Traffic Tunneling
&
Overlay Networks

Redes de Comunicações II

Licenciatura em
Engenharia de Computadores e Informática
DETI-UA

universidade de aveiro
deti.ua.pt

Traffic Tunnel Concept

- Main purposes

  Em relação ao ponto 1: Isto está relacionado com o Policy-Based Routing dos slides anteriores, o Tunnel é como se tivessemos um cabo direto entre Aveiro e Brasil. Forçar o tráfego a ir por um determinado caminho

  - Guarantee that a packet that reaches a network node will reach a specific secondary network node independently of the intermediary nodes routing processes,

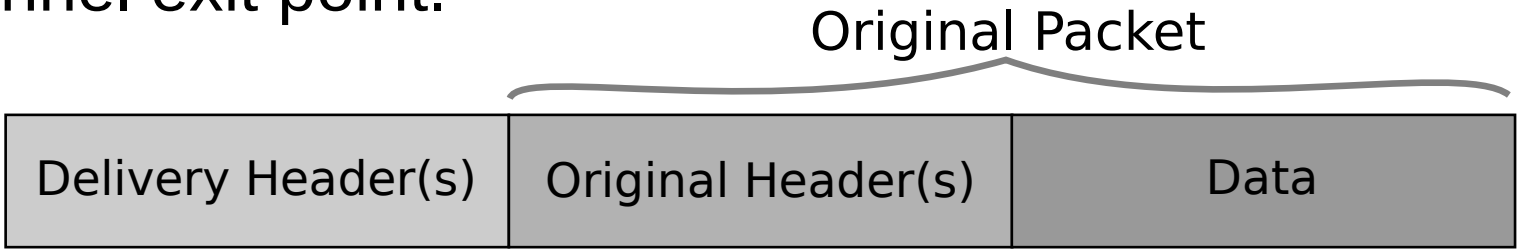
  Exemplo: Antes não havia IPv6, usa-se um tunnel Ipv6 numa rede IPv4 para utilizar certos serviços de IPv6. Pensar nisto para outras tecnologias que não IPv6.

  - Guarantee the delivery of a packet to a remote node when the intermediary nodes do not support the original packet network protocol, and,

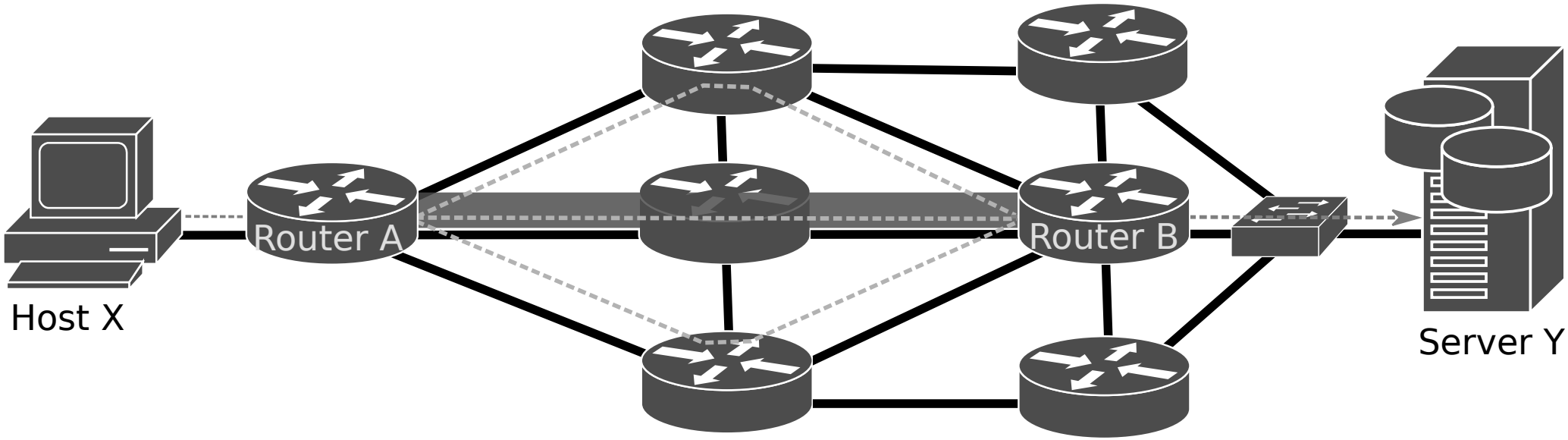
  As vezes não se quer que os nossos pacotes passem por uma empresa ou um país específico (espionagem por exemplo), então faz-se um tunel de forma que os pacotes não passem por lá.

  - Define a virtual channel that adds additional data transport features in order to provide differentiated QoS, security requirements and/or optimized routing.

