Traffic Tunnelling & Overlay Networks

Redes de Comunicações II

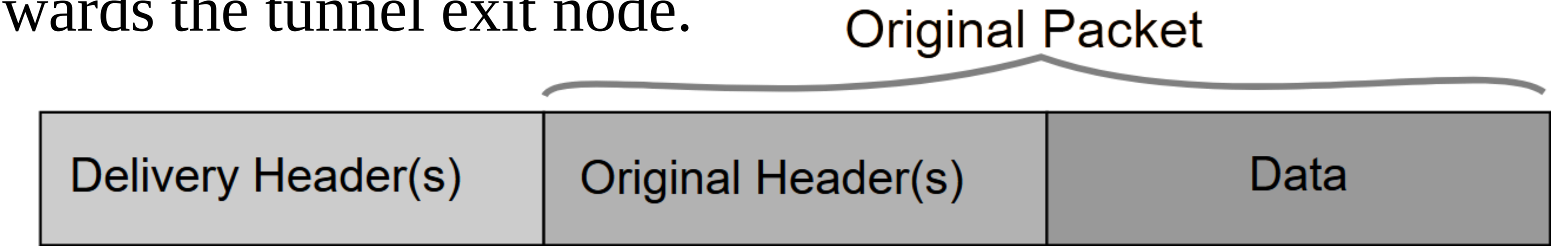
Licenciatura em Engenharia de Computadores e Informática

Prof. Amaro de Sousa (asou@ua.pt)

DETI-UA, 2024/2025

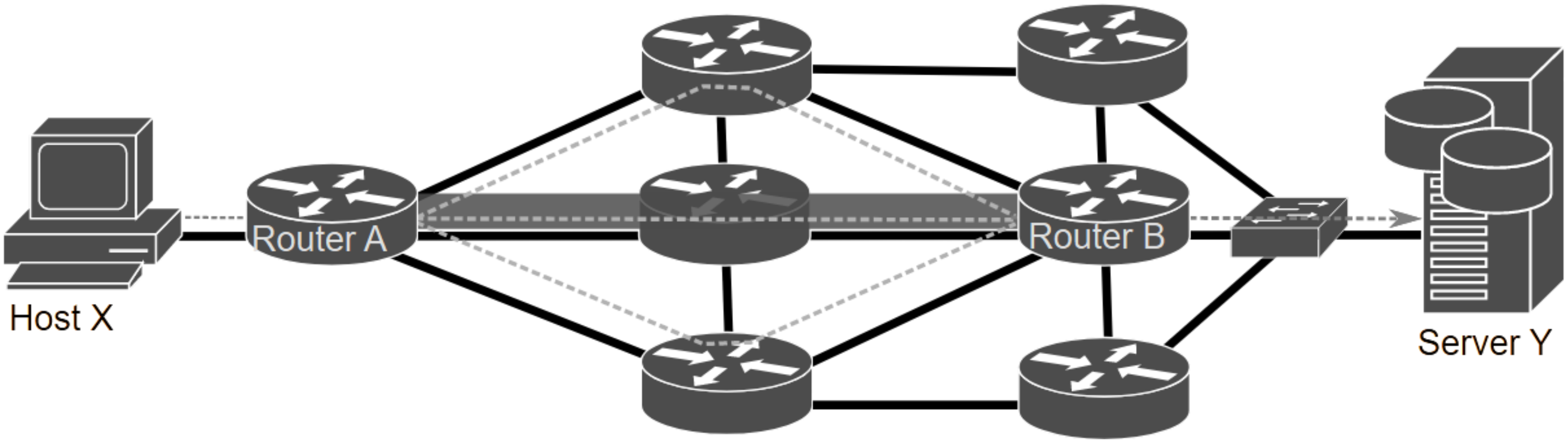
Traffic Tunnel Concept

- A tunnel is implemented by adding (at the tunnel entry node) one or more headers to the original IP packets used to forward the packets towards the tunnel exit node.



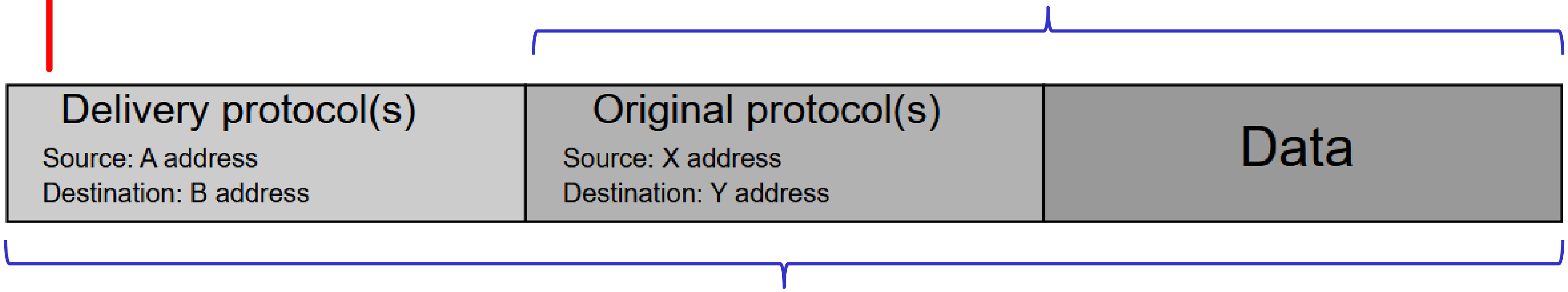
- Main purposes of traffic tunnelling:
  - To guarantee that the IP packets for a given destination network are routed through a specific network node in their routing path towards the destination.
  - To guarantee the forwarding of IP packets to a remote node when the intermediary nodes do not support the original packet network protocol
    - IPv6 packets forwarded through IPv4 networks
    - IPv4 packets forwarded through IPv6 networks
  - To define virtual channels that consider additional transport header data to provide differentiated Quality of Service, security and/or optimized routing.
    - Transport header data: type (UDP or TCP), source and destination port numbers

