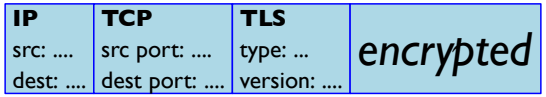
Authenticated and Confidential Communication

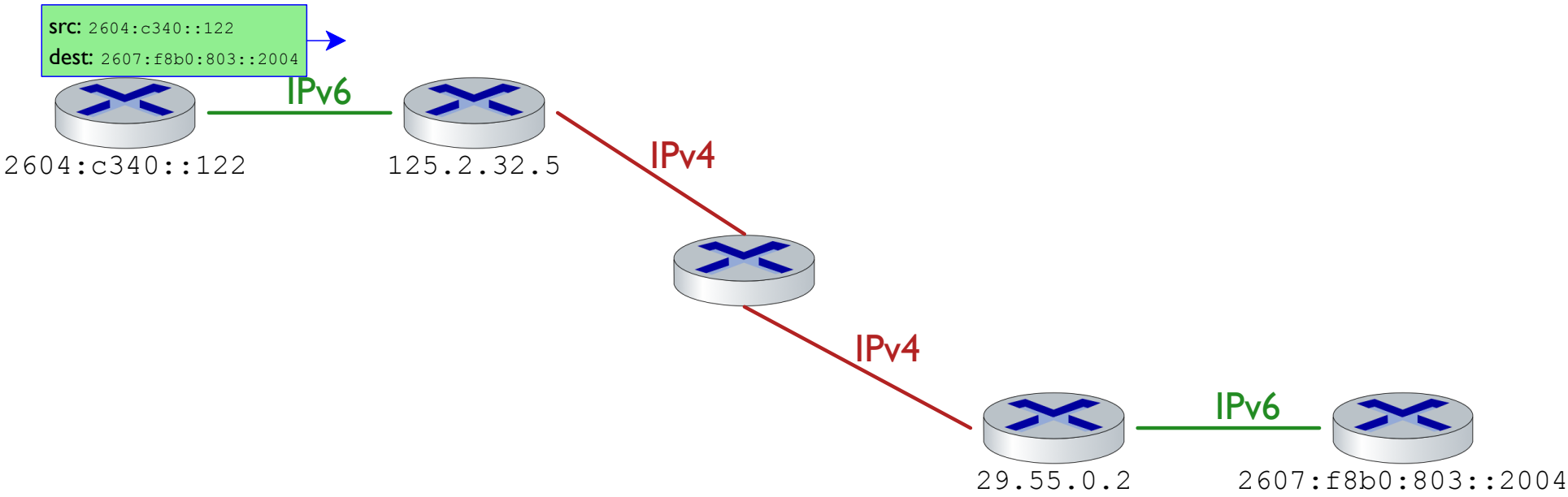


- Data in packet is encrypted and authenticated, but source and distination address are not
- Anyone can send a packet to any IP address

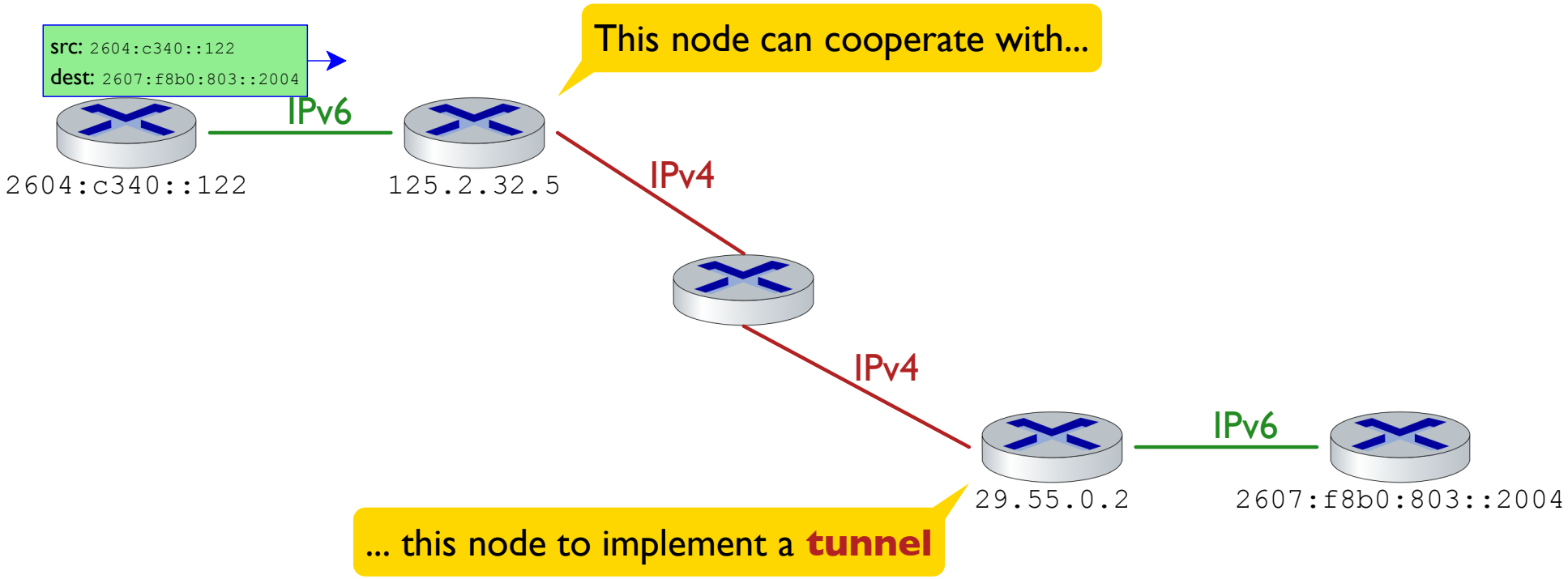
Addressing these problems requires a new protocol at the network layer

