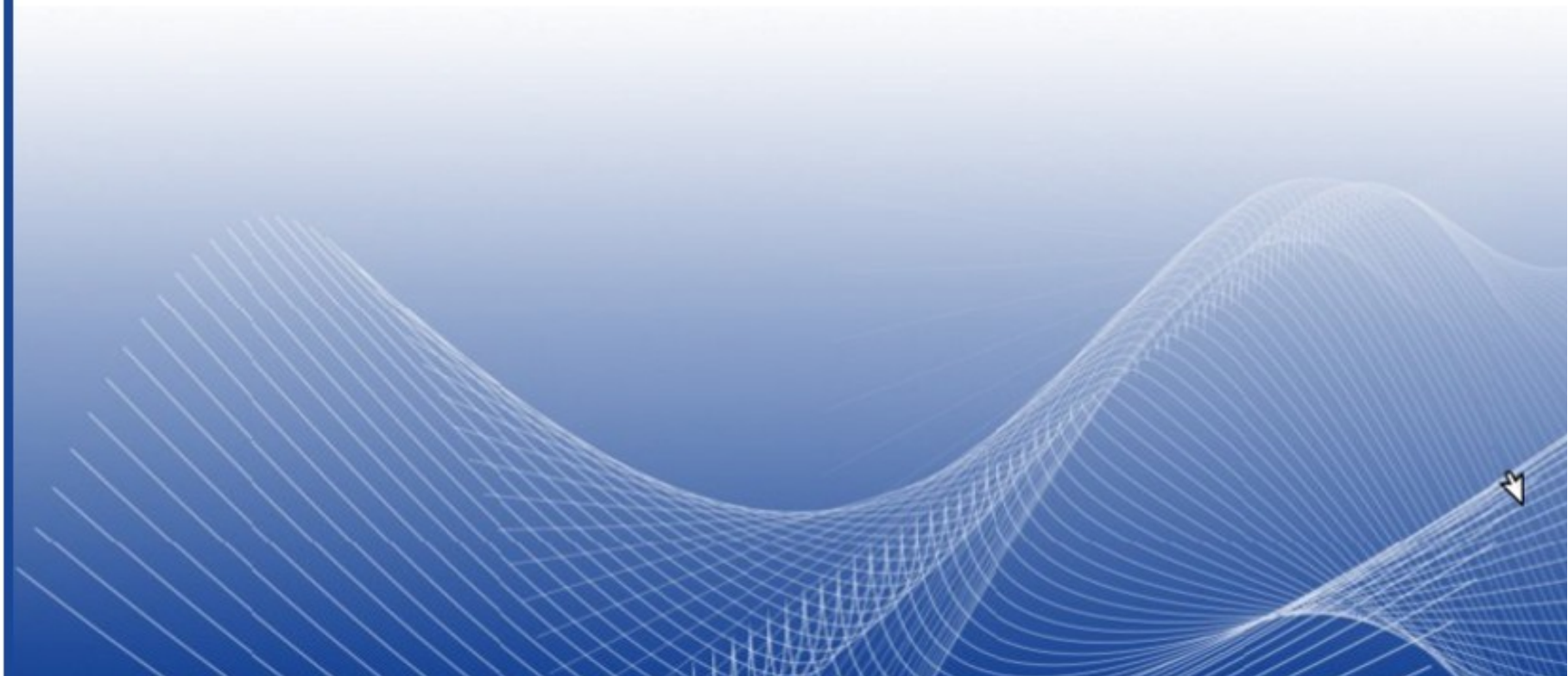
Traffic Tunneling
&
Overlay Networks

Arquitetura de Redes Avançadas



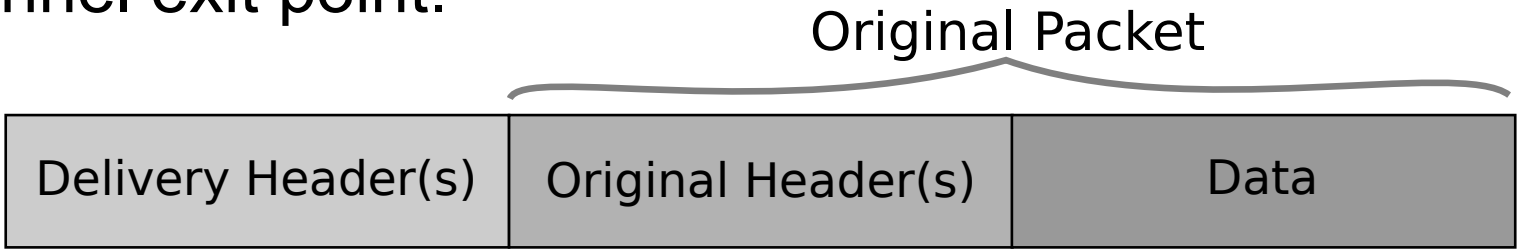
universidade de aveiro
deti.ua.pt

Traffic Tunnel Concept

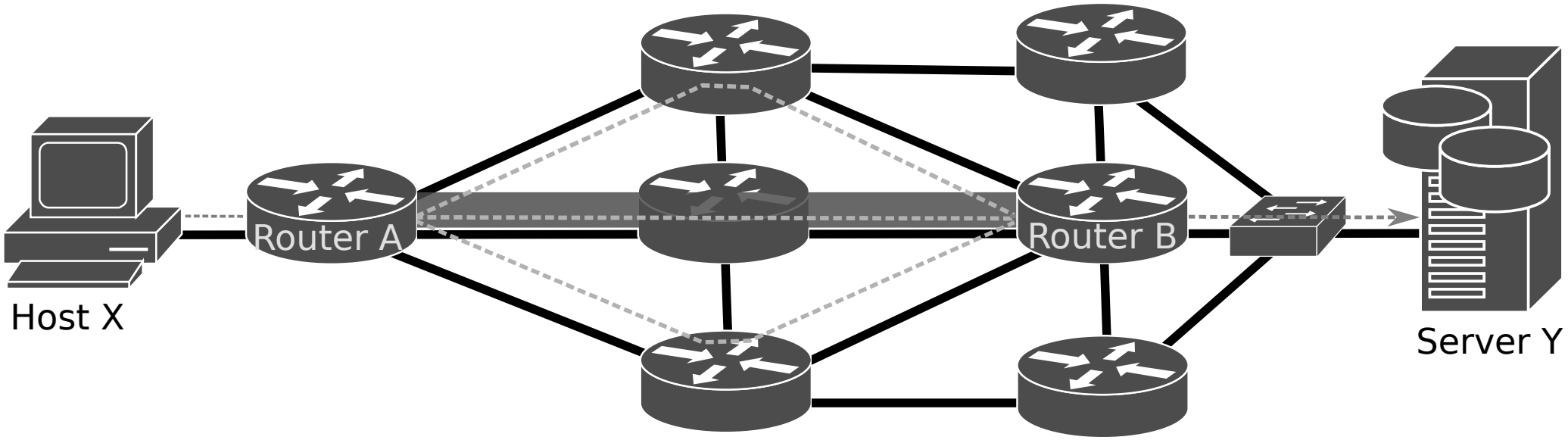
- Main purposes
  - Guarantee that a packet that reaches a network node will reach a specific secondary network node independently of the intermediary nodes routing processes,
  - Guarantee the delivery of a packet to a remote node when the intermediary nodes do not support the original packet network protocol, and,
  - Define a virtual channel that adds additional data transport features in order to provide differentiated QoS, security requirements and/or optimized routing.

ISPs can use to give networks to clients and define policies (bandwith, etc.)