- Achieved by adding, at the tunnel entry point, one or more protocol headers to the original packets to handle their delivery to the tunnel exit point.



Tunnel End-Points



Delivery protocol(s)	Original protocol(s)	Data
Source: A address Destination: B address	Source: X address Destination: Y address	

Virtual Tunnel Interface (VTI)

- Logical construction that creates a virtual network interface that can be handled as any other network interface within a network equipment.
- 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 in order to enable IP processing on the interface.
  - The tunnel interface may have a explicitly bound network address or reuse an address of another interface already configured on the router.

```
#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
```

VTI Requirements

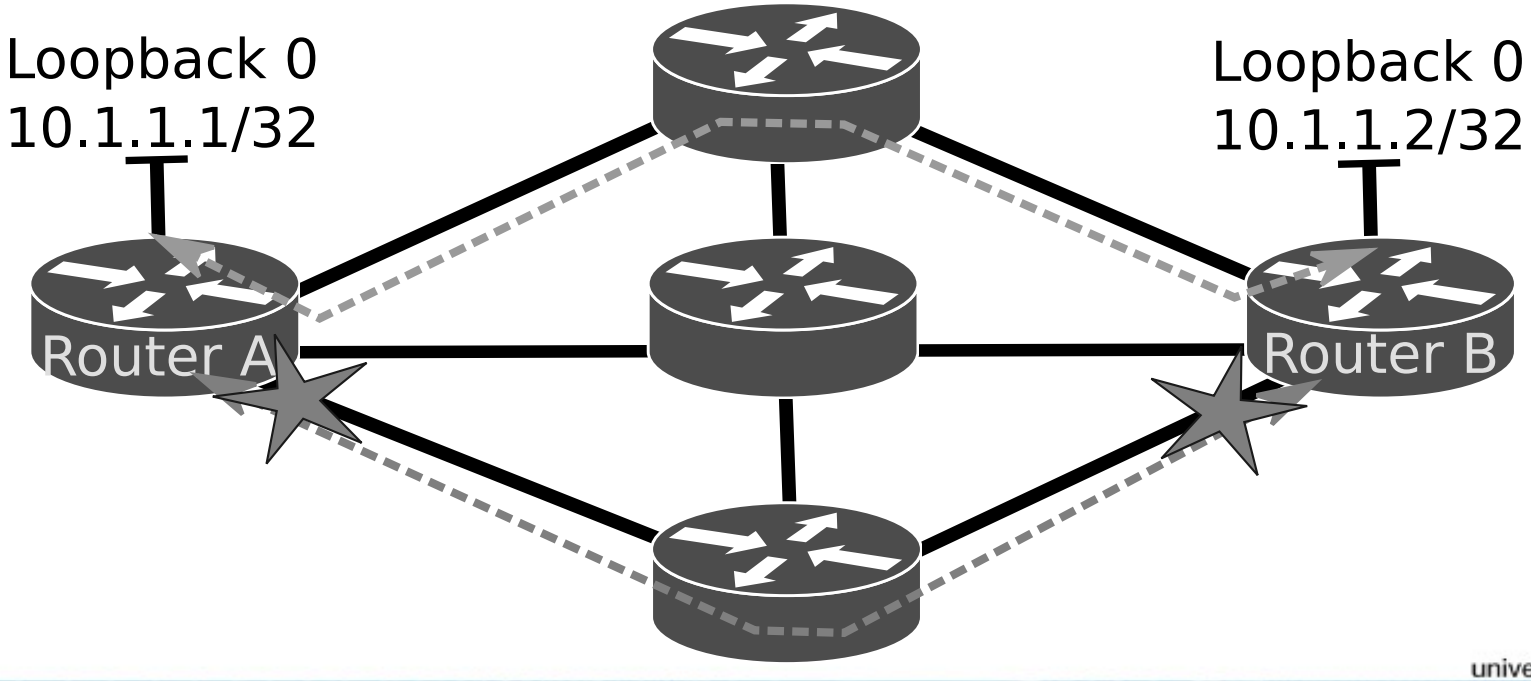
- A numeric identifier,
- A bounded IP address, this will enable IP processing,
  - Add the tunnel interface to the routing table and allow routing via the interface,

```
1  #interface Tunnel 1
2   #ip address 10.1.1.1 255.255.255.252
3   #ipv6 address 2001:A:A::1/64
4   #ip unnumbered FastEthernet0/0
5   #ipv6 unnumbered FastEthernet0/0
6   #ip ospf cost 10
7   #ipv6 ospf 1 area 0
8   #tunnel mode ipip
9   #tunnel source FastEthernet0/0
10  #tunnel destination 200.2.2.2
```

- A defined mode or type of tunnel,
  - Availability of tunnel models depends on the Router model, operating software and licenses.
- 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.
  - This definition is not mandatory for all types of tunnels because in some cases the tunnel end-point is determined dynamically.
- May optionally have additional configurations for routing, security and QoS purposes.

