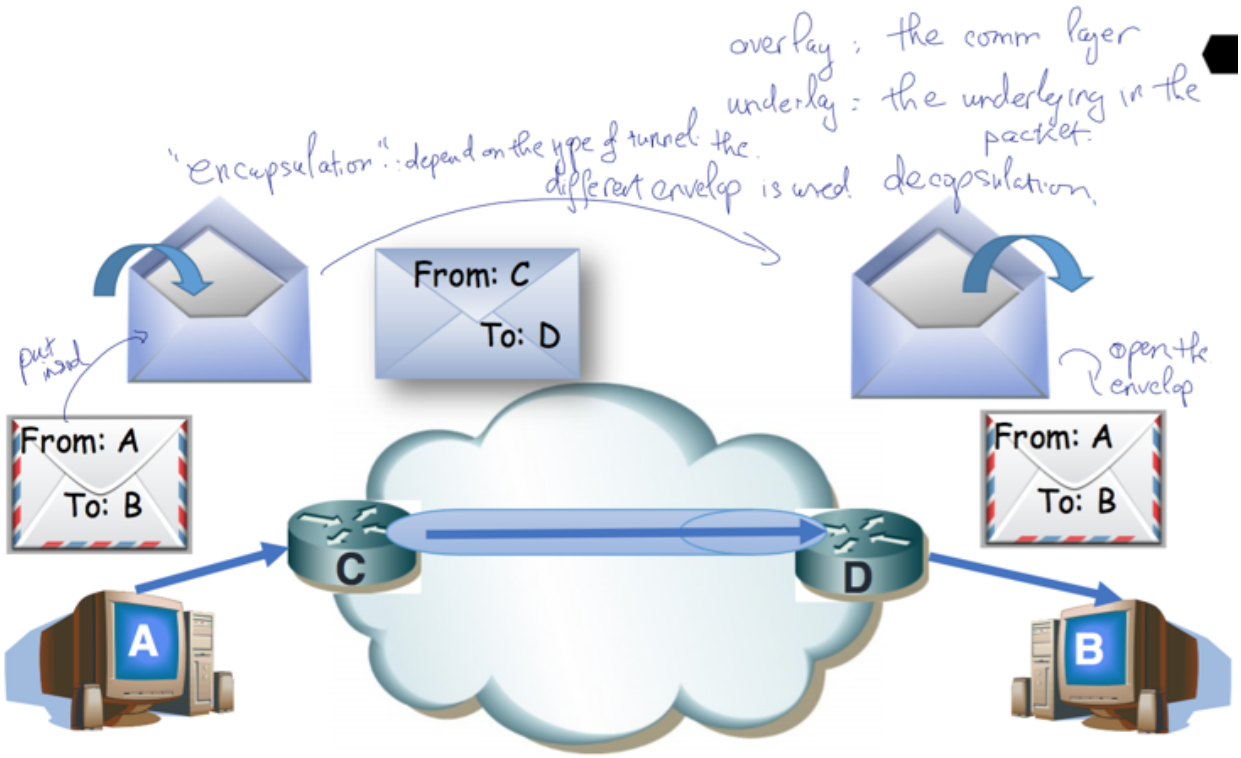
Chapter 05 - TUNNELS

Definition

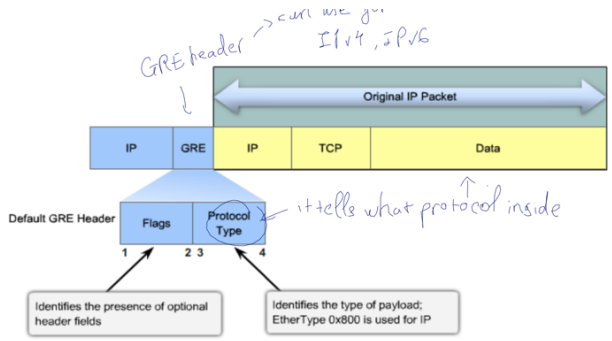
- Use for encrypted path through a public network (IPSec) by encapsulating a packet



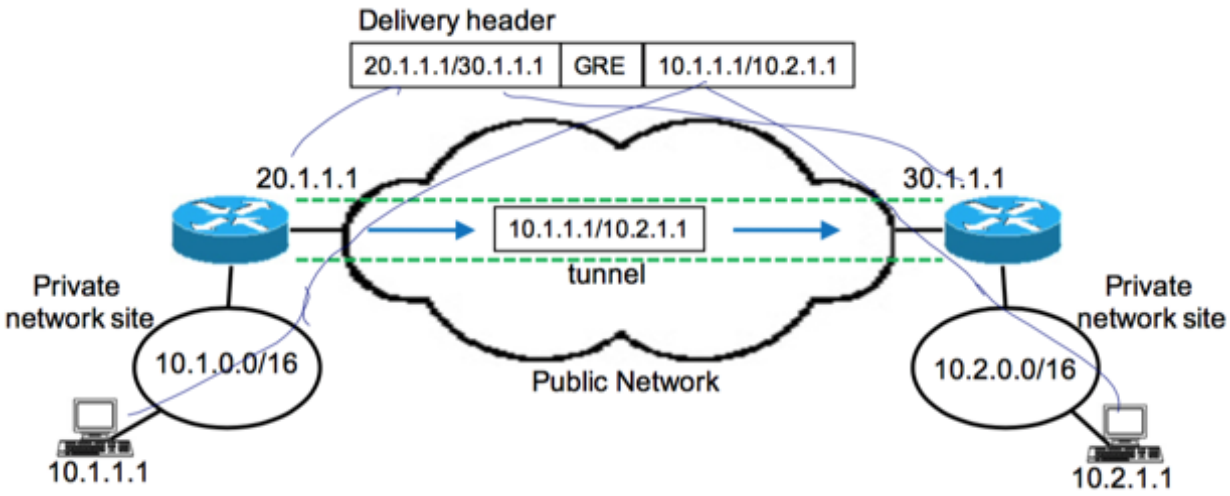
GRE (Generic Routing Encapsulation)

> *Specifies a protocol for encapsulation of an arbitrary protocol over another arbitrary network layer protocol.*

- Used for IPv4 over IPv6 (4in6), IPv6 over IPv4 (6in4)
- Support multicast, broadcast.
