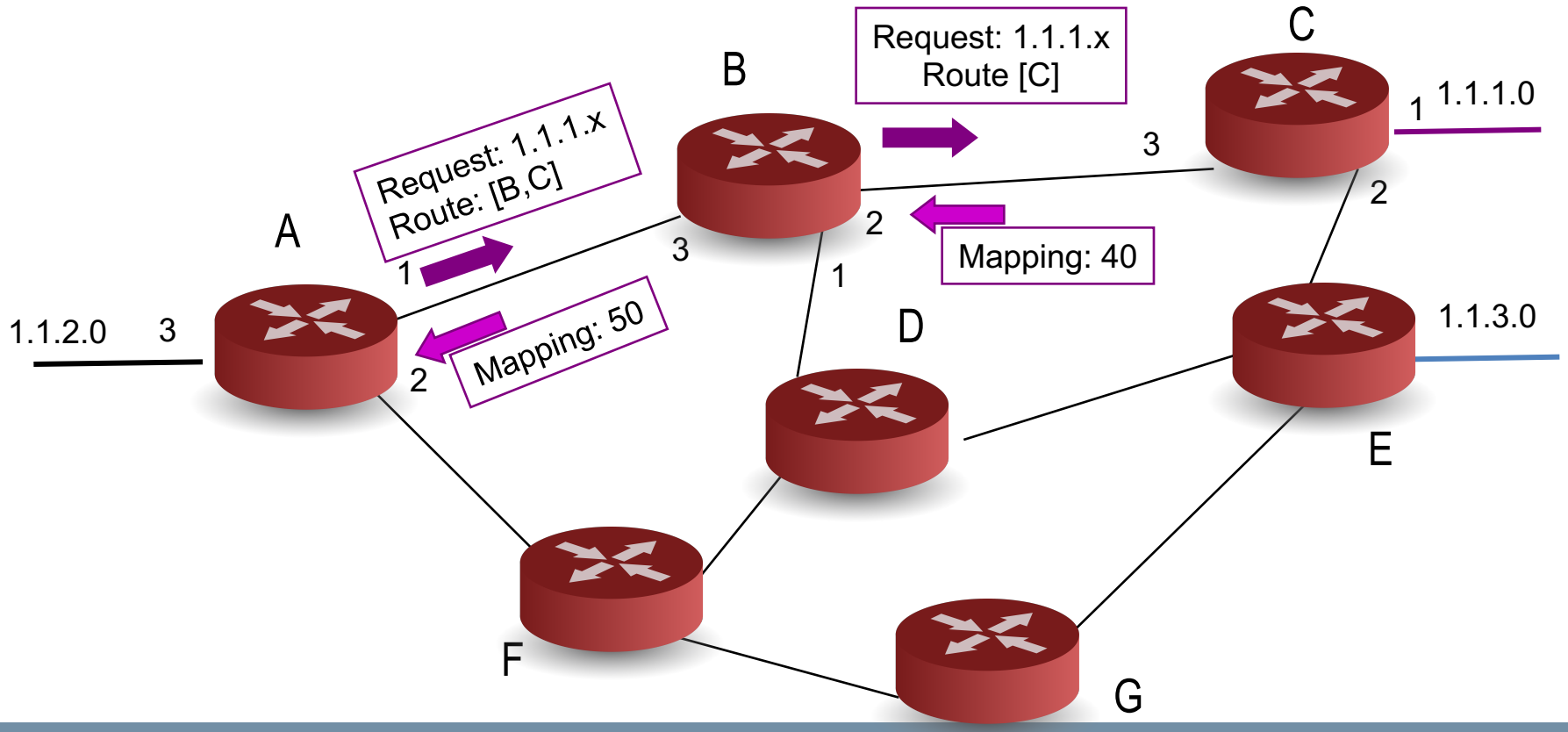


Explicitely Routed-LDP

Inf. IN	Dest.	Inf. Out	Label OUT
3	1.1.1.3	1	50
3	1.1.1.1	2	20



CR-LDP


Request: 1.1.1.x
Route [C]
Request: 1.1.1.x
Route: [B,C]
Mapping: 40
Mapping: 50
A
B
C
D
E
F
G
1.1.2.0
1.1.1.0
1.1.3.0
1
2
3