Tunnel End-Points



Original Packet from Host X to Server Y:
sent from Host X to Router A
sent from Router B to Server Y

Parte adicional



Delivery protocol(s)
Source: A address
Destination: B address

Original protocol(s)
Source: X address
Destination: Y address

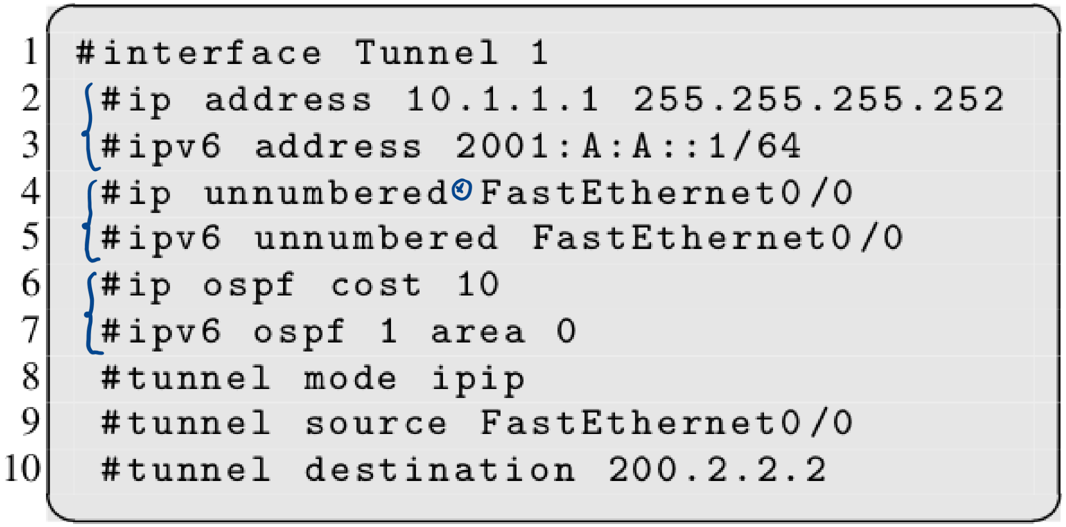
Data

Tunnel packet sent:
from Router A (the entry end-point) to Router B (the exit end-point)

Virtual Tunnel Interface (VTI)

- A VTI is a logical construction that creates a virtual network interface in a network equipment that can be handled as any other network interface.
- A tunnel does not require to have any network addresses other the ones already bound to the end-point router.
- However, most implementations impose that a network address must be bound to a tunnel interface to enable IP processing on the interface.
  - The tunnel interface may have an explicitly bound network address (recommended to be able to apply routing policies to the traffic router through the tunnel)
  - The tunnel interface may reuse an address of another interface already configured on the router.

VTI Configuration



```
#interface Tunnel 1
 #ip address 10.1.1.1 255.255.255.252
 #ipv6 address 2001:A:A::1/64
 #ip unnumbered ⓐ FastEthernet0/0
 #ipv6 unnumbered FastEthernet0/0
 #ip ospf cost 10
 #ipv6 ospf 1 area 0
 #tunnel mode ipip
 #tunnel source FastEthernet0/0
 #tunnel destination 200.2.2.2
```

ⓐ Endereço da própria interface

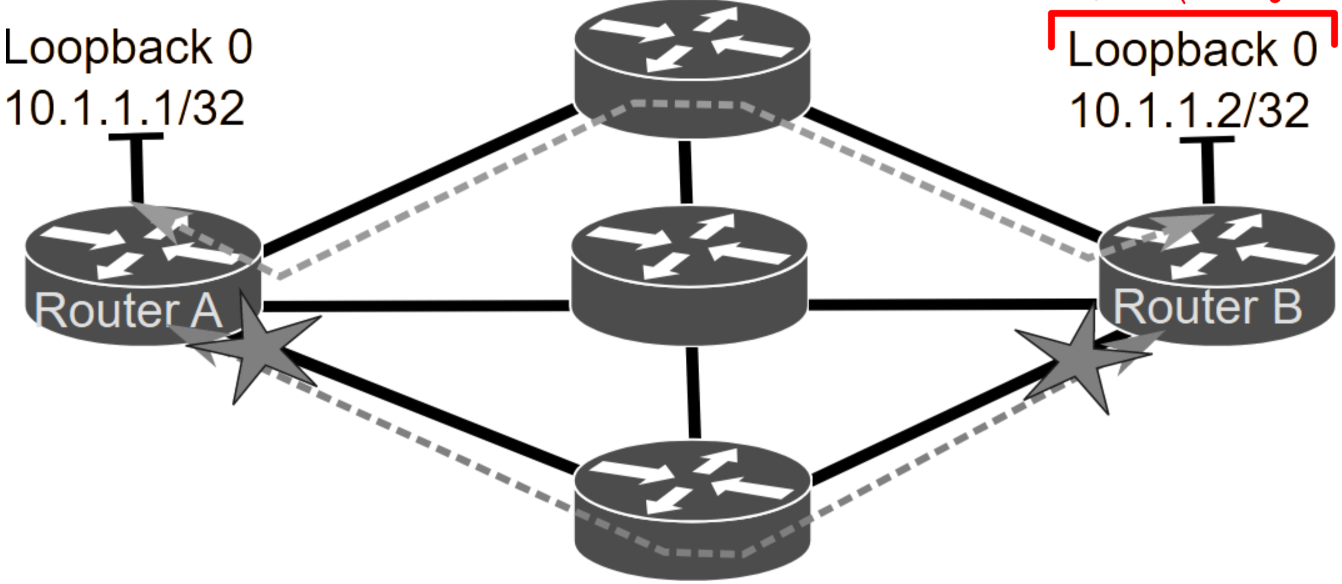
⚠ Não recomendado

- A numeric identifier
- A bounded IP address, this will enable IP processing
  - the router adds the tunnel interface to the routing table and allows routing via the interface
- A defined mode or type of tunnel
- Tunnel source, defined as the name of the local interface or IPv4/IPv6 address depending on the type of the tunnel.
- Tunnel destination, defined as a domain name or IPv4/IPv6 address depending on the type of the tunnel.
  - not mandatory in all types of tunnels (in some cases, the tunnel destination end-point is determined dynamically).
- May optionally have additional configurations for routing, security and QoS purposes.