- No default encryption (different than IPSec). Can have IPSec Tunnel over GRE (additional header).
- Notes: **GRE header is 4 bytes** minimum.



Example



- RFC 2784 – Generic Routing Encapsulation

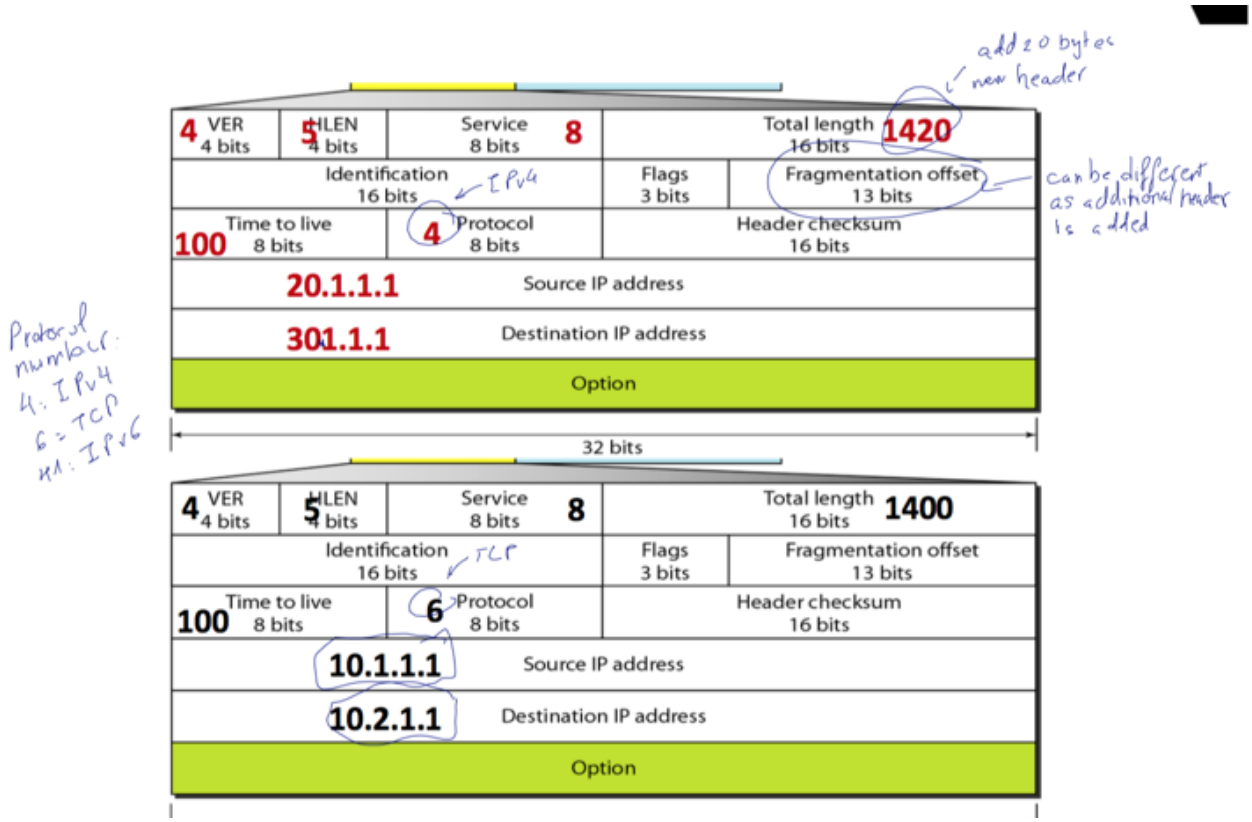
```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|       Reserved0          | Ver |         Protocol Type         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Checksum (optional)      |       Reserved1 (Optional)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

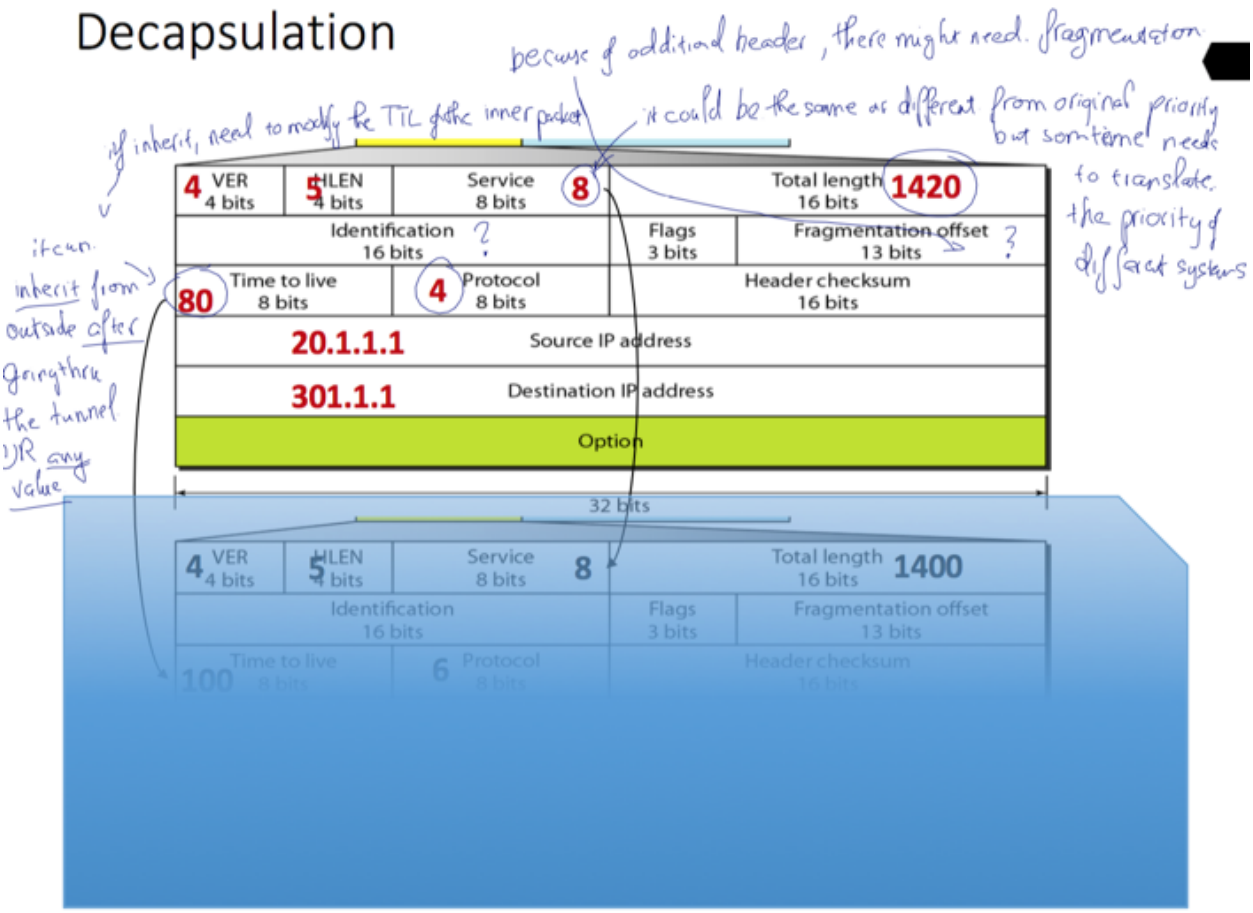
must have
others are optional

Protocol Type – EtherType in RFC 1700. Examples below:

EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x86DD	Internet Protocol Version 6 (IPv6)

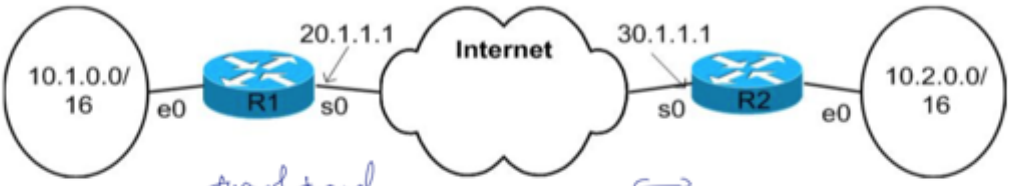
Encapsulation (IPv4/IPv4)


add 20 bytes new header
4 VER 4 bits
5 HLEN 4 bits
Service 8 bits
8
Total length 16 bits
1420
Identification 16 bits
IPv4
Flags 3 bits
Fragmentation offset 13 bits
can be different as additional header is added
100 Time to live 8 bits
4 Protocol 8 bits
Header checksum 16 bits
20.1.1.1 Source IP address
301.1.1 Destination IP address
Option
Protocol number: 4: IPv4 6 = TCP 41: IPv6
32 bits
4 VER 4 bits
5 HLEN 4 bits
Service 8 bits
8
Total length 16 bits
1400
Identification 16 bits