Since changing IP is not practical, that leaves **tunneling** as an option

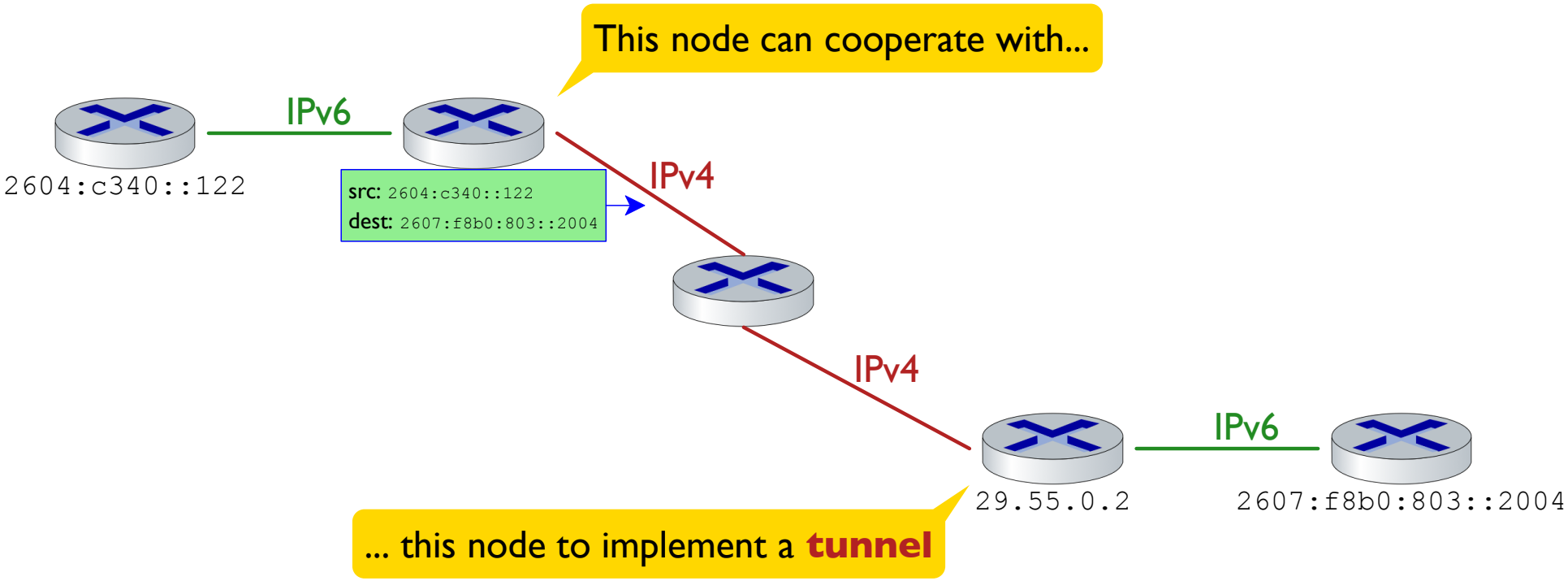
Earlier Tunneling Example: IPv6 over IPv4



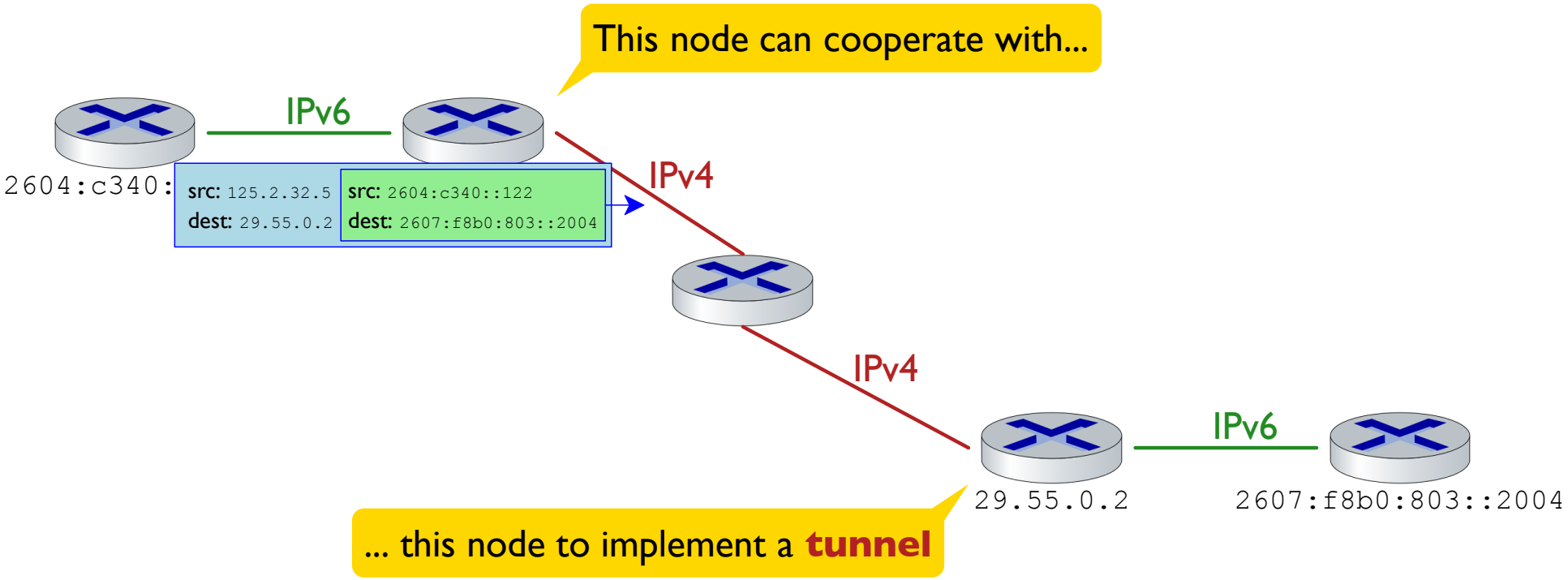
Earlier Tunneling Example: IPv6 over IPv4



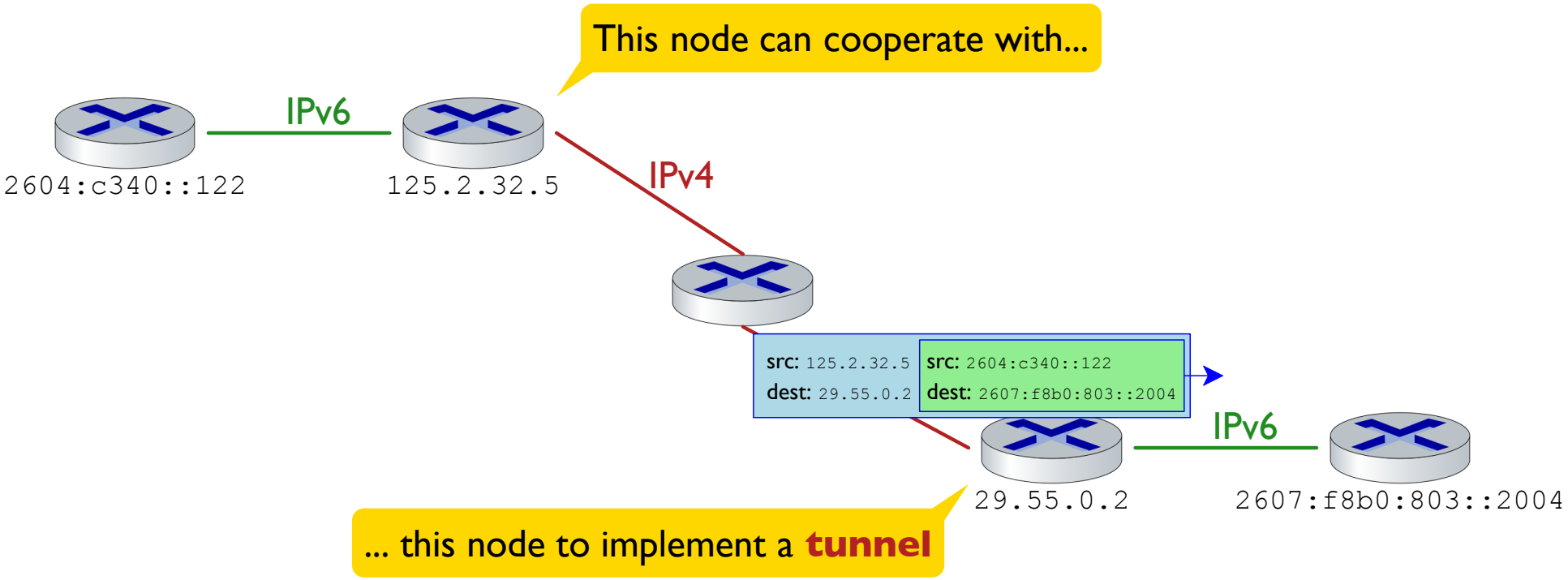
Earlier Tunneling Example: IPv6 over IPv4