- 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

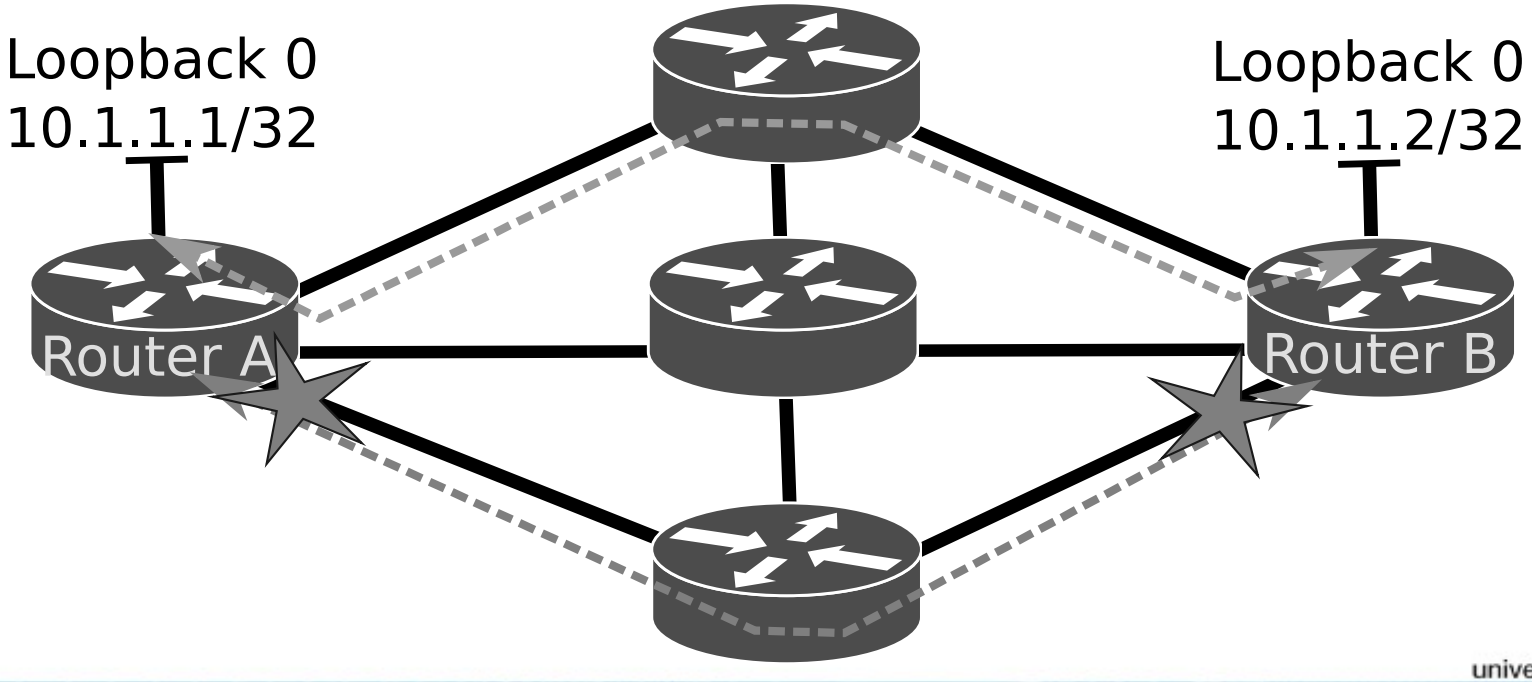
- A numeric identifier,
- A bounded IP address, this will enable IP processing,
  - Add the tunnel interface to the routing table and allow routing via the interface,

```
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.

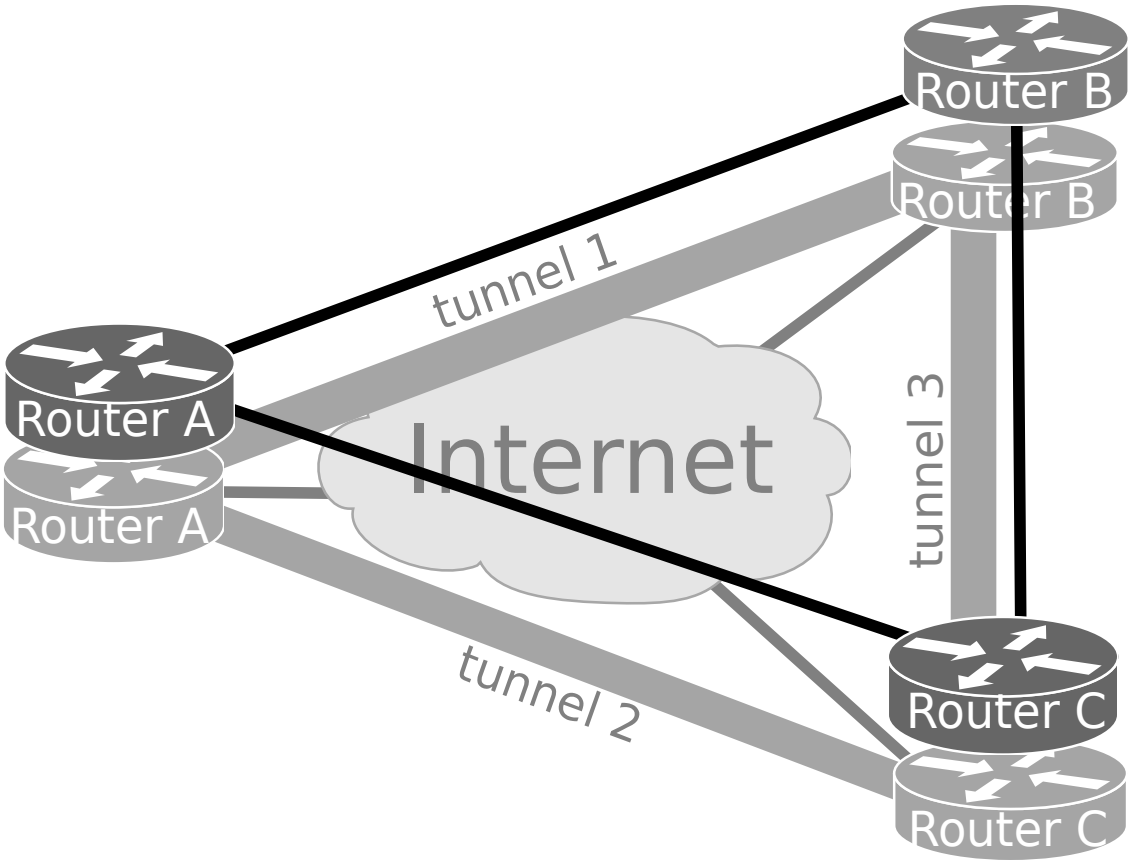


IP Tunnel Types

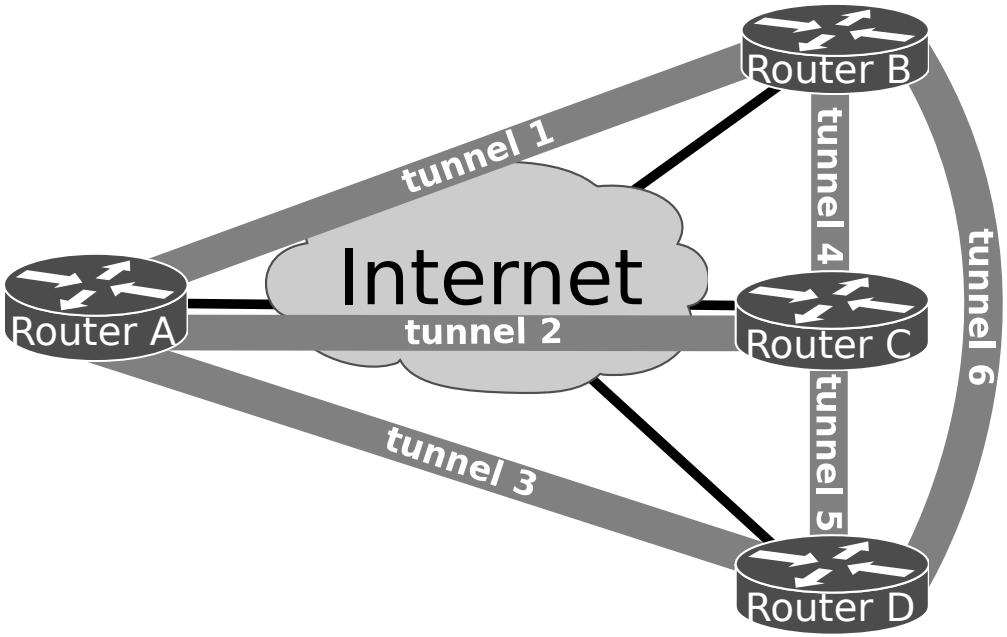
- IPv4-IPv4