TCP
Flags 3 bits
Fragmentation offset 13 bits
100 Time to live 8 bits
6 Protocol 8 bits
Header checksum 16 bits
10.1.1.1 Source IP address
10.2.1.1 Destination IP address
Option


Decapsulation
because of additional header, there might need fragmentation
if inherit, need to modify the TTL of the inner packet
it could be the same as different from original priority but sometime needs to translate the priority of different systems
it can inherit from outside after going thru the tunnel OR any value
4 VER 4 bits
5 HLEN 4 bits
Service 8 bits
8
Total length 16 bits
1420
Identification 16 bits
Flags 3 bits
Fragmentation offset 13 bits
80 Time to live 8 bits
4 Protocol 8 bits
Header checksum 16 bits
20.1.1.1 Source IP address
301.1.1 Destination IP address
Option
32 bits
4 VER 4 bits
5 HLEN 4 bits
Service 8 bits
8
Total length 16 bits
1400
Identification 16 bits
Flags 3 bits
Fragmentation offset 13 bits
100 Time to live 8 bits
6 Protocol 8 bits
Header checksum 16 bits

GRE Routing

Generic Routing Encapsulation (GRE)



type of tunnel

Symmetric conn

```
interface tunnel0
  mode GRE
  tunnel source 20.1.1.1
  tunnel destination 30.1.1.1
!
ip route 10.2.0.0 255.255.0.0 tunnel0
```

```
interface tunnel0
  mode GRE
  tunnel source 30.1.1.1
  tunnel destination 20.1.1.1
!