Loopback Interfaces as End-Points

- A loopback interface is another logical construction that creates a virtual network interface completely independent from the remaining physical and logical router network interfaces.
- The main propose of a loopback interface is to provide a network address to serve as router identifier in remote network configurations and distributed algorithms.
- The main advantage of using loopback interfaces as tunnel end-points is to obtain a tunnel not bounded to any physical network interface that may fail.

Construção Lógica



IP Tunnel Types

IPv4-IPv4

- Original IPv4 packets are delivered using IPv4 as network protocol.

GRE IPv4

- The original packets protocol is indicated in the GRE (Generic Routing Encapsulation) header and packets are delivered using IPv4 as network protocol.

IPv6-IPv6

- Original IPv6 packets are delivered using IPv6 as network protocol.

GRE IPv6

- The original packets protocol is indicated in the GRE header and packets are delivered using IPv6 as network protocol.

IPv6-IPv4

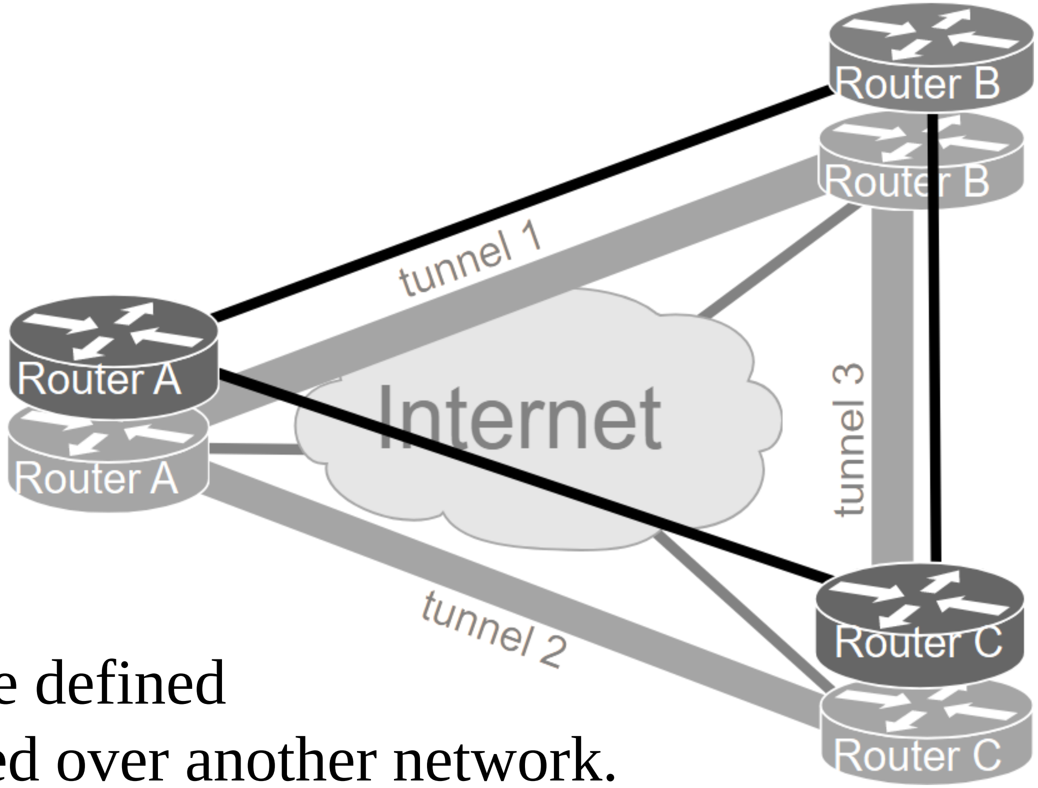
- Original IPv6 packets are delivered using IPv4 as network protocol.

IPv4-IPv6

- Original IPv4 packets are delivered using IPv6 as network protocol.