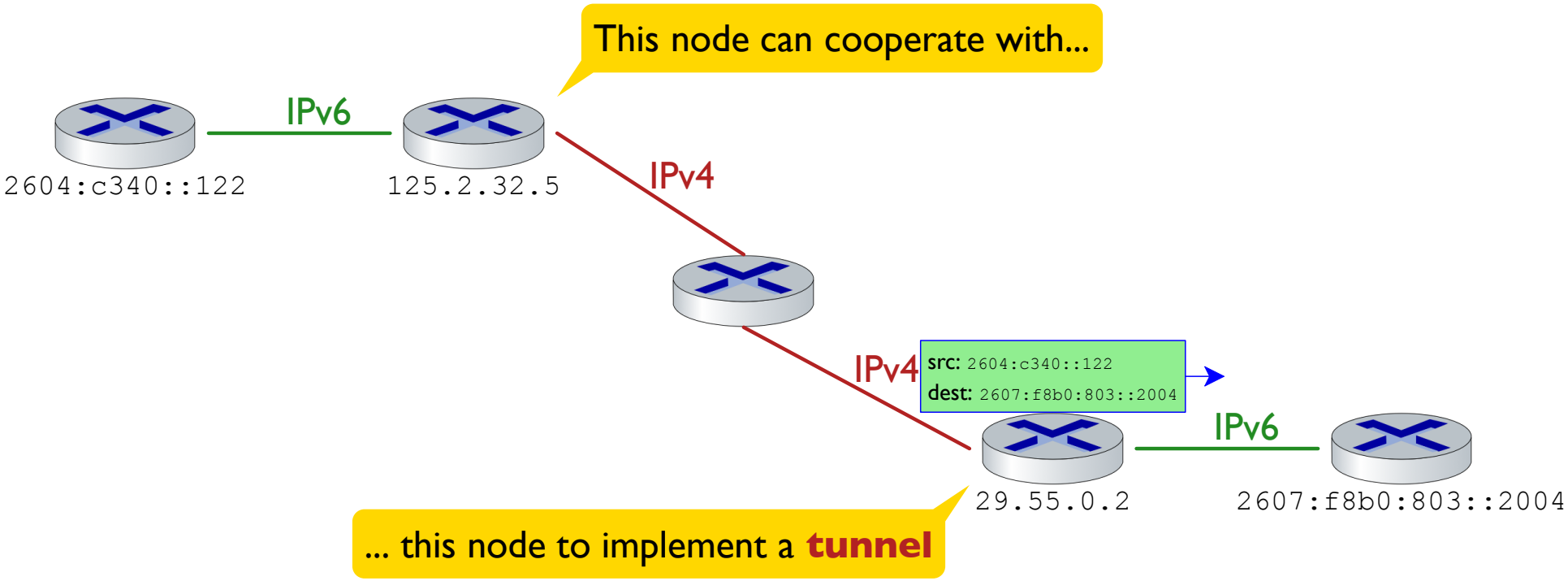
Earlier Tunneling Example: IPv6 over IPv4



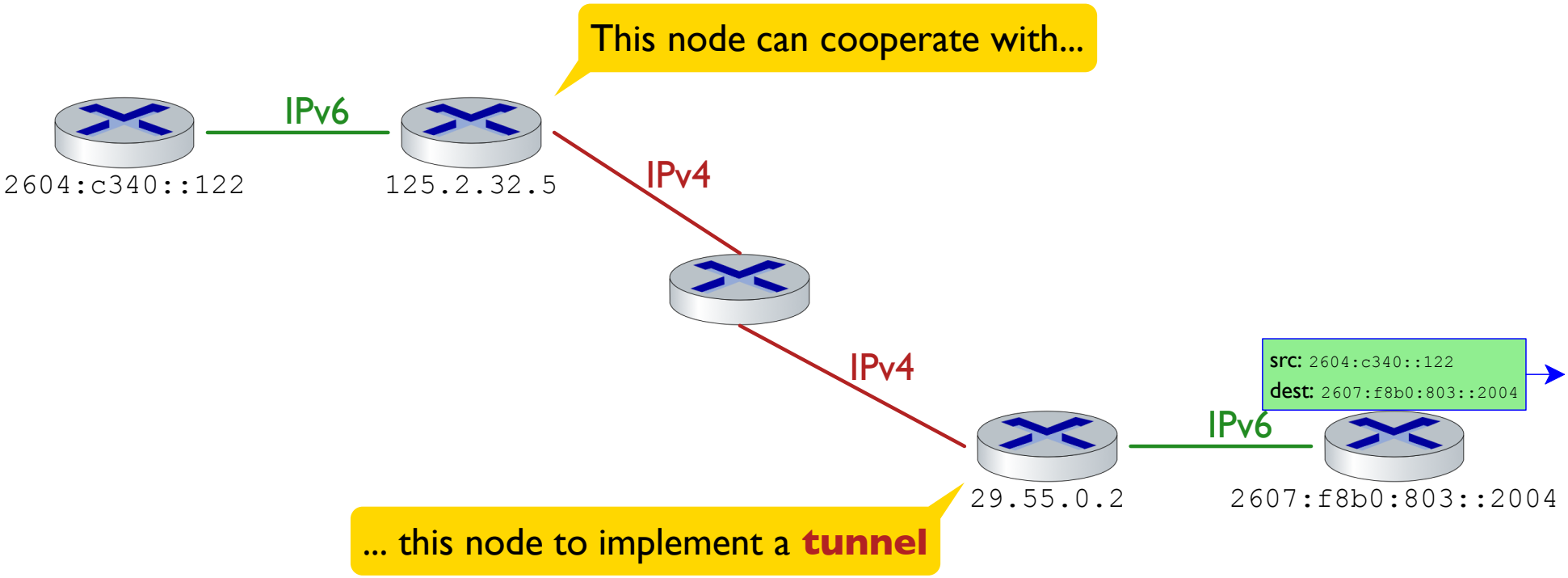
Earlier Tunneling Example: IPv6 over IPv4