  - Original IPv4 packets are delivered using IPV4 as network protocol.
- IPv6-IPv4
  - Original IPv6 packets are delivered using IPv4 as network protocol.
- IPv4-IPv6
  - Original IPv4 packets are delivered using IPv6 as network protocol.
- IPv6-IPv6
  - Original IPv6 packets are delivered using IPv6 as network protocol.
- GRE IPv4
  - Original packets protocol (any network protocol) is defined by GRE header and delivered using IPv4 as network protocol.
- GRE IPv6
  - Original packets protocol (any network protocol) is defined by a GRE header and delivered using IPv6 as network protocol.

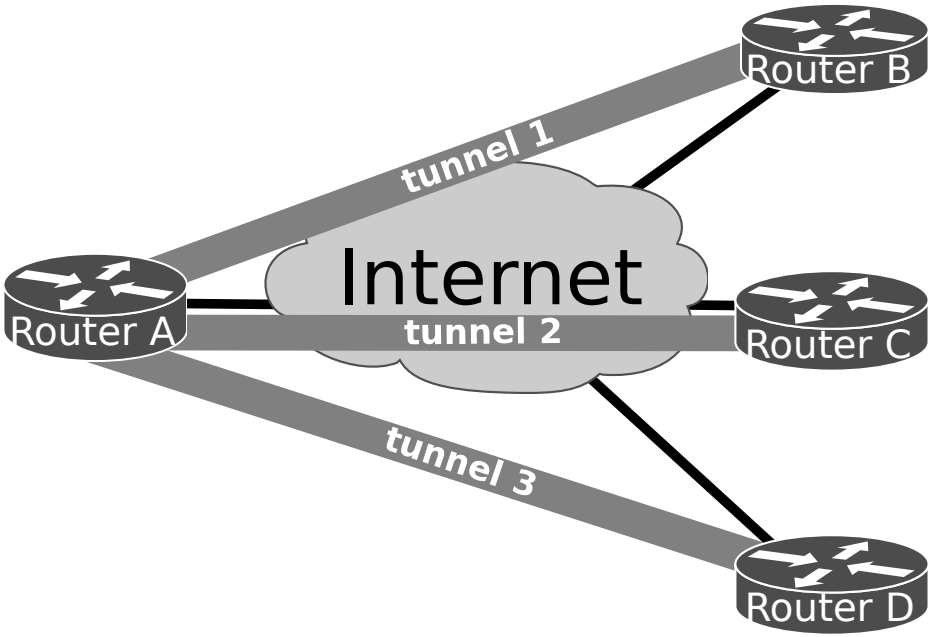
Overlay Network

- 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).



Full/Partial Overlay Mesh

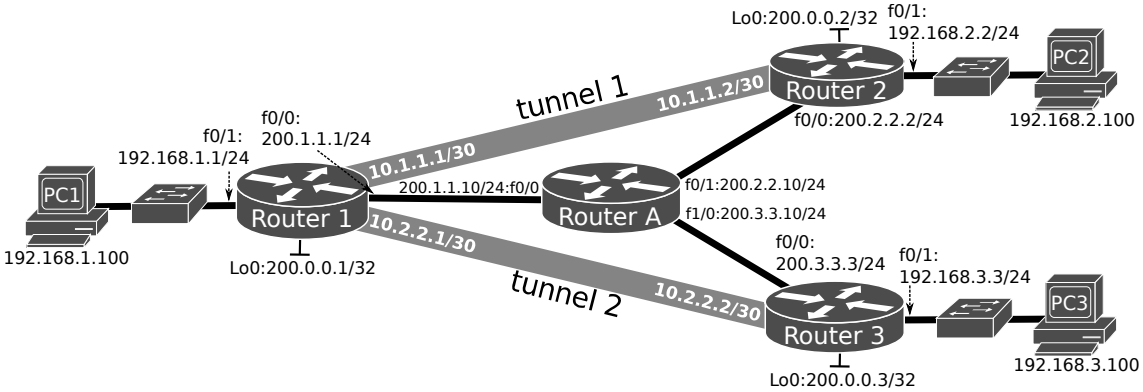




Routing Through/Between Tunnels

- 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
```