Loopback Interfaces as End-Points

- 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 distribute algorithms.
- The main advantage of using loopback interfaces as tunnel end-points, is the creation of a tunnel not bounded to any individual network card/link that may fail.

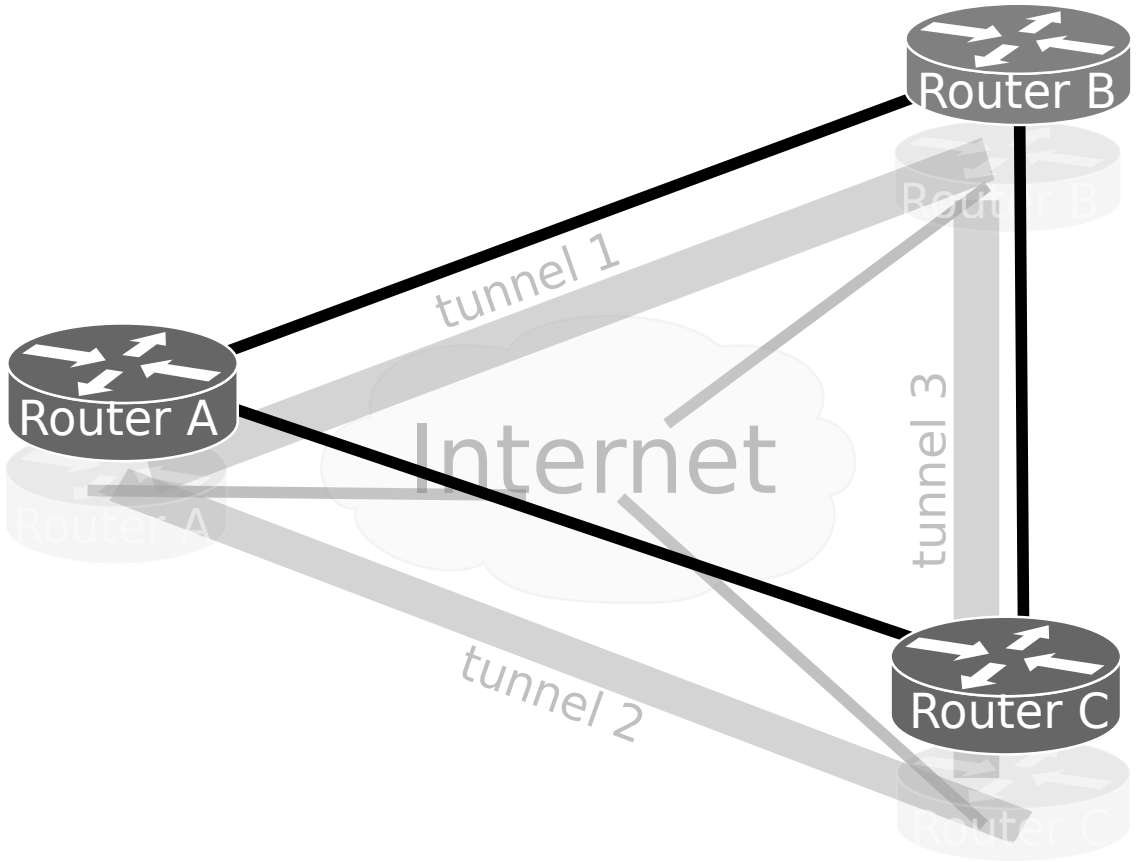


IP Tunnel Types

- IPv4-IPv4
  - Original IPv4 packets are delivered using IPV4 as network protocol.
- GRE IPv4 Generic Routing Encapsulaption -> "Teoricamente não é para nada", mas usa-se pq as vezes é mais facil de implementar na prática.
  - Original packets protocol (any network protocol) is defined by GRE header and delivered using IPv4 as network protocol.
- IPv6-IPv6
  - Original IPv6 packets are delivered using IPv6 as network protocol.
- GRE IPv6 Estabalecem um tunnel entre dois pontos Ipv4 ou Ipv6 (basicamente são 2Bytes a dizer o que é está dentro do tunnel), cria-se o tunnel e lá dentro pode ir qualquer coisa, Ipv4, Ipv6, Ethernet, qqlr coisa
  - Original packets protocol (any network protocol) is defined by a GRE header and delivered using IPv6 as network protocol.
- IPv6-IPv4 Usar uma tecnologia quando a rede não tem essa tecnologia -> "Transportar uma texnologia para uma rede que não tem essa tecnologia"
  - Original IPv6 packets are delivered using IPv4 as network protocol.
- IPv4-IPv6 Já não é tão comum, mas poderá vir a ser. O IPv4 poderá no futuro ir desaparecendo, sendo preciso implementar esta tecnlogia em alguma rede que só use IPv6 por exemplo
  - Original IPv4 packets are delivered using IPv6 as network protocol.