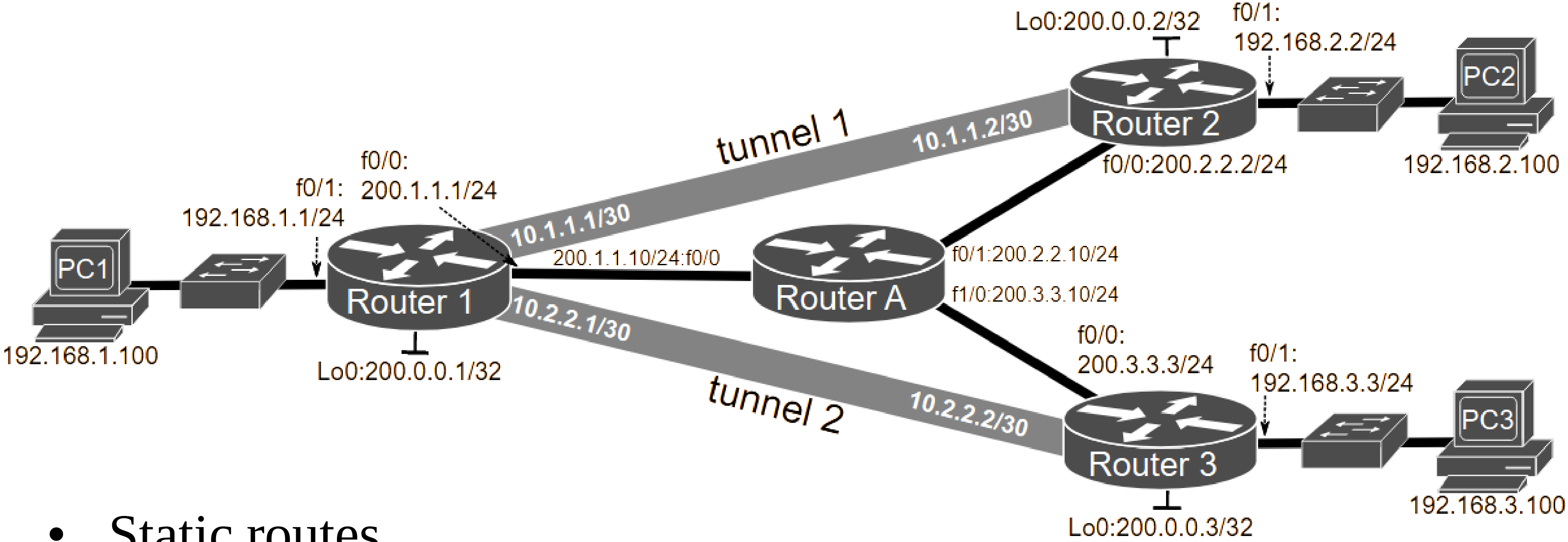
Overlay Network

Rede Virtual suportada por uma Rede Fisica

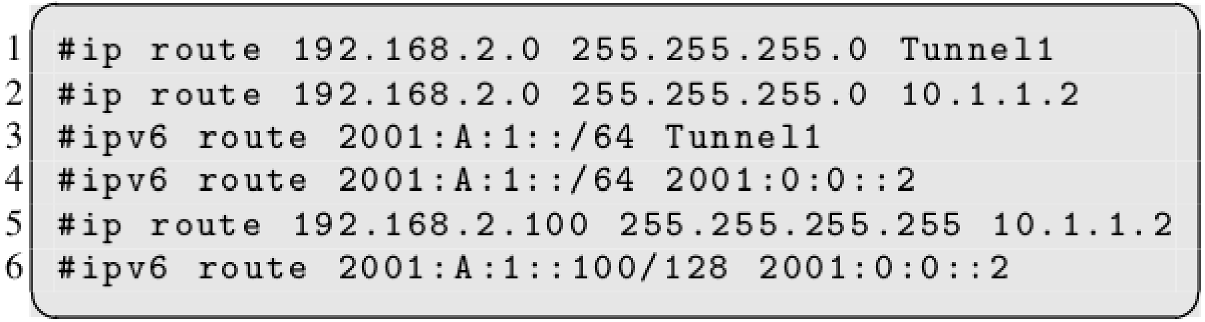


- An overlay network can be defined as a virtual network defined over another network.
  - For a specific purpose like private transport/routing policies, QoS, security.
- The underlying network can be physical or also virtual.
  - May result in multiple layers of overlay networks.
- When any level of privacy protocol is present on an overlay network, it is named a Virtual Private Network (VPN).

Routing Through/Between Tunnels

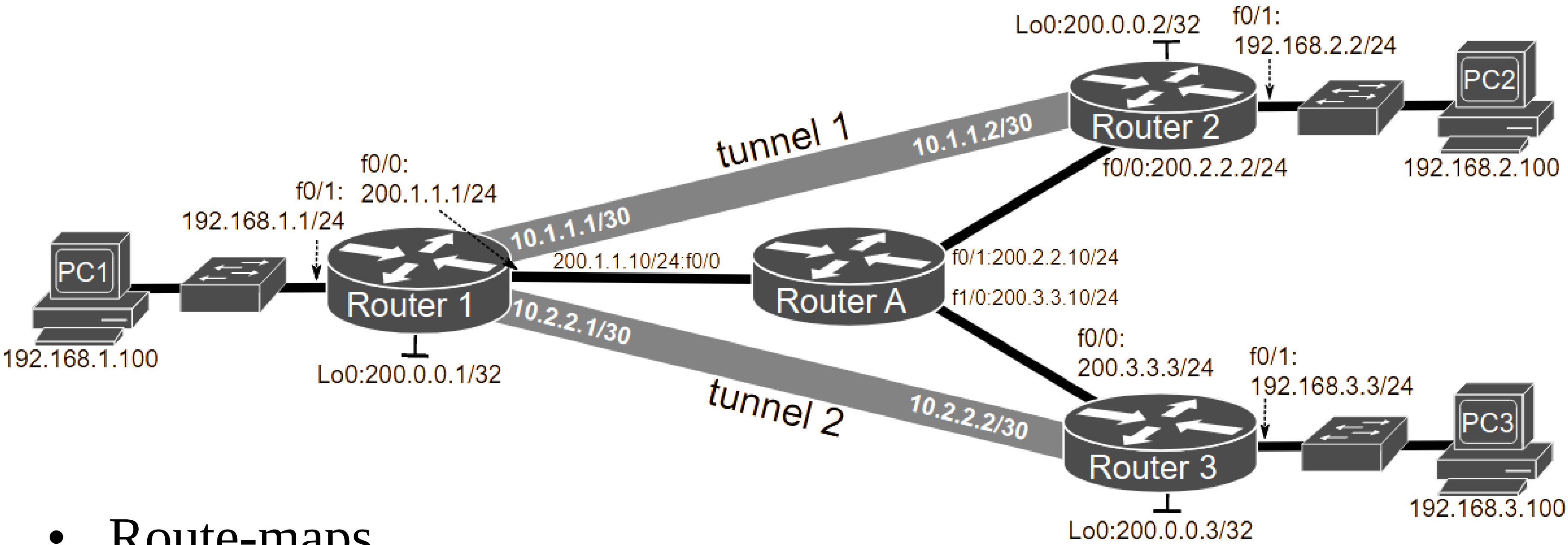


- Static routes



```
#ip route 192.168.2.0 255.255.255.0 Tunnel1
#ip route 192.168.2.0 255.255.255.0 10.1.1.2
#ipv6 route 2001:A:1::/64 Tunnel1
#ipv6 route 2001:A:1::/64 2001:0:0::2
#ip route 192.168.2.100 255.255.255.255 10.1.1.2
#ipv6 route 2001:A:1::100/128 2001:0:0::2
```