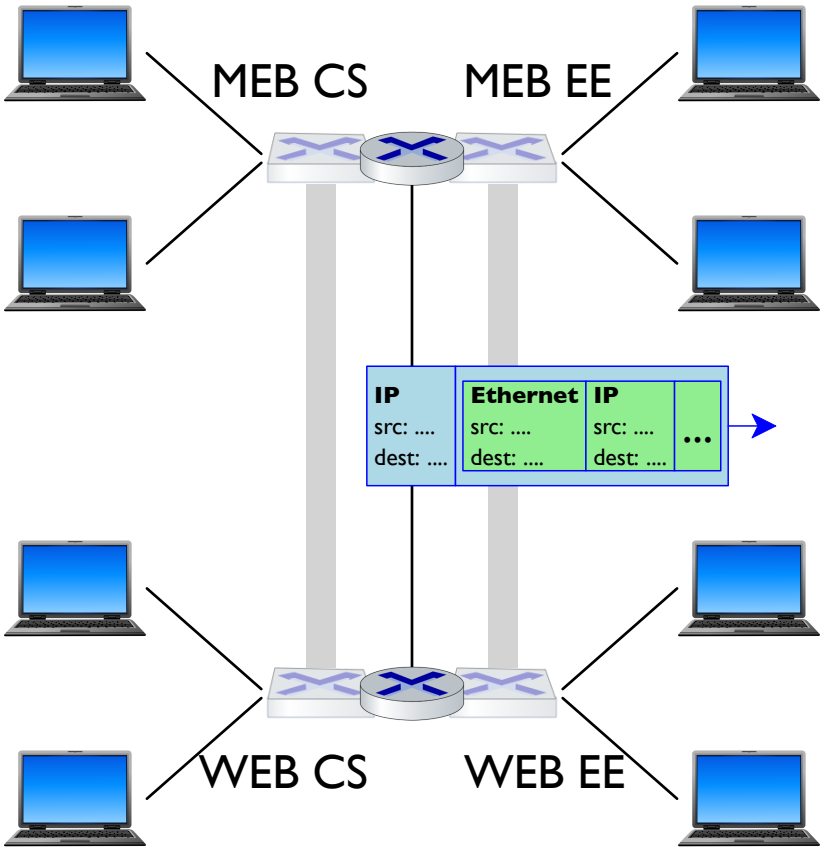
Earlier Tunneling Example: IPv6 over IPv4



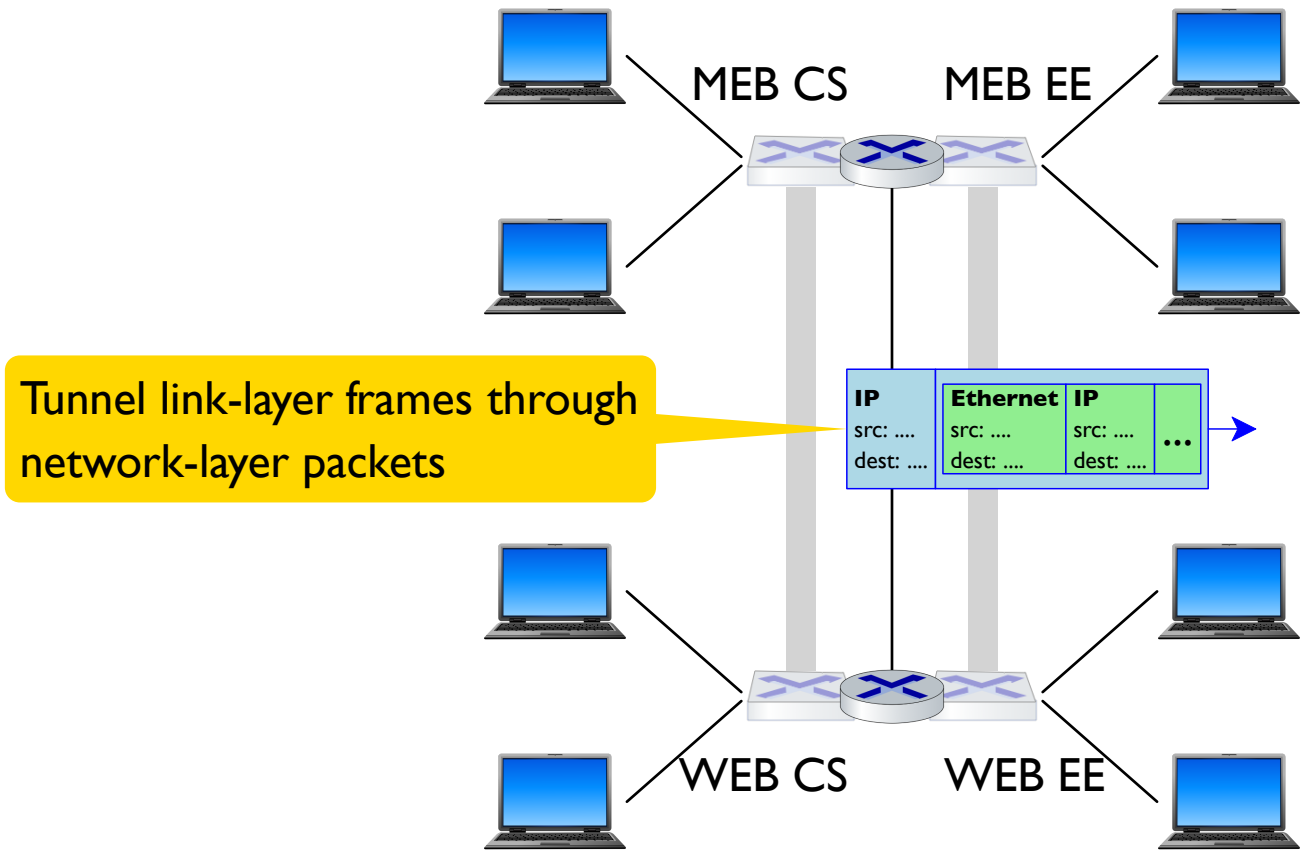
Earlier Tunneling Example: IPv6 over IPv4