Overlay Network

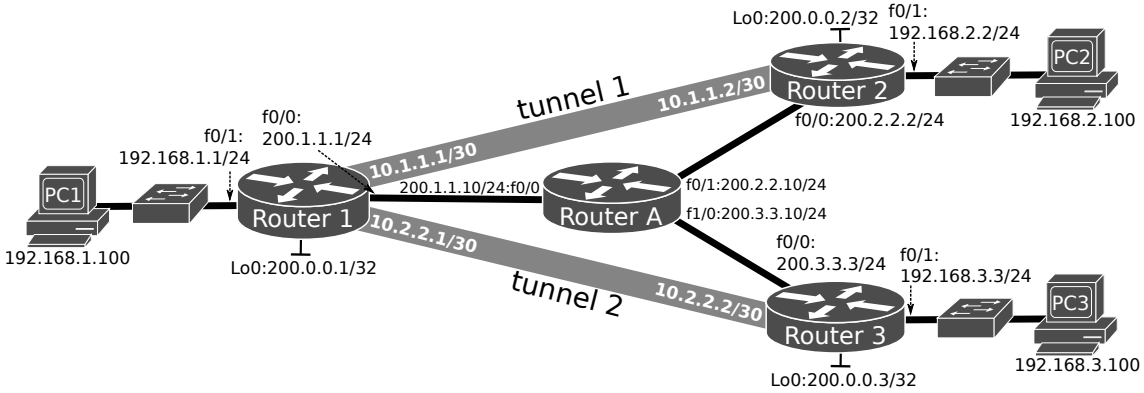
- An overlay network can be defined as a virtual network defined over another network.
  - For a specific purpose like private transport/routing policies, QoS, security.
- The underlying network can be physical or also virtual.
  - May result in multiple layers of overlay networks.
- When any level of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