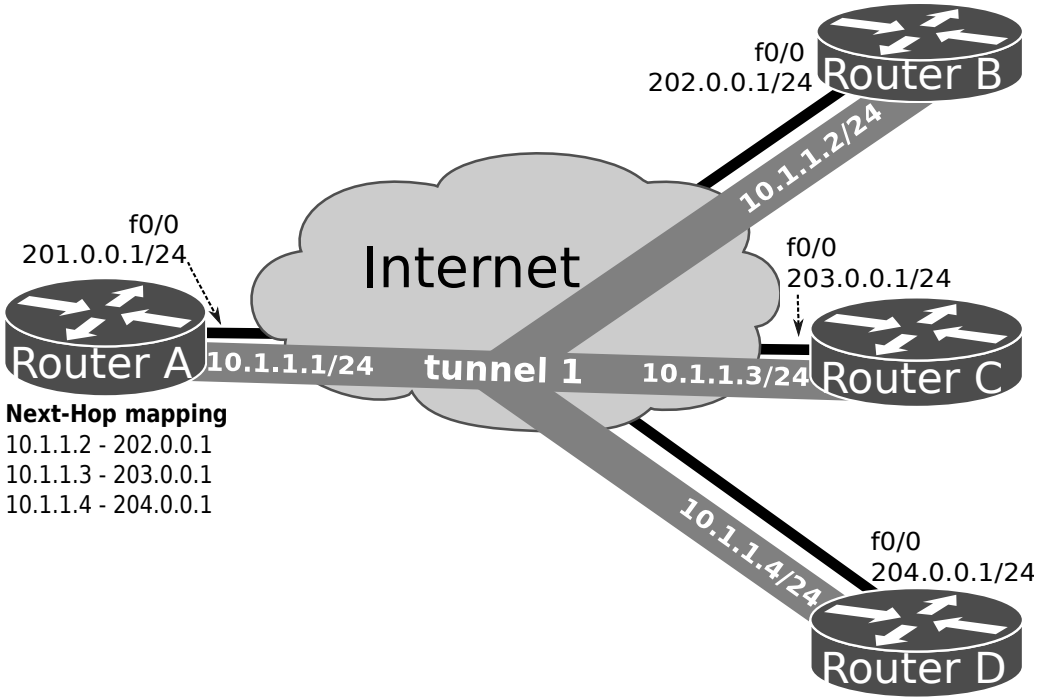
- Route-maps

```
#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
```