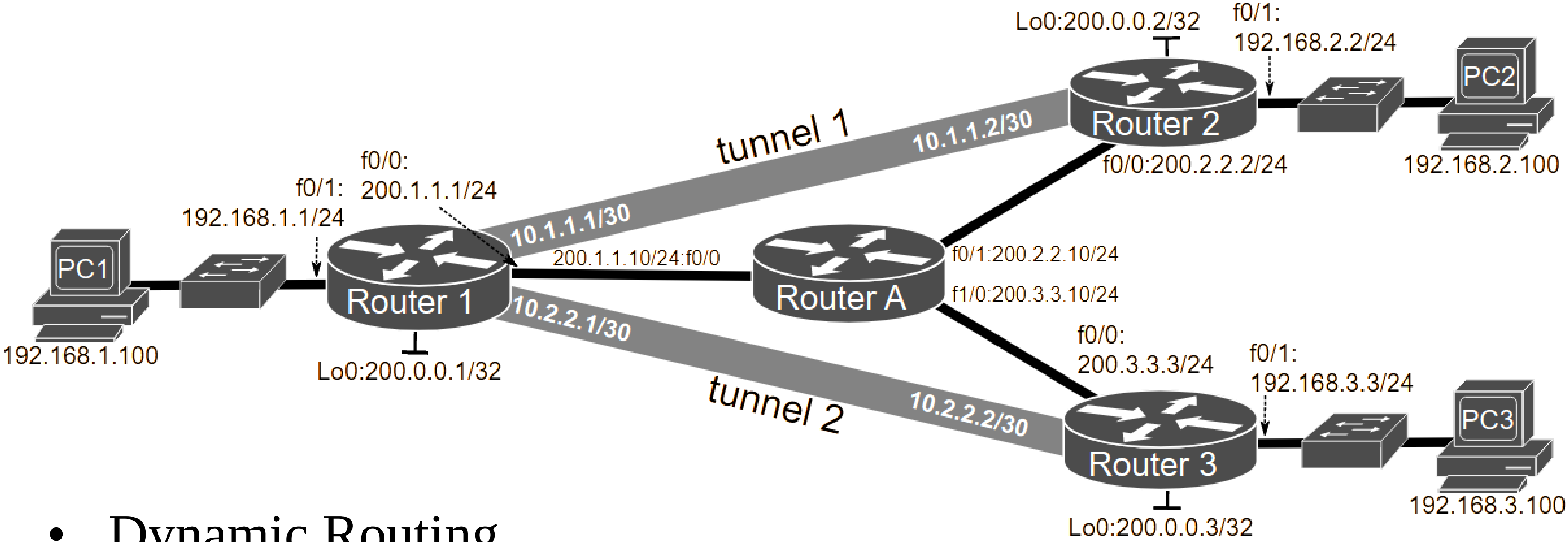
Routing Through/Between Tunnels



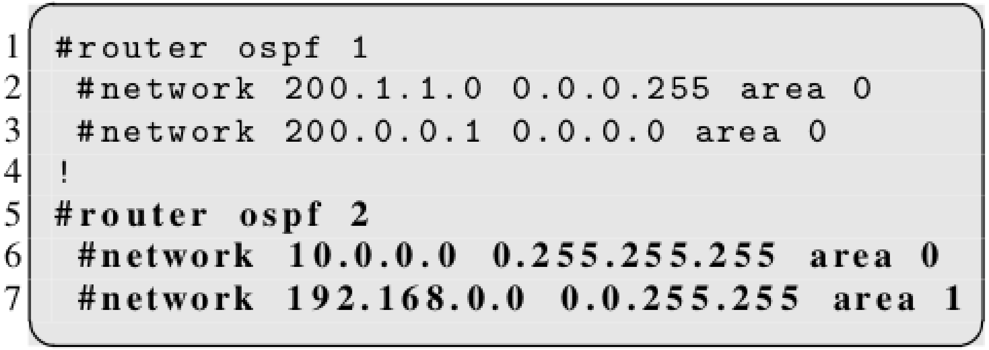
- Route-maps

```
#access-list 100 permit ip host 192.168.1.100 192.168.2.0 255.255.255.0
#route-map routeT1
 #match ip address 100
 #set ip next-hop 10.1.1.2
#interface FastEthernet0/1
 #ip policy route-map routeT1
```

Routing Through/Between Tunnels



- Dynamic Routing
  - Distinct routing processes:
    - One for the overlay network
    - One for the underlying network