- 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
```

- Dynamic Routing
  - Multiple (distinct) routing processes.
    - One per overlay network, and
    - One for the underlying network.

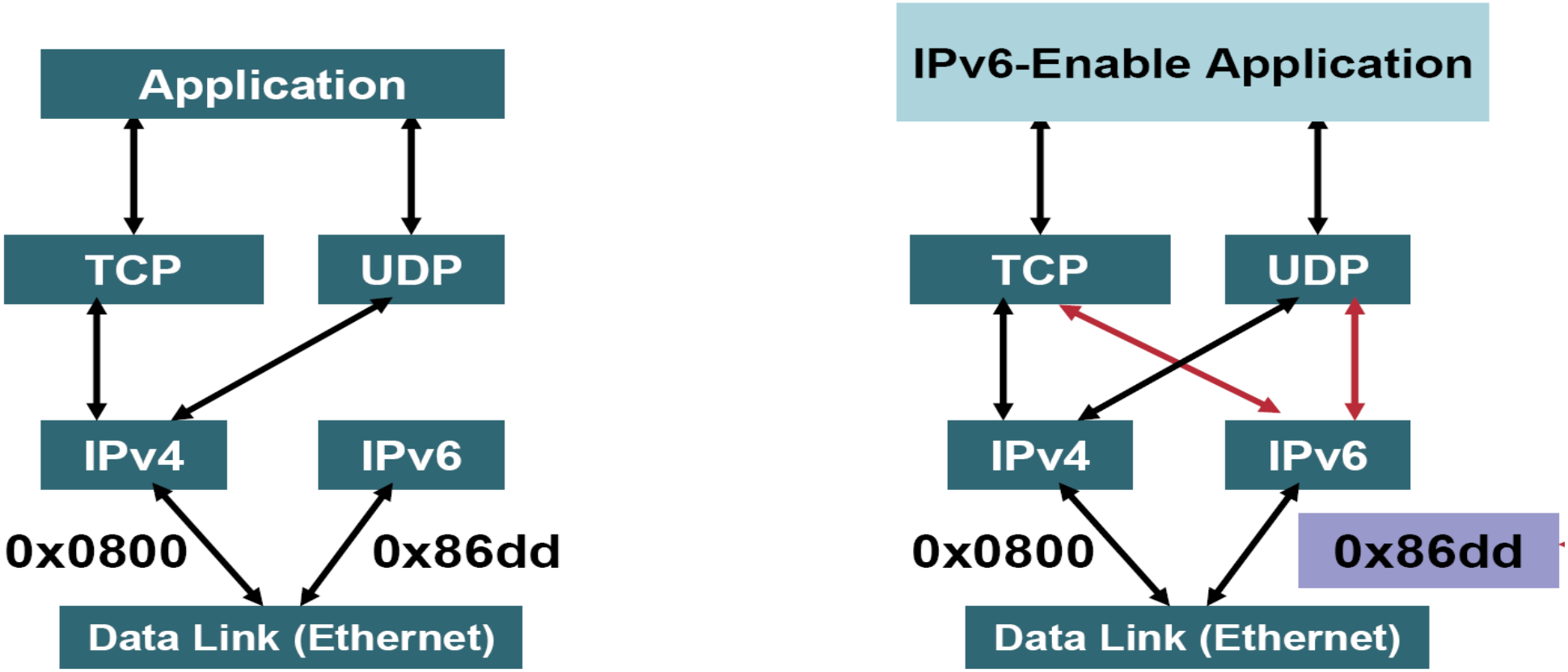
```
#router ospf 1
 #network 200.1.1.0 0.0.0.255 area 0
 #network 200.0.0.1 0.0.0.0 area 0
!
#router ospf 2
 #network 10.0.0.0 0.255.255.255 area 0
 #network 192.168.0.0 0.0.255.255 area 1
```

IPv6 Deployment Techniques

- Deploying IPv6 using dual-stack backbones
  - IPv4 and IPv6 applications coexist in a dual IP layer routing backbone
  - All routers in the network need to be upgraded to be dual-stack
- IPv6 over IPv4 tunnels
  - Manually configured
    - With and without Generic Routing Encapsulation (GRE)
  - Semiautomatic tunnel mechanisms
  - Fully automatic tunnel mechanisms (IPv4-compatible and 6to4)

Há uns anos atrás não todos os PCs suportavam IPv4 e IPv6

Dual Stack



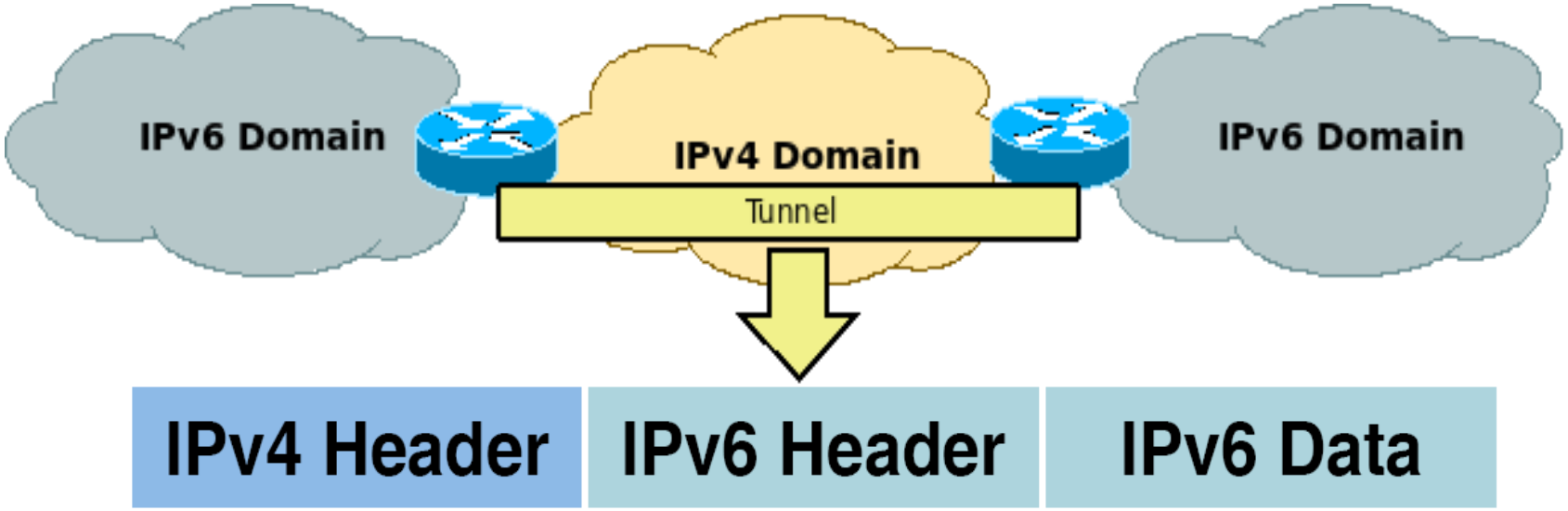
- Applications may talk to both