Earlier Tunneling Example: VLAN over IP



Earlier Tunneling Example: VLAN over IP



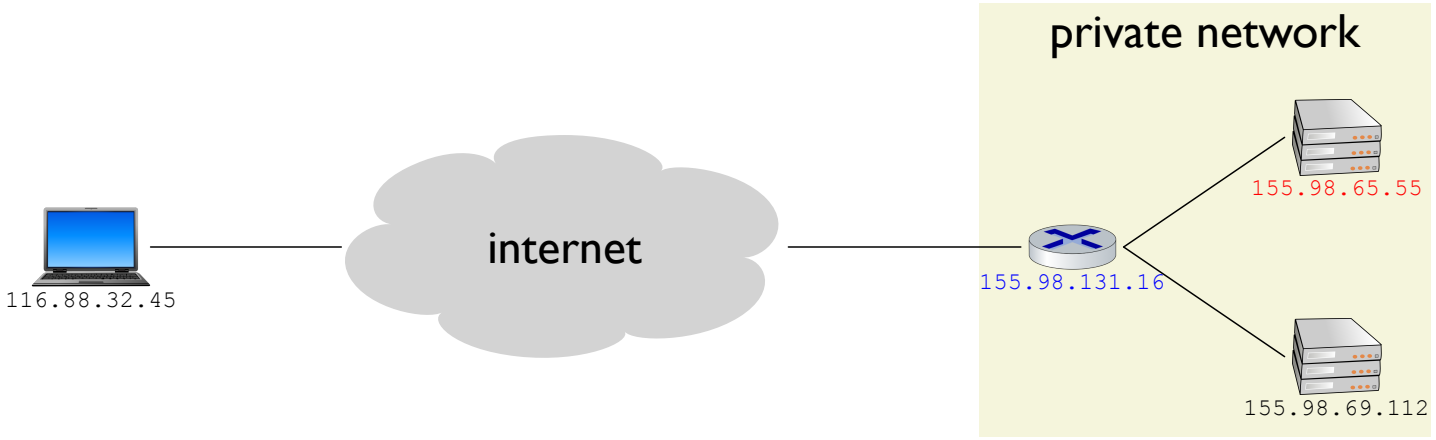
Tunnels for Authenticated and Confidential Communication

Two prominent examples:

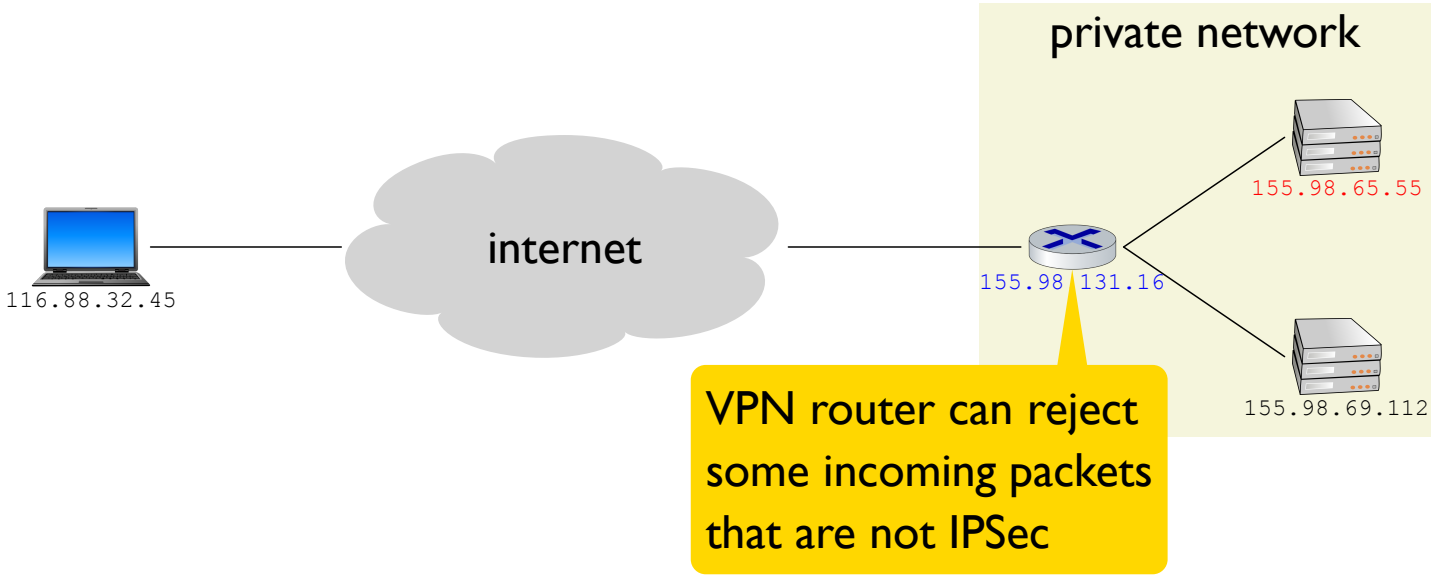
A **virtual private network (VPN)** tunnels with **IPSec** through IP