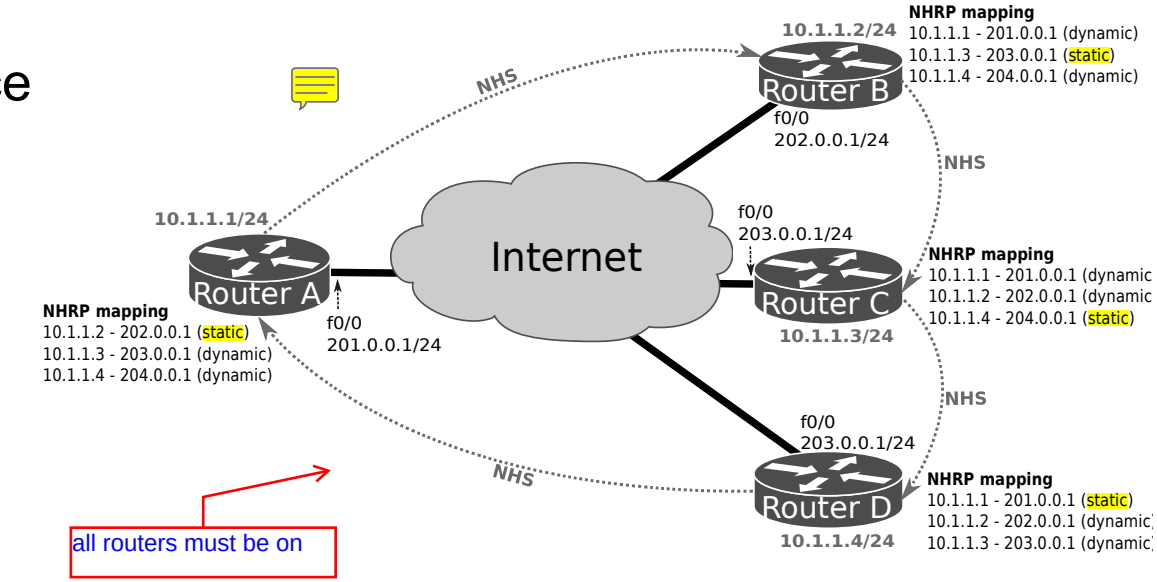
Multipoint Tunnels

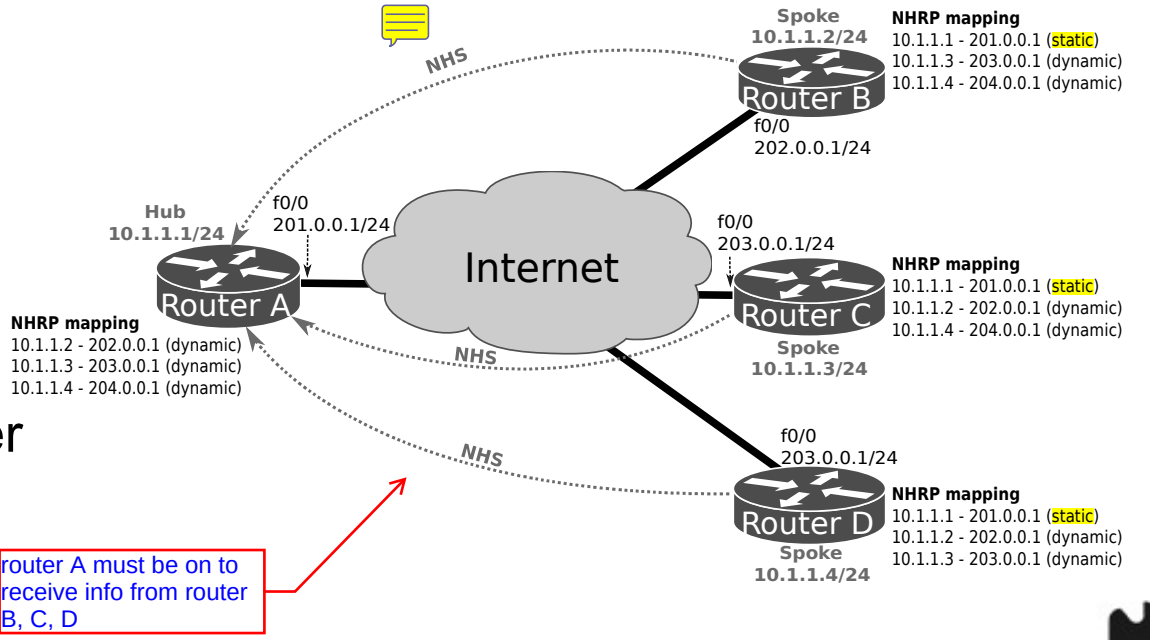


- In a scenario with many nodes to interconnect, the simpler and more efficient approach is to have a single tunnel that interconnect multiple nodes - a multipoint tunnel.
- Directly connect using a single virtual overlay IP network, defined within a multipoint tunnel.
- In a multipoint tunnel scenario, the delivery header address is determined based on the address of the next hop within the overlay network.
- Address mapping between overlay and underlying network addresses may be statically defined or dynamically obtained.