ip route 10.1.0.0 255.255.0.0 tunnel0
```

if want to reach this IP use this tunnel0

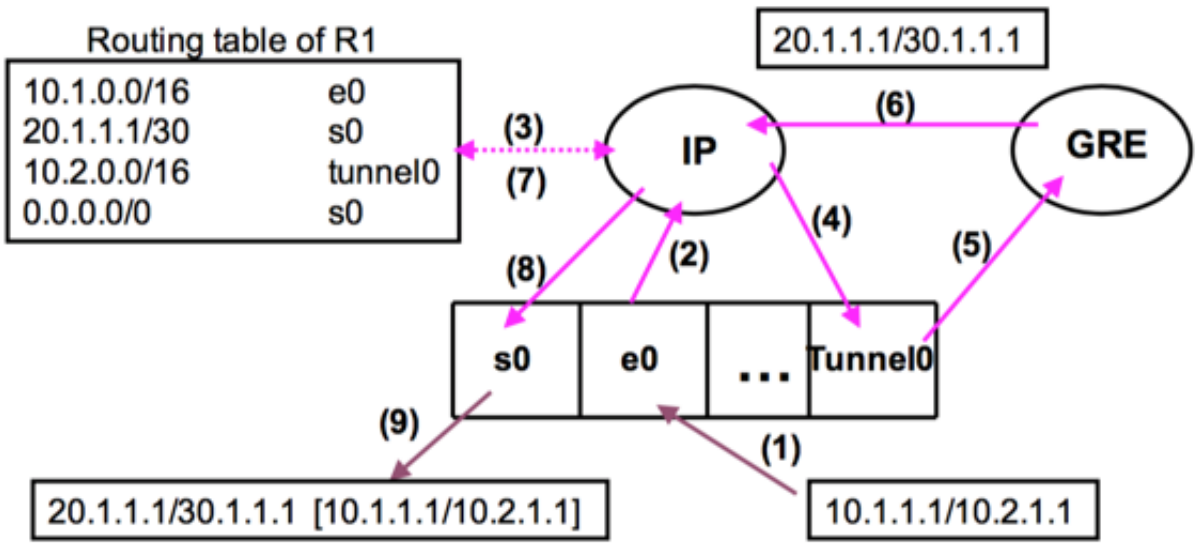
Routing table of R1

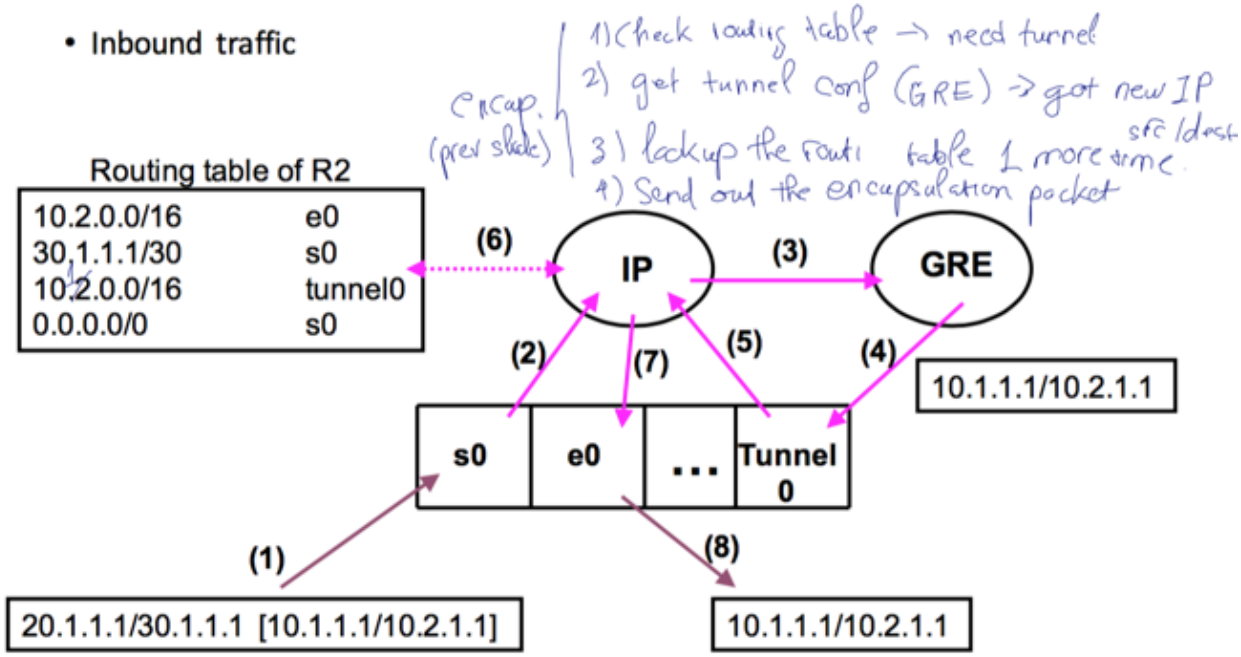
10.1.0.0/16	e0
20.1.1.1/30	s0
10.2.0.0/16	tunnel0
0.0.0.0/0	s0

Routing table of R2

10.2.0.0/16	e0
30.1.1.1/30	s0
10.1.0.0/16	tunnel0
0.0.0.0/0	s0

- Outbound traffic

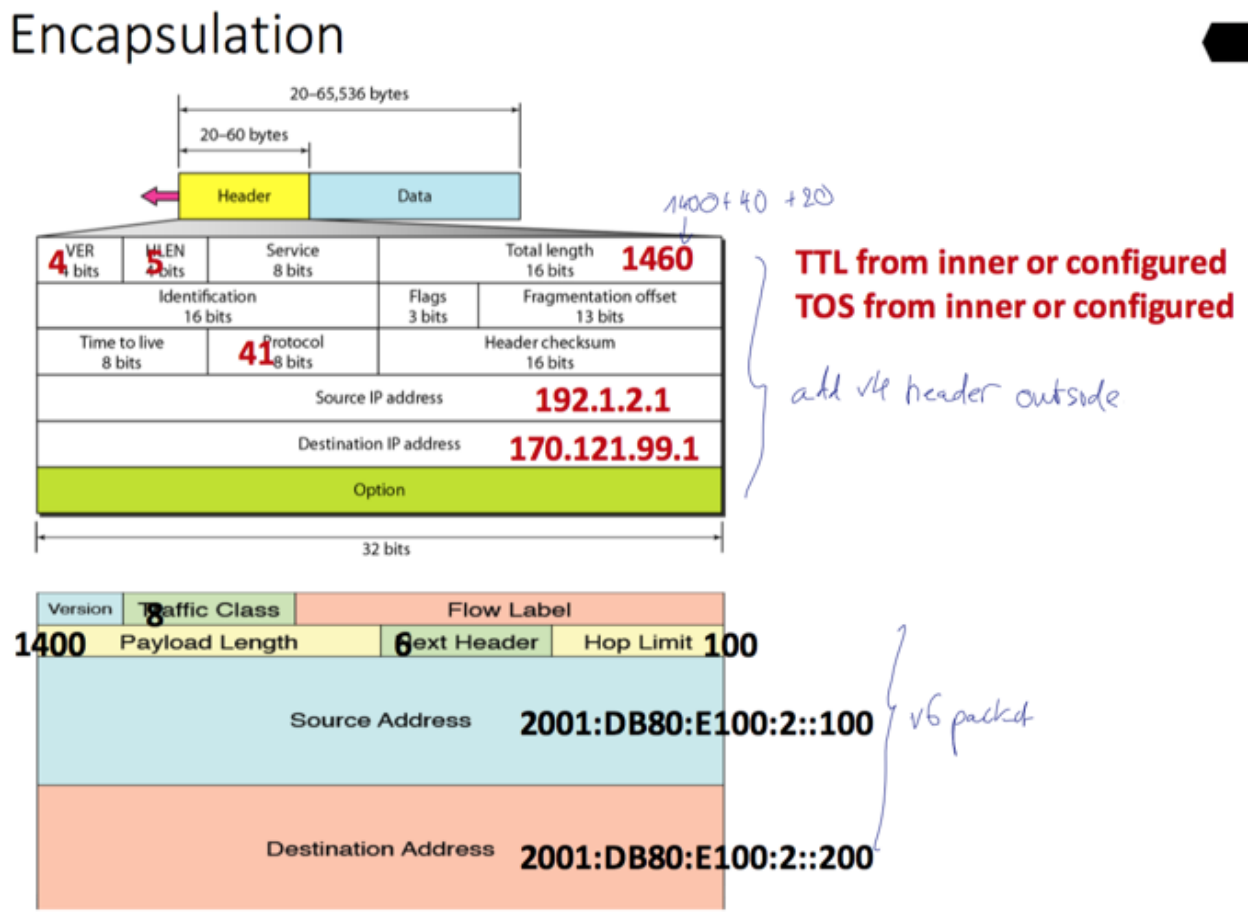




Tunnel is also used as one of the 3 strategies to migrate from IPv4 to IPv6.