Tor tunnels with **onion routing** through TCP

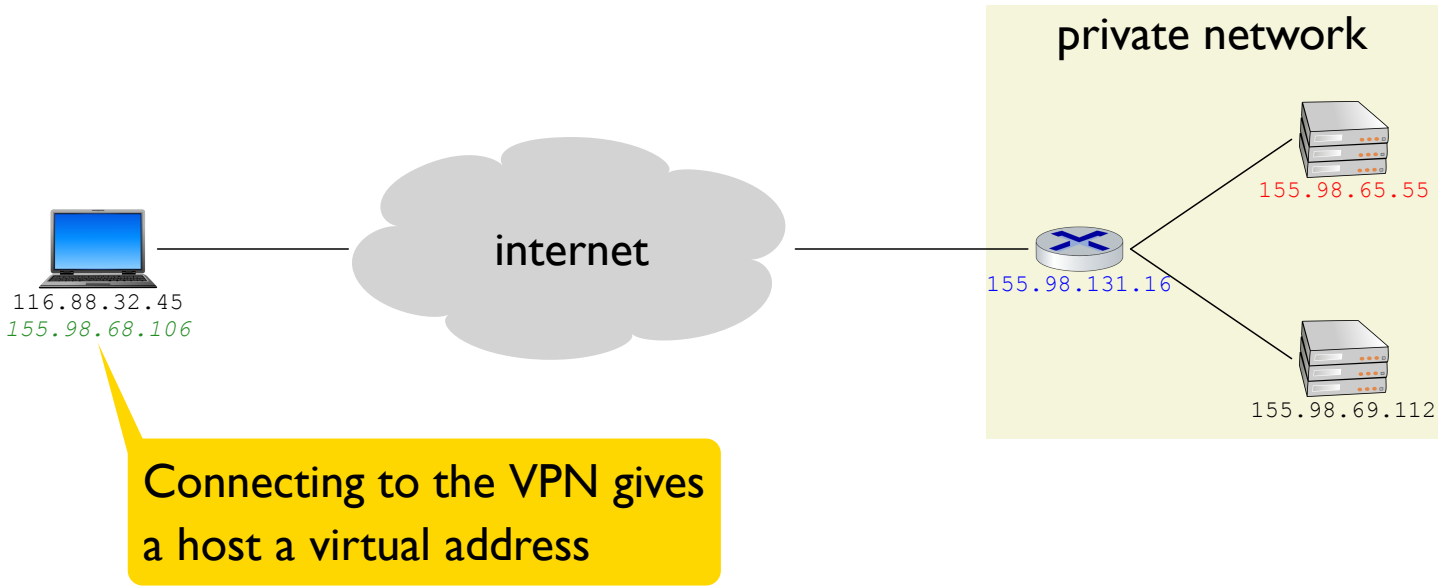
VPN using IPSec



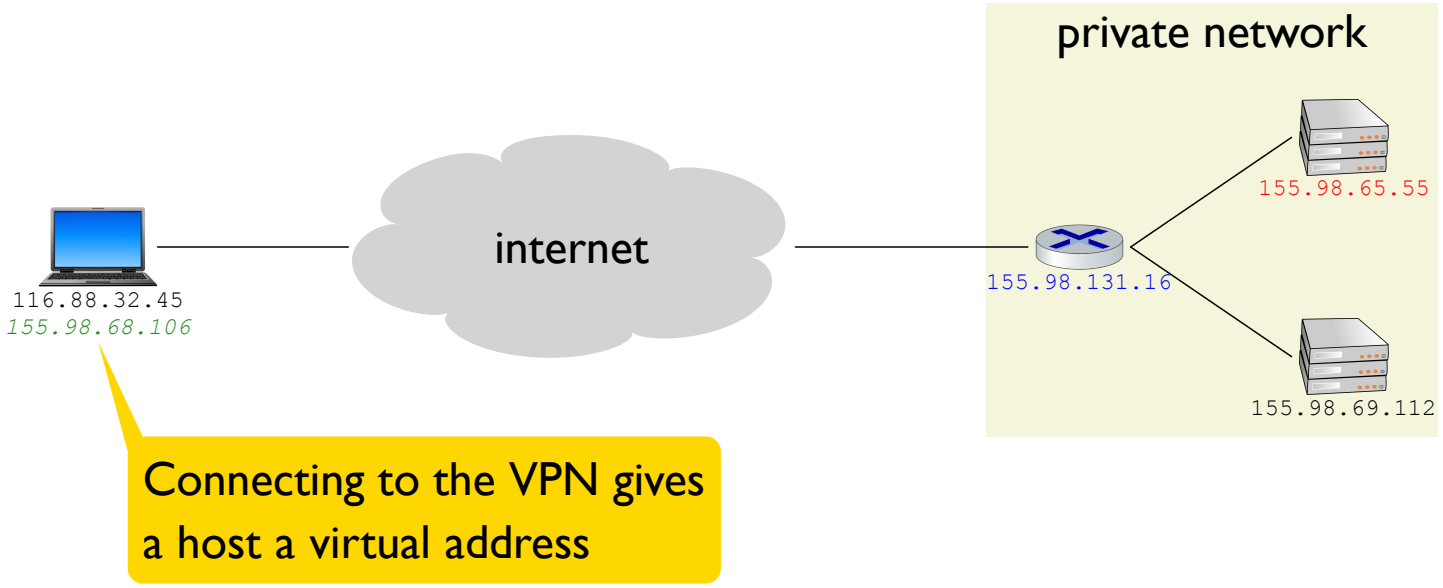
VPN using IPSec



VPN using IPSec