- Choice of the IP version is based on DNS responses and application preferences

IPv6 Overlay Tunneling

- Manual
  - IPv6 Manually Configured IPv6 over IPv4
  - IPv6 over IPv4 GRE Tunnel
- Semi-automatic mechanisms
  - Tunnel Broker
  - Teredo
  - Dual Stack Transition Mechanism (DSTM)
- Automatic mechanisms
  - Automatic IPv4 Compatible Tunnel (deprecated)
  - 6to4 Tunnel
  - ISATAP Tunnels

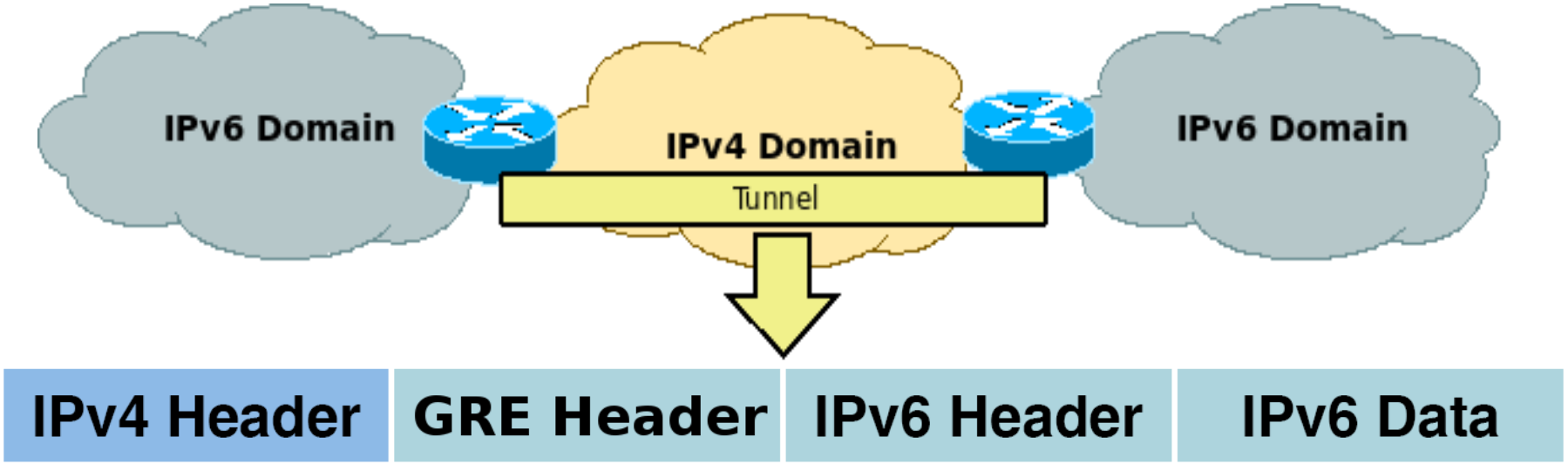
IPv6 Manually Configured

- Permanent link between two IPv6 domains over an IPv4 backbone
- Primary use is for stable connections that require regular secure communication between
  - Two edge routers, end system and an edge router, or for connection to remote IPv6 networks
- Tunnel between two points
- Complex management



IPv6 over IPv4 GRE Tunnel

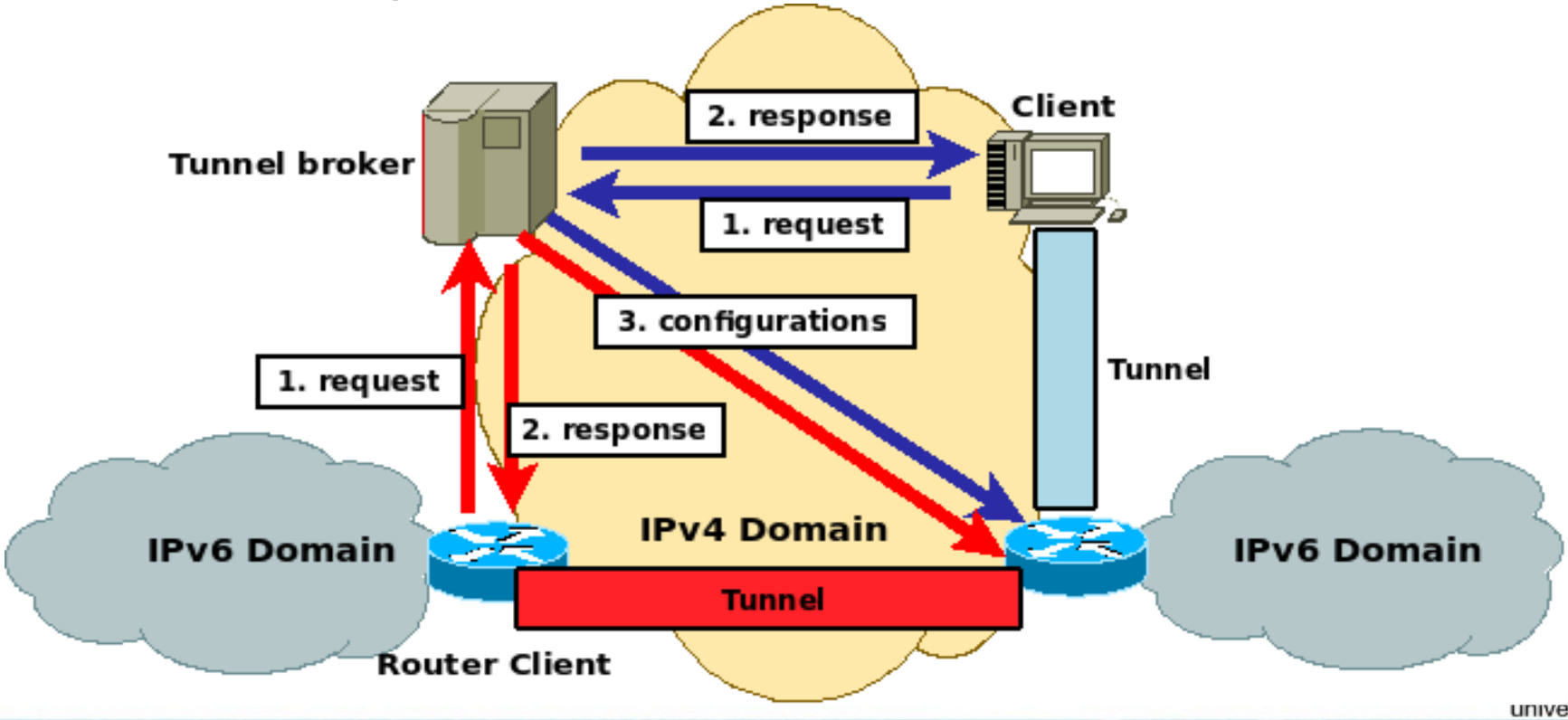
- Uses the standard GRE tunneling technique
  - GRE – Generic Route Encapsulation
- Also must be manually configured
- Primary use is for stable connections that require regular stable communications
- IPv4 over IPv6 also possible