- Dual Stack system: router able to speak IPv4 and IPv6 at the same time
- Tunneling: 6in4
- Header translation: IPv6 header is translated to IPv4 at certain router where destination network does not support IPv6 yet. Payload remains the same.

Encapsulation (IPv4/IPv6 i.e. 6in4)

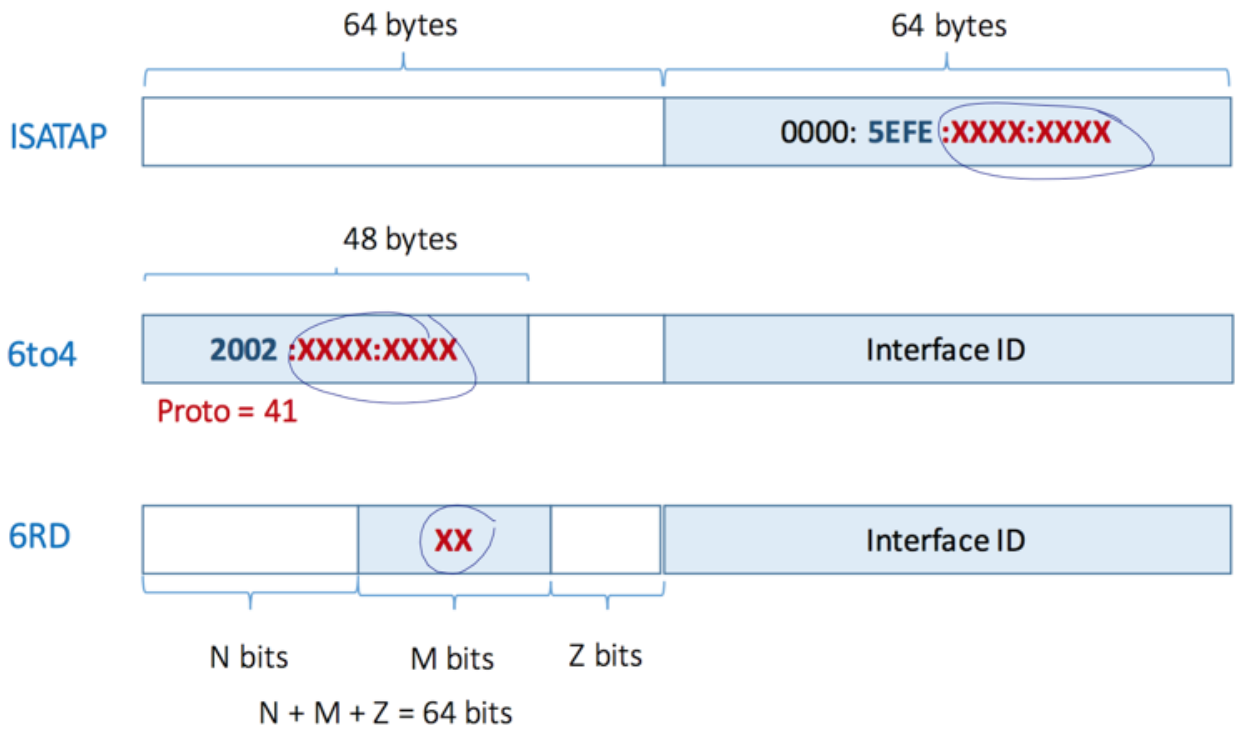


Some issues with Tunnel:

- MTU Fragmentation
- ICMPv4 error handling: only send ICMP back to the tunnel source, the origin does not know.