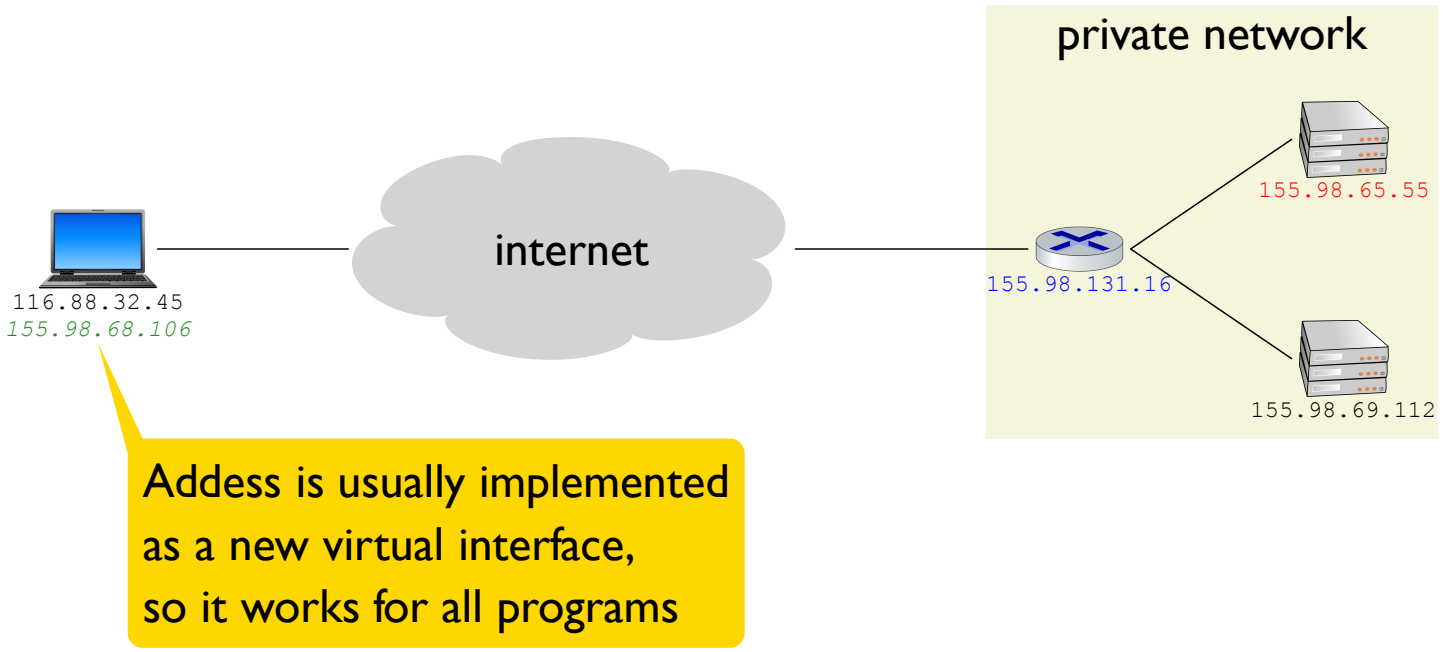


VPN using IPSec

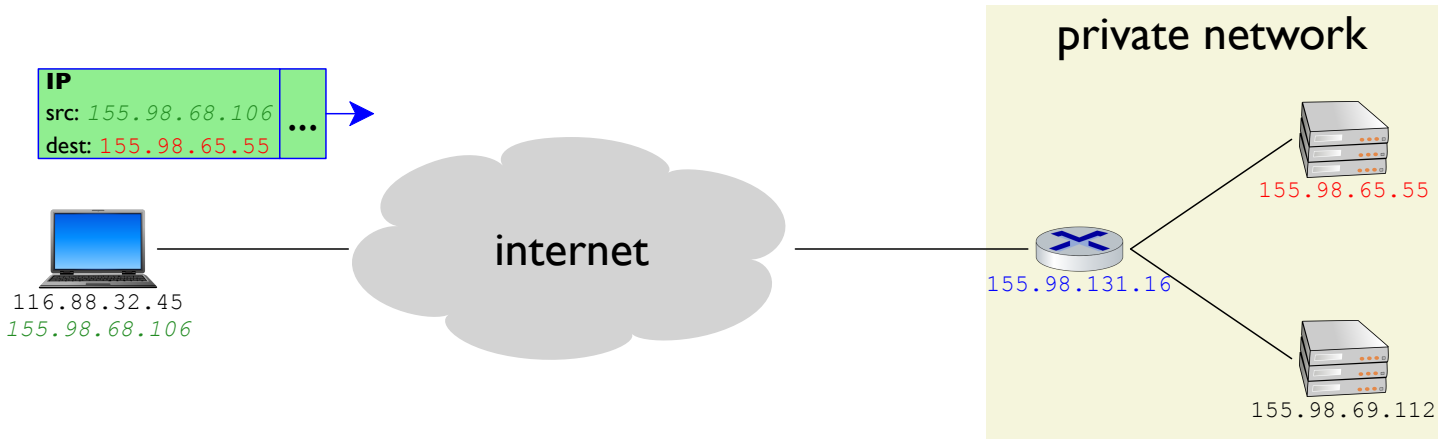


see demo using department VPN

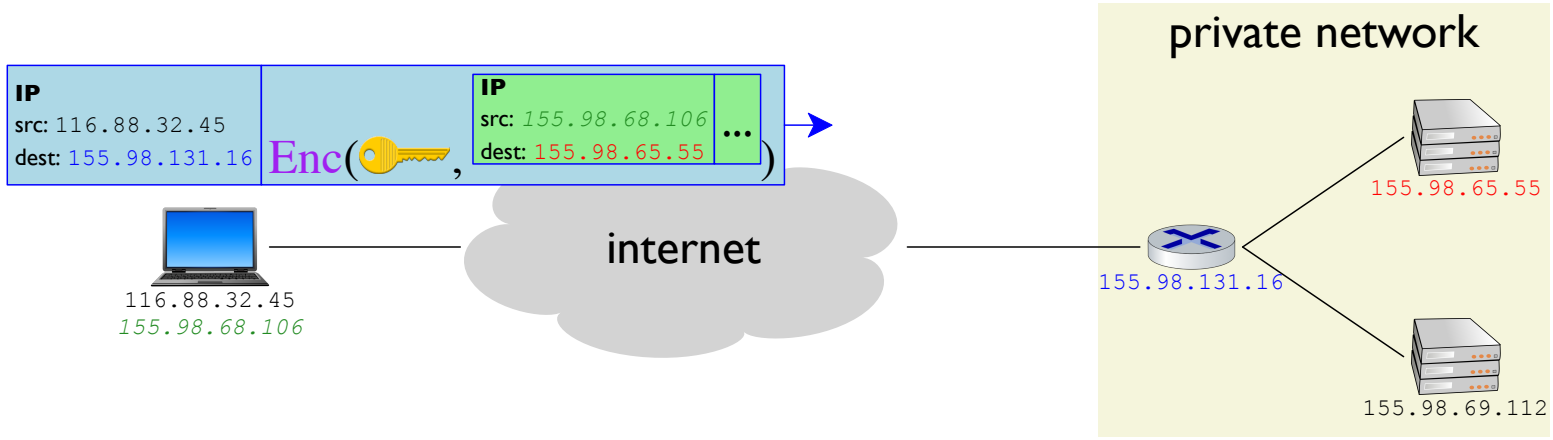
VPN using IPSec



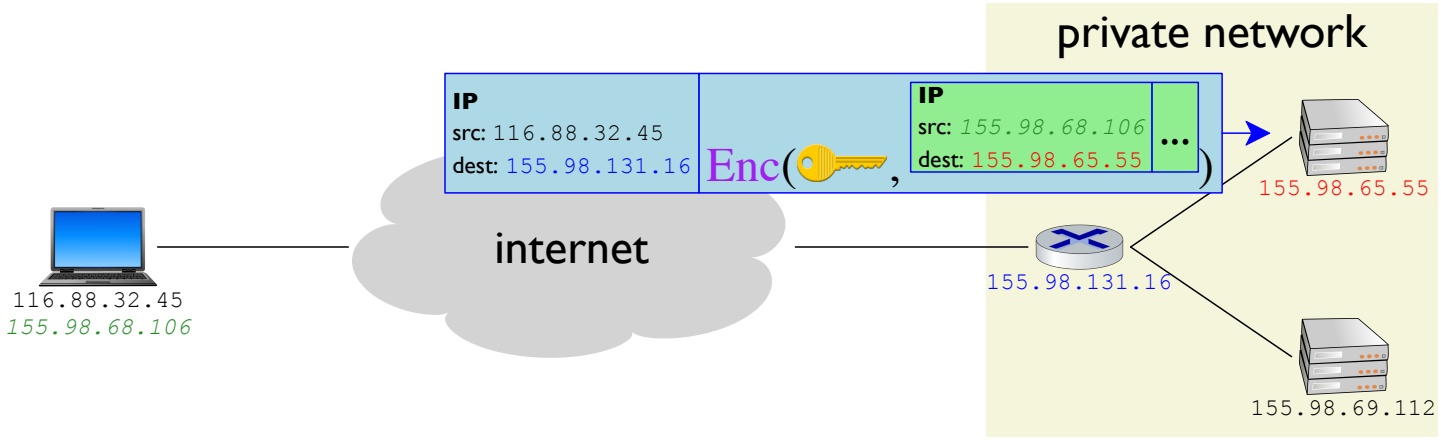