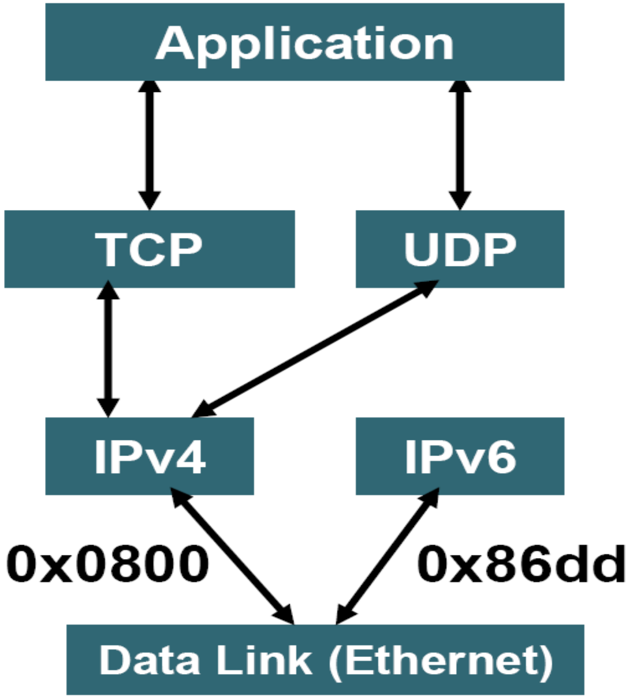


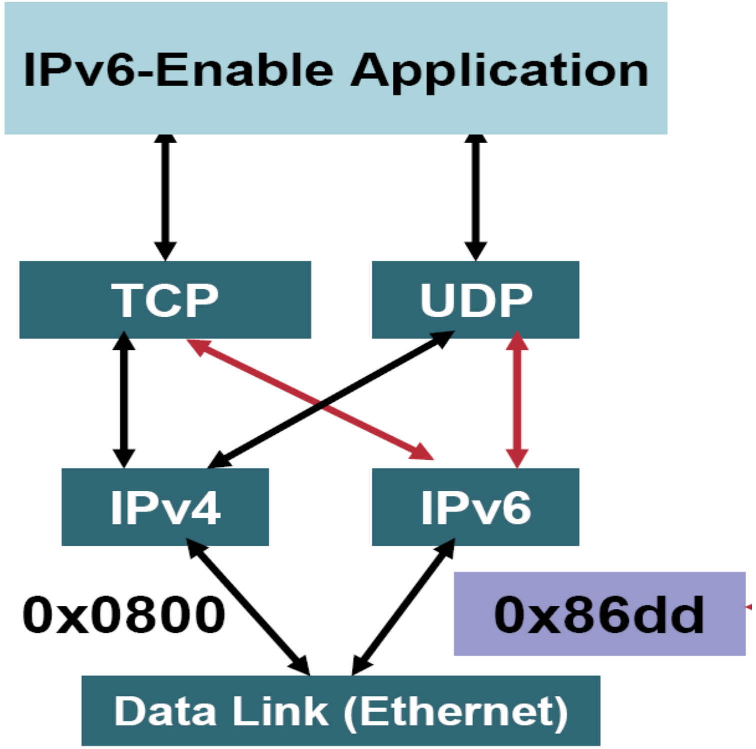
```
#router ospf 1
 #network 200.1.1.0 0.0.0.255 area 0
 #network 200.0.0.1 0.0.0.0 area 0
!
#router ospf 2
 #network 10.0.0.0 0.255.255.255 area 0
 #network 192.168.0.0 0.0.255.255 area 1
```

IPv6 Deployment Techniques

- The target (in the future) is to deploy IPv6 with dual-stack backbones
  - IPv4 and IPv6 network protocols coexist in a dual IP layer routing backbone
  - All routers in the network need to be upgraded to be dual-stack
- Meanwhile, transition scenarios are required in which IPv6 connectivity is supported over IPv4 networks through tunnelling. Available options:
  - Manually configured tunnels
    - With and without Generic Routing Encapsulation (GRE)
  - Semiautomatic tunnel mechanisms
  - Fully automatic tunnel mechanisms

Dual Stack Hosts





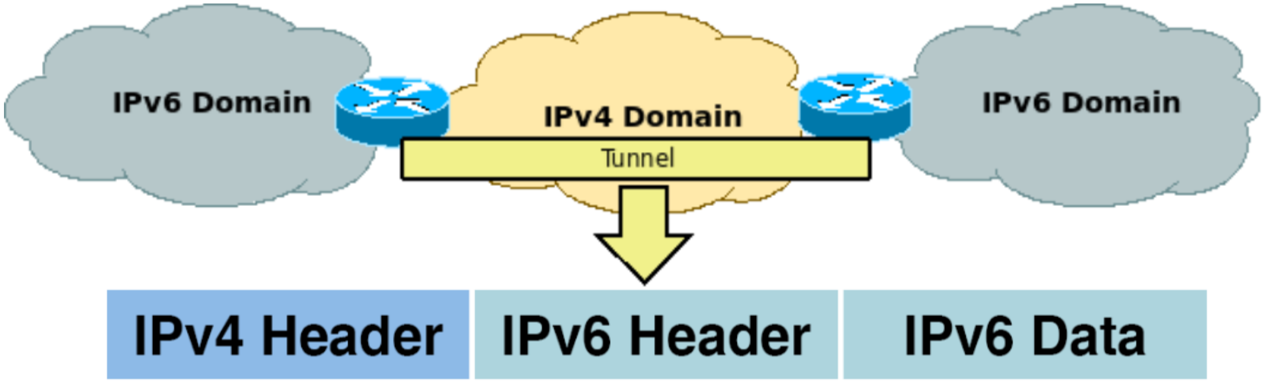
- Applications may talk through both network protocols
- Choice of the IP version is based on DNS responses and/or on application preferences