- Filtering protocol 41: does not know what inside, so drop the tunnel packet
- NAT

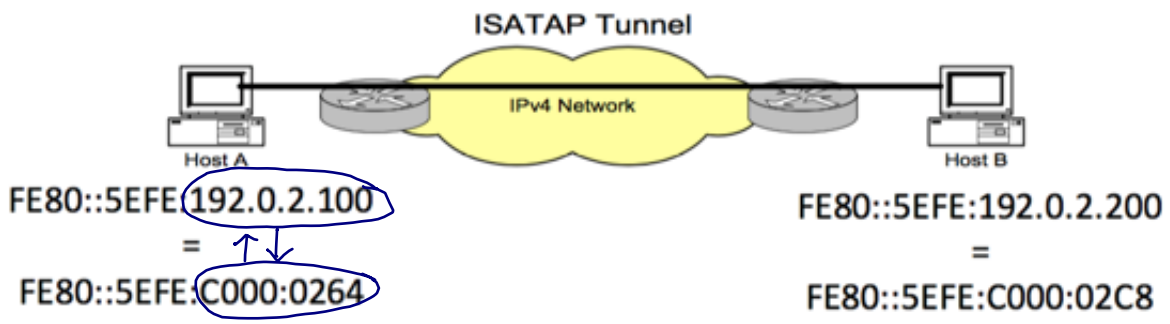
IPv6 Tunnel Address Format

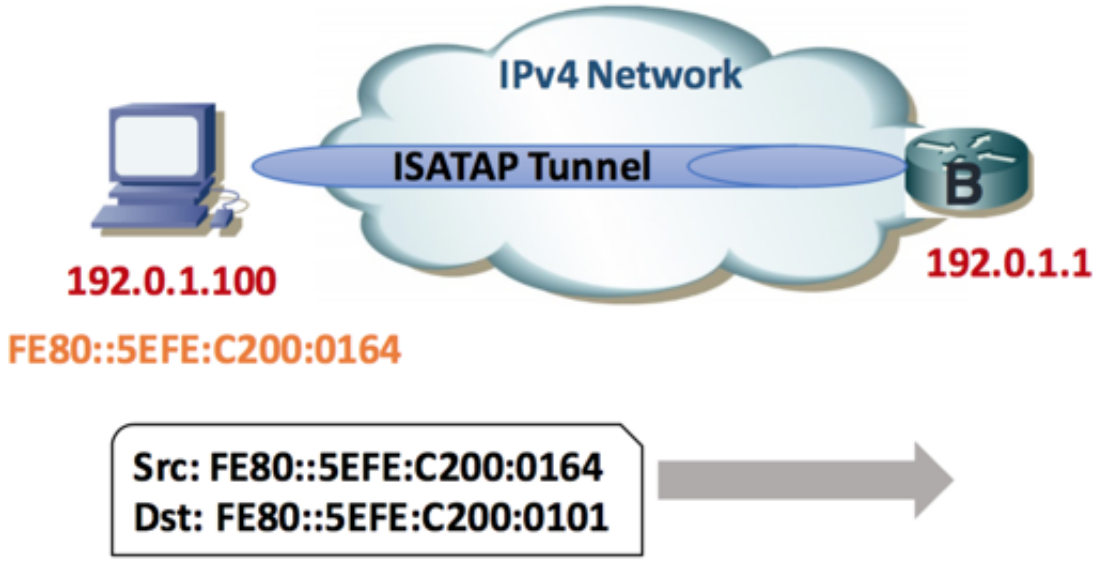
- Includes: **ISATAP**, **6to4**, and **6RD**



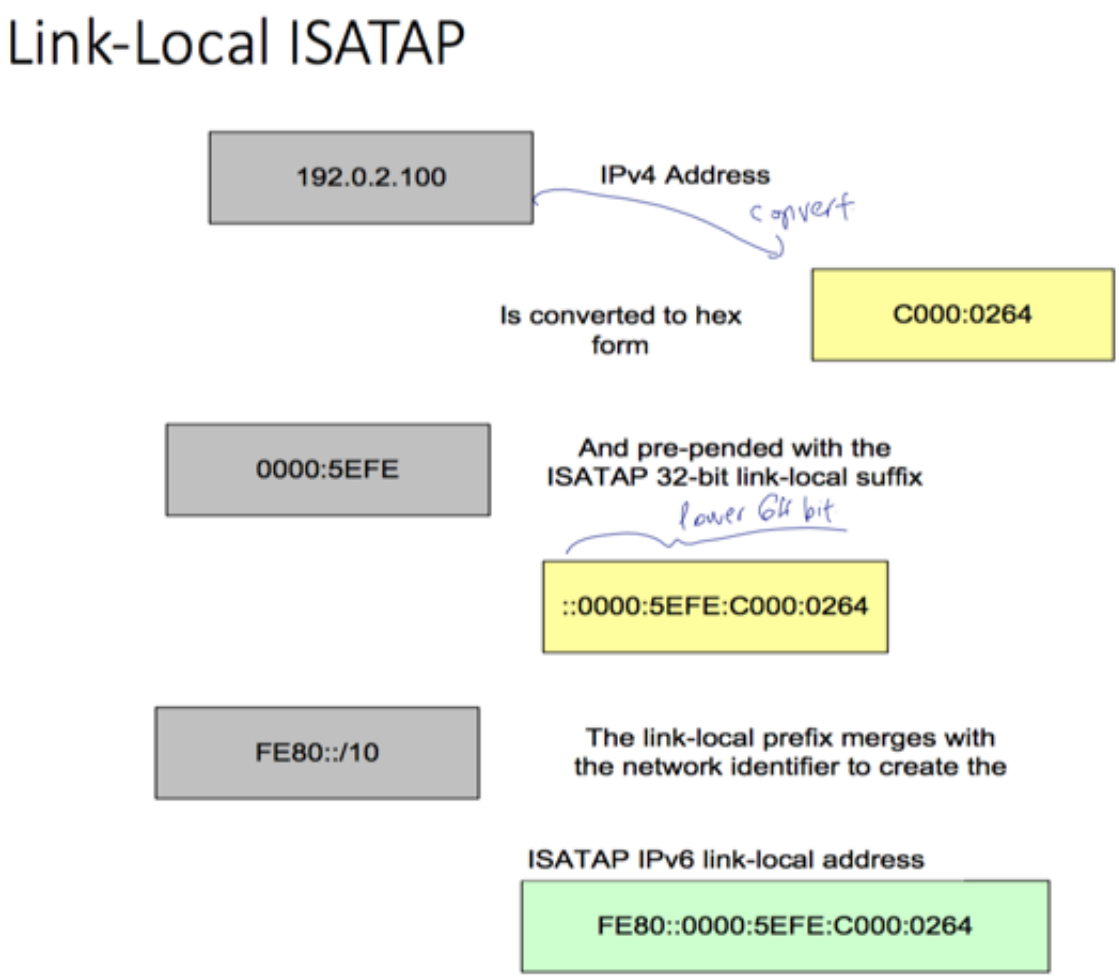
ISATAP (Intra-Site Automatic Tunneling Address Protocol)

> **ISATAP** is a managed technology for providing IPv6 on an IPv4 network. It emulates IPv6 connectivity on the IPv4 infrastructure. IPv6 Router Discovery usually uses multicast. This isn't