Não é preciso uma intervenção humana. Imaginemos que era pra fazer um tunnel IPv6-IPv6 sobre IPv4, num dos Routers pedia-se o tunel, o servidor avisa ao outro Router que vai ser feito o Tunnel e ambos os Routers ficam configurados de forma semi-automática

Tunnel Broker

- A tunnel broker service allows IPv6 applications on dual-stack systems access to an IPv6 backbone
- Automatically manages tunnel requests and configuration
- Potential security implications
  - Broker is a single point of failure
- Most common implementation: Teredo.

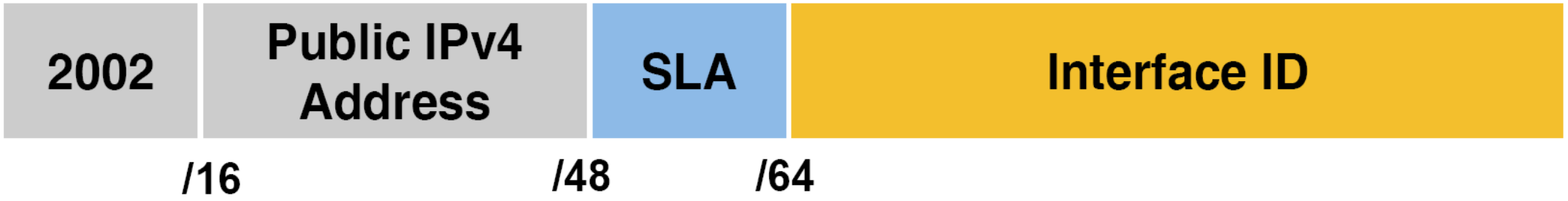


Automatic IPv4 Compatible Tunnel

- IPv4 tunnel end-point address is embedded within the destination IPv6 address
- An automatic IPv4-compatible tunnel can be configured between edge routers or between an edge router and an end system.
- Systems must be dual-stack
- Communication only with other IPv4-compatible sites
- This tunneling technique is currently deprecated

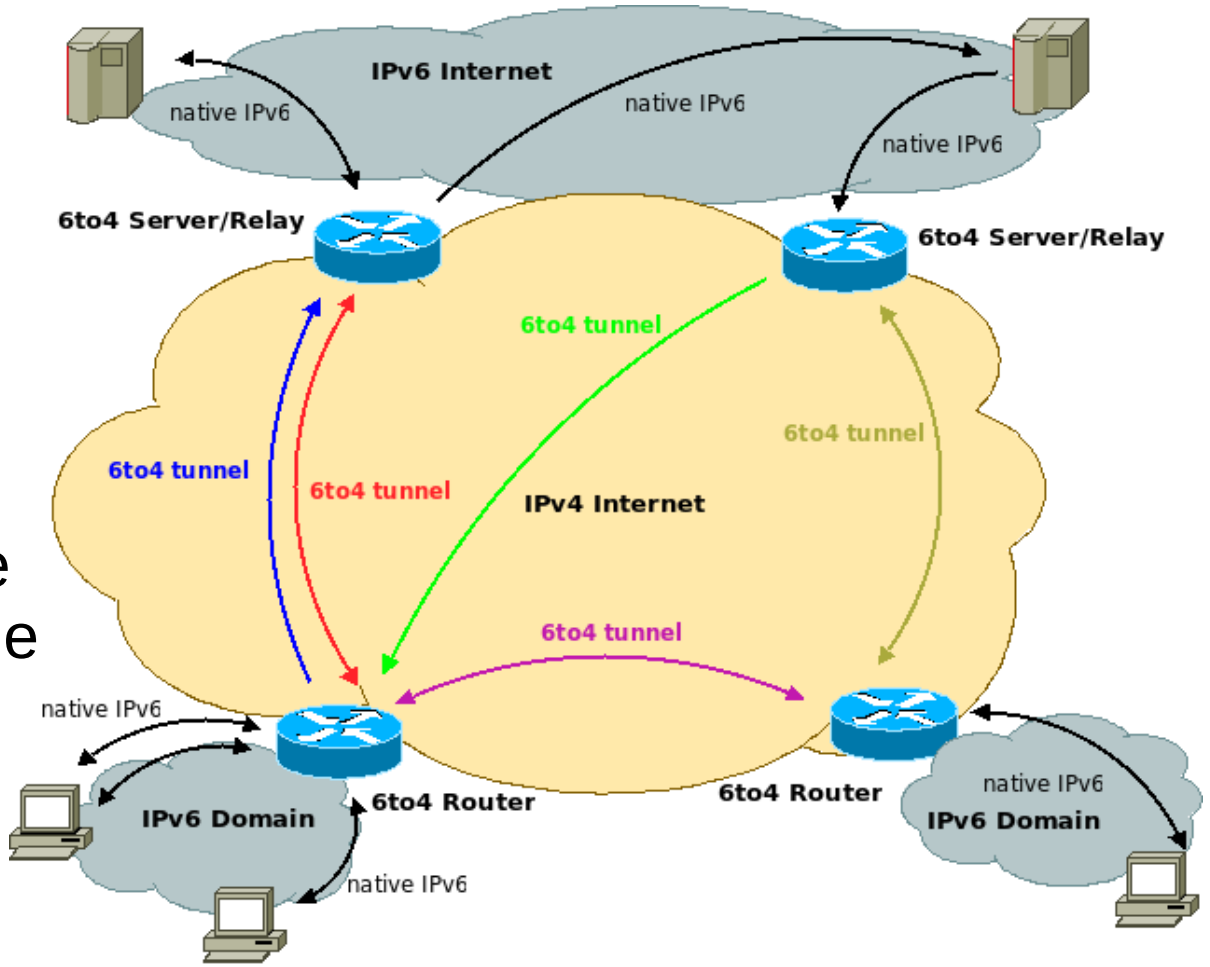
Automatic 6to4 Tunnels

- IPv4 tunnel end-point address is embedded within the destination IPv6 address
  - Automatic 6to4 tunnel allows isolated IPv6 domains to connect over an IPv4 network
  - Unlike the manually configured tunnels are not point-to-point, they are multipoint tunnels
  - 6to4 host/router needs to have a globally addressable IPv4 address
  - Cannot be located behind a NAT box
  - Unless the NAT box supports protocol 41 packets forwarding
  - Address format is:



6to4 Relay Routers

- 6to4 router
  - Connects 6to4 hosts from a IPv6 domain and
    - Other 6to4 routers
    - The IPv6 Internet through a 6to4 relay router
- 6to4 relay router
  - Connects 6to4 routers on the IPv4 Internet and hosts on the IPv6 Internet.



ISATAP Tunnels

- Intra-site Automatic Tunnel Address Protocol
- Point-to-multipoint tunnels that can be used to connect systems within a site
- Used to tunnel IPv4 within as administrative domain to create a virtual IPv6 network over a IPv4 network
- Scalable approach for incremental deployment
- Encode IPv4 Address in IPv6 Address within the interface ID