IPv6 Overlay Tunnelling in Transition Scenarios

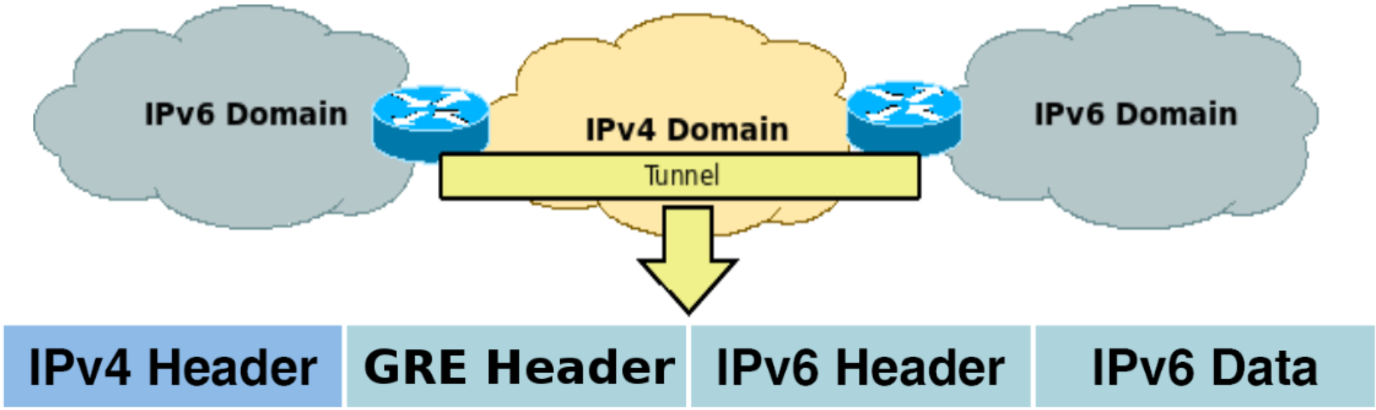
- Manual mechanisms
  - IPv6 supported through IPv6-IPv4 tunnel types
  - IPv6 supported through GRE IPv4 tunnel types
- Semi-automatic mechanisms
  - Tunnel Broker (most common implementation: Teredo)
- Automatic mechanisms
  - Common idea of automatic mechanisms:
    - the size of an IPv6 address (16 bytes) is much larger than the size of an IPv4 address (4 bytes)
    - embedding IPv4 addresses into the IPv6 addresses enables the automatic determination of the tunnel exit end-point IPv4 addresses
  - Examples:
    - 6to4 Tunnels
    - ISATAP Tunnels

IPv6 over Manually Configured Tunnels

- IPv6-IPv4 tunnel type:

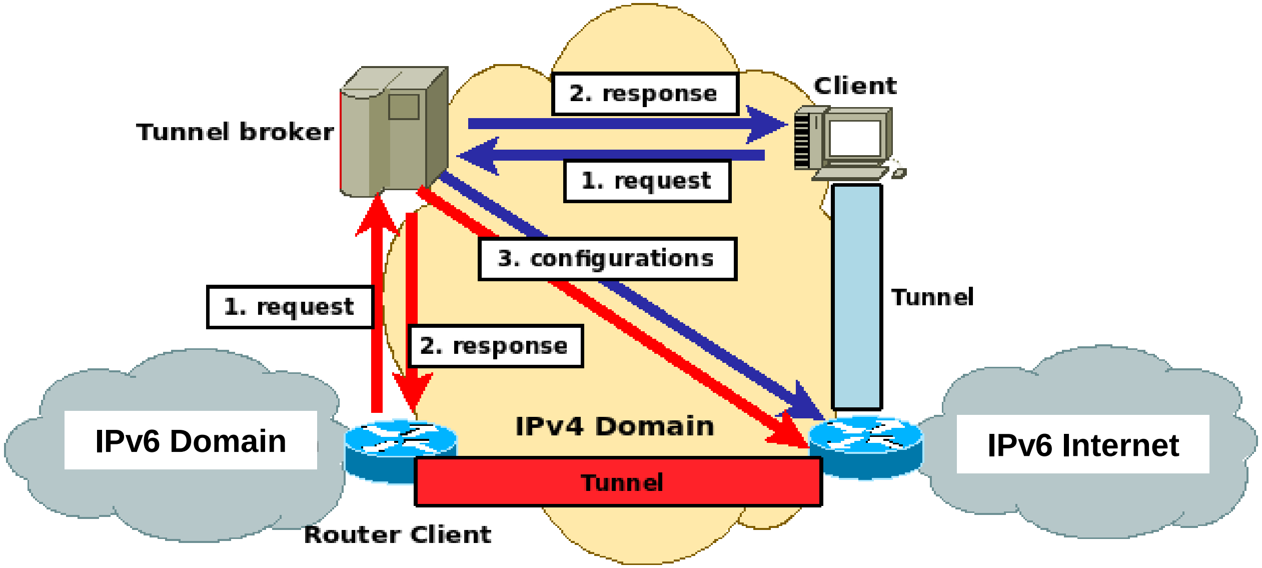


- GRE IPv4 tunnel type:



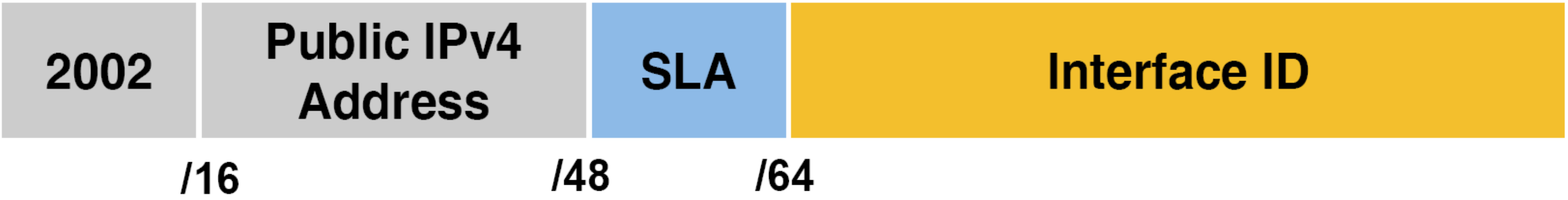
Tunnel Broker

- A tunnel broker service allows IPv6 applications on dual-stack systems access to an IPv6 backbone through a IPv4 network
- The Broker manages tunnel requests and configuration
- Potential security issue as the broker is a single point of failure
- Most common implementation: Teredo.
  - The Teredo IPv6 address block is 2001:0:XXXX:XXXX::/64 where XXXX:XXXX is the public IPv4 address of the broker