possible on an infrastructure based on IPv6-over-IPv4 tunnels, so ISATAP solves that in a different way. An ISATAP router is provided on the network and its IPv4 address is made known to the ISATAP hosts (usually using the hostname isatap. in DNS). The ISATAP hosts then can use that address to set up their IPv6 connectivity.





This is how an IPv4 address is converted to a Link-Local ISATAP IPv6 address in above example:

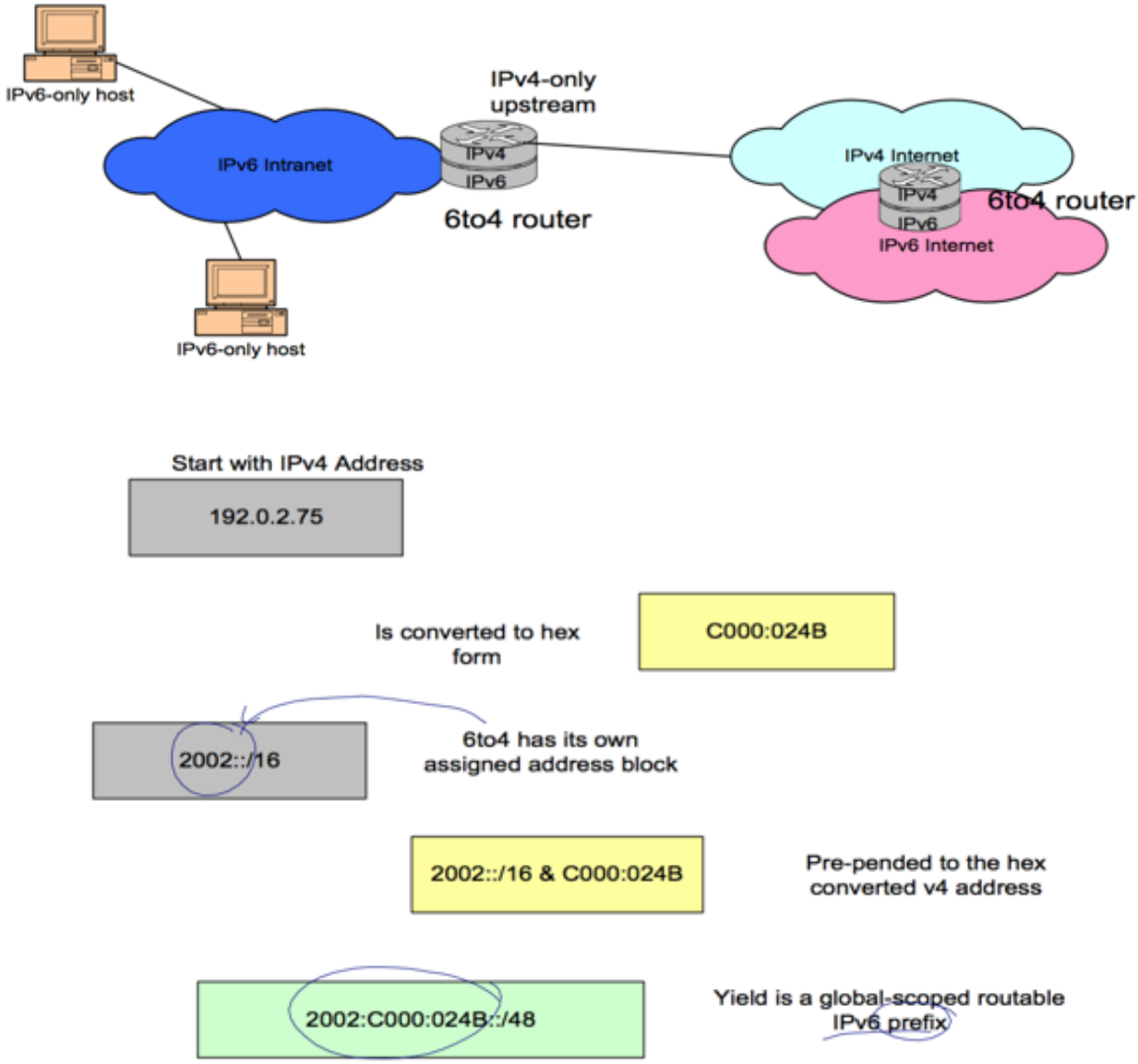


- ISATAP is also globally-routable, through ISATAP routers.