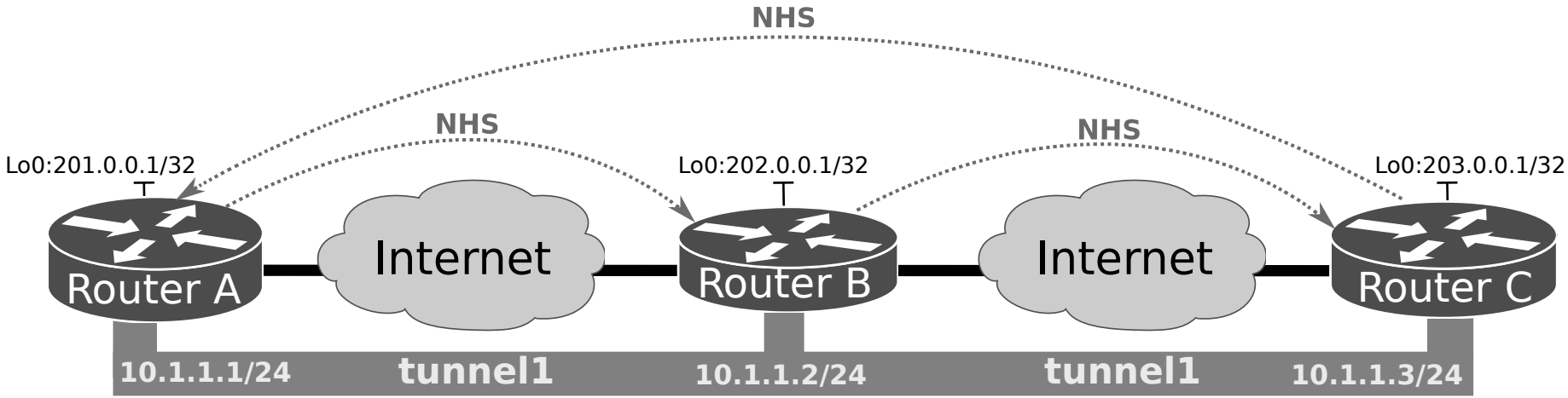
Next Hop Resolution Protocol (NHRP)

- NHRP allows to map a tunnel interface IP address (overlay network) to the respective underlying network interface IP address.
- NHRP tunnel requires that all intervening nodes should be able to find a path to any of the other nodes.
- Each node should at least know one other overlay node (and respective overlay and underlaying addresses) through which he will try to find the other nodes address mappings.
  - Next Hop Server (NHS).
- Moreover, all nodes must be configured in a way that all nodes have at least one valid path to all other nodes - forming a partial mesh.





NHRP Information Exchange



NHRP mapping
10.1.1.2 - 202.0.0.1 (static)

NHRP Register Request
10.1.1.1 - 201.0.0.1

NHRP Register Reply
10.1.1.1 - 201.0.0.1
Responder Address Extension
10.1.1.2 - 202.0.0.1

NHRP Register Request
10.1.1.2 - 202.0.0.2

NHRP mapping
10.1.1.1 - 201.0.0.1 (static)

NHRP Register Reply
10.1.1.2 - 202.0.0.1
Responder Address Extension
10.1.1.3 - 203.0.0.1

NHRP mapping
10.1.1.1 - 201.0.0.1 (static)
10.1.1.2 - 202.0.0.1 (dynamic)

NHRP Resolution Request
10.1.1.1 - 201.0.0.1
10.1.1.3 - ?

NHRP Resolution Reply
10.1.1.1 - 201.0.0.1
10.1.1.3 - 203.0.0.1
Responder Address Extension
10.1.1.2 - 202.0.0.1

NHRP mapping
10.1.1.2 - 202.0.0.1 (static)
10.1.1.3 - 203.0.0.1 (dynamic)

NHRP Resolution Request
10.1.1.2 - 202.0.0.1
10.1.1.3 - ?

NHRP Resolution Reply
10.1.1.2 - 202.0.0.1
10.1.1.3 - 203.0.0.1
Responder Address Extension
10.1.1.3 - 203.0.0.1

If "10.1.1.3 - 203.0.0.1" entry not on RouterB NHRP mapping