6to4 Tunnels

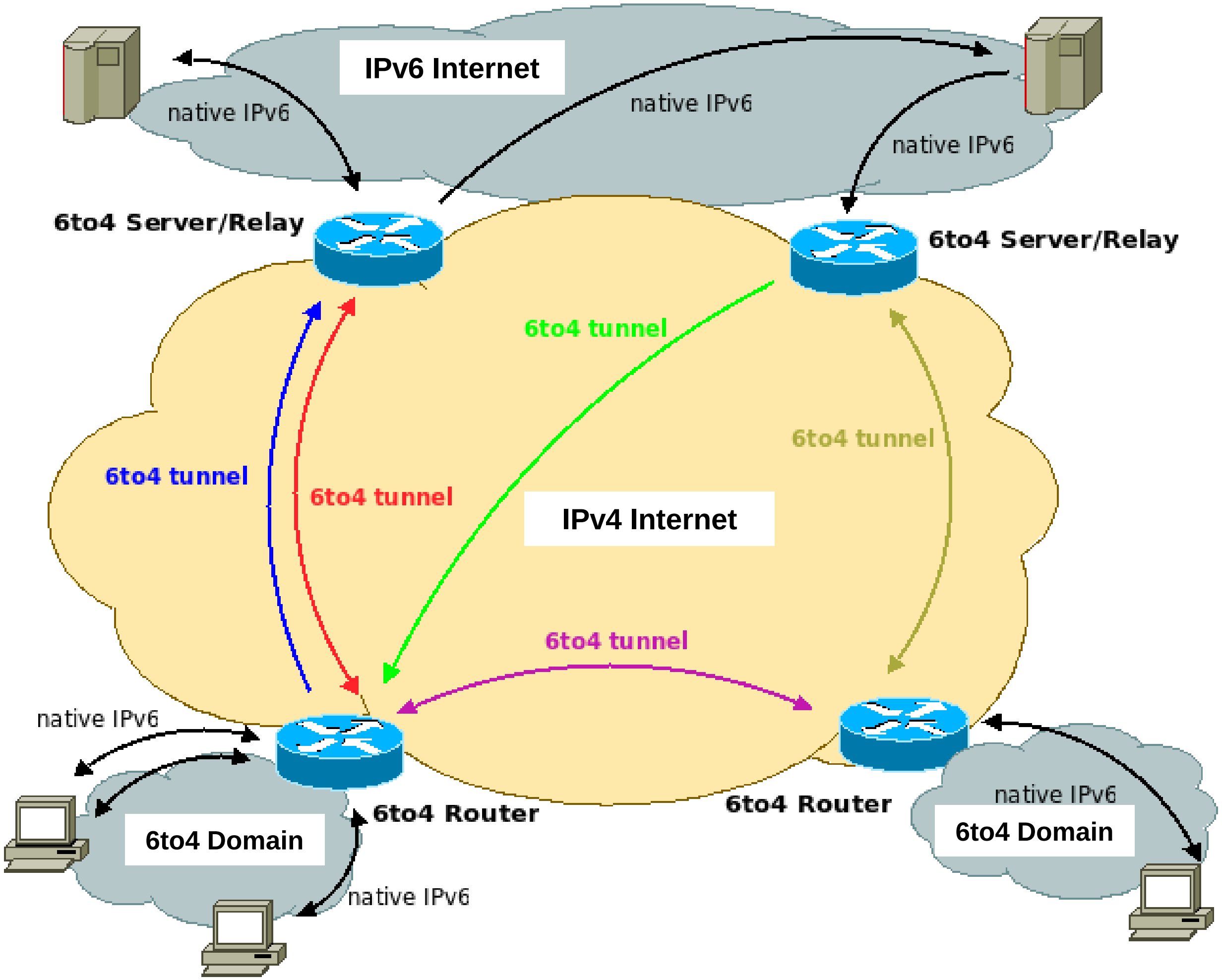
- Automatic 6to4 tunnels allow isolated IPv6 domains to connect (between them or with the IPv6 Internet) over an IPv4 network
- IPv4 tunnel end-point address is embedded within the 6to4 IPv6 address:



- 6to4 hosts/routers need to have a globally addressable IPv4 address:
  - Cannot be located behind a NAT box
  - unless the NAT box supports protocol 41 packets forwarding

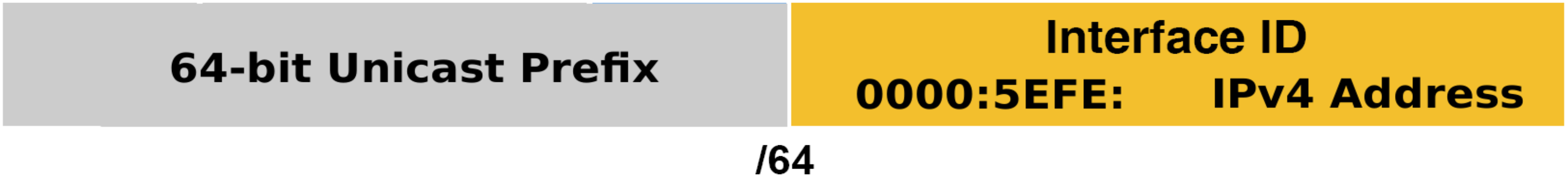
6to4 Relay Routers

- 6to4 routers:
  - Provide the connectivity between 6to4 IPv6 networks and the IPv4 Internet
- 6to4 relay routers:
  - Provide the connectivity between the IPv4 Internet and the IPv6 Internet.



ISATAP Tunnels

- ISATAP (Intra-site Automatic Tunnel Address Protocol)
  - is an automatic overlay tunnelling mechanism that uses the underlying IPv4 network as a non-broadcast multiple access link layer for IPv6.
  - is designed for transporting IPv6 packets within a site where a native IPv6 infrastructure is not yet available
- It encodes IPv4 Address in IPv6 Address within the interface ID:



- Although similar to other automatic tunnelling mechanisms, ISATAP is designed for transporting IPv6 packets within a site, not between sites.
- The unicast IPv6 prefix (/64) can be link local, site local or global (including 6to4 prefixes), enabling IPv6 routing locally or on the Internet.