- It scales better than manually configured tunnels inside the enterprise.
- No authentication protocol.

6to4

> ***6to4*** *is a mechanism where a router with a public IPv4 address can be an IPv6 gateway/provider for a whole set of LANs. The IPv6 prefix starts with 2002: followed by the 32*

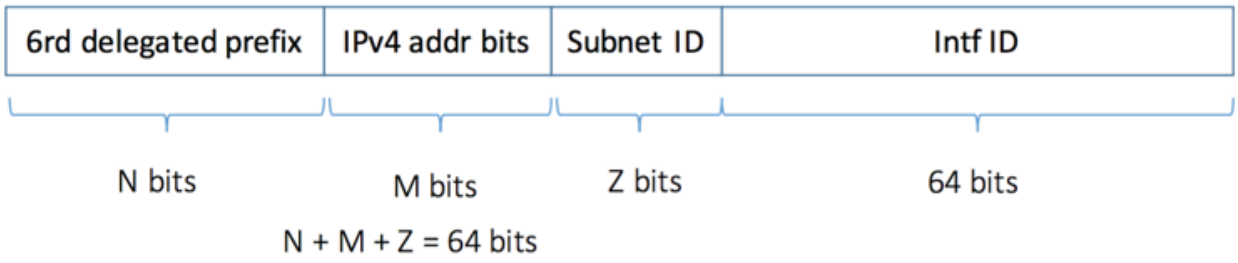
> *bits of the public IPv4 address. This gives a /48 prefix which can be used to provide 65536 LANs with a /64 each. The problem is that to reach the normal IPv6 internet the 6to4 router needs to use public 6to4 relays, and these relays are not always reliable. Add to this that the inbound and outbound traffic use different relays most of the time, and the reliability of 6to4 networks leaves a lot to be desired. These days using 6to4 is strongly discouraged.*



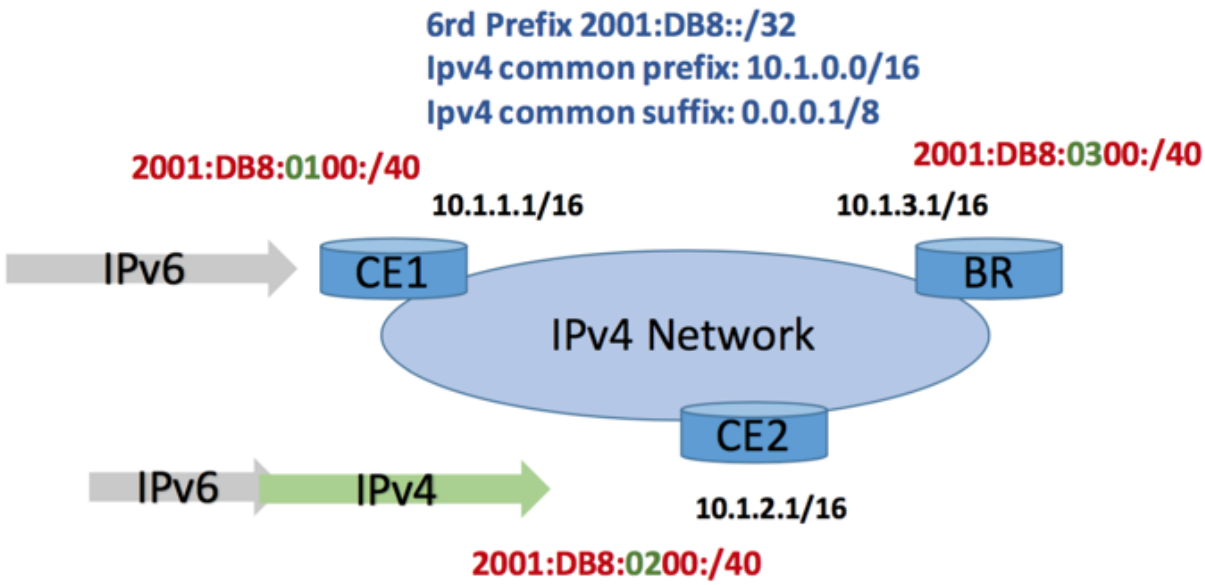
6RD

> *Derived from 6to4. Comparison to 6to4:*
> *6to4 works by relaying traffic between native IPv6 and IPv4 using relay servers which advertise common IPv4 and IPv6 prefixes to networks they are prepared to provide relay services for, but there is no guarantee that all native IPv6 hosts have a working route toward such a relay. Because of this, a 6to4 host is not guaranteed to be reachable by all native IPv6 hosts. Even when a relay is available, it is often operated by a third party who has no obligation to maintain a good quality of service as traffic grows. 6rd changes this model by making each ISP use one of its own IPv6 prefixes instead of the special 2002::/16 prefix standardized for 6to4,[8] so a provider is guaranteed that its 6rd hosts will be reachable from all native IPv6 hosts that can*

> *reach their IPv6 network. Because the relay is fully under the ISP's control, it keeps full responsibility for the quality of service for its customers.*
> *Because 6rd relays can only be used by a limited set of hosts that are all under the control of the same administrative entity, it also reduces the scope for traffic anonymization attacks such as those possible with 6to4.*



Parameter	Value
6rd Prefix/length	2001:DB8::/32
IPv4 Common prefix/length	10.1.0.0/16
IPv4 Common suffix/length	0.0.0.1/8



IPv6: 2001:DB8:0100::C15C:0 → 2001:DB8:0200::C26B:0
IPv4: 10.1.1.1 → 10.2.1.1