VPN using IPSec



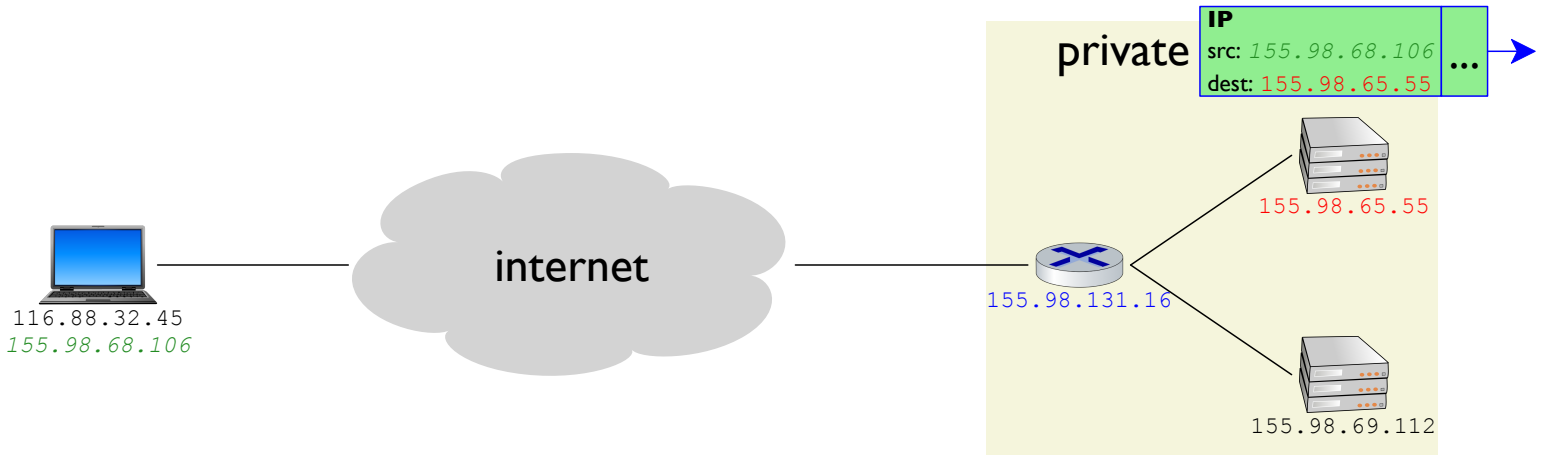
VPN using IPSec



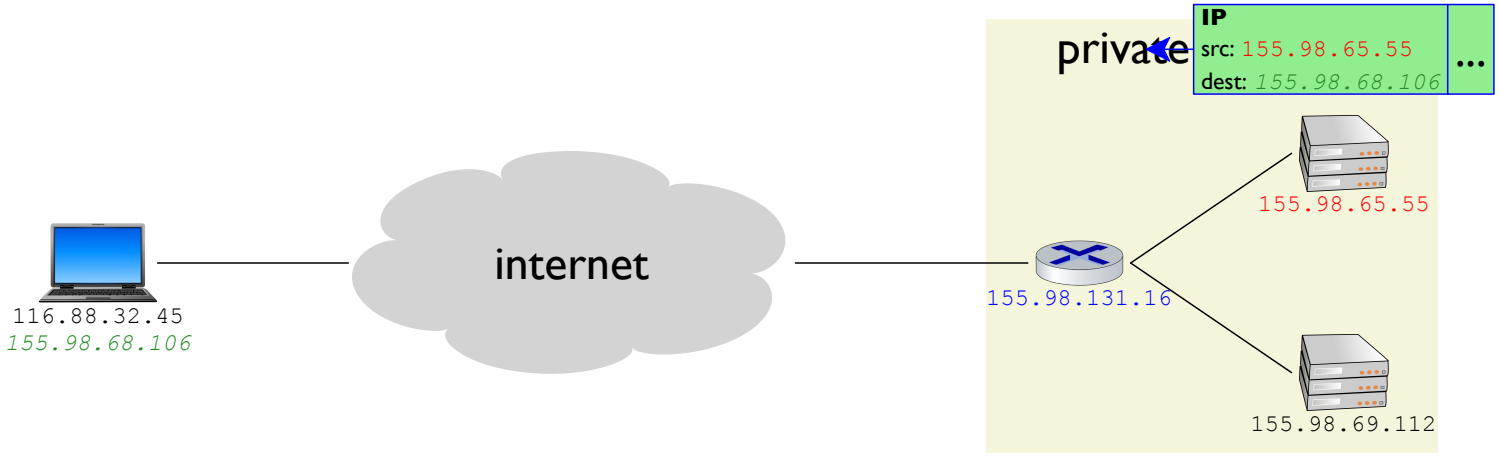
VPN using IPSec



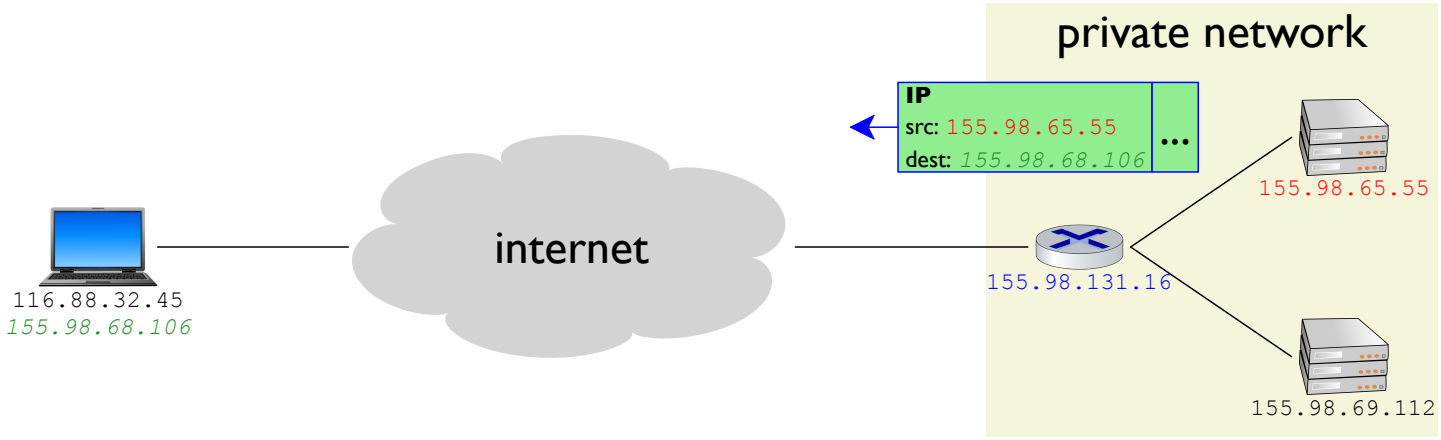
VPN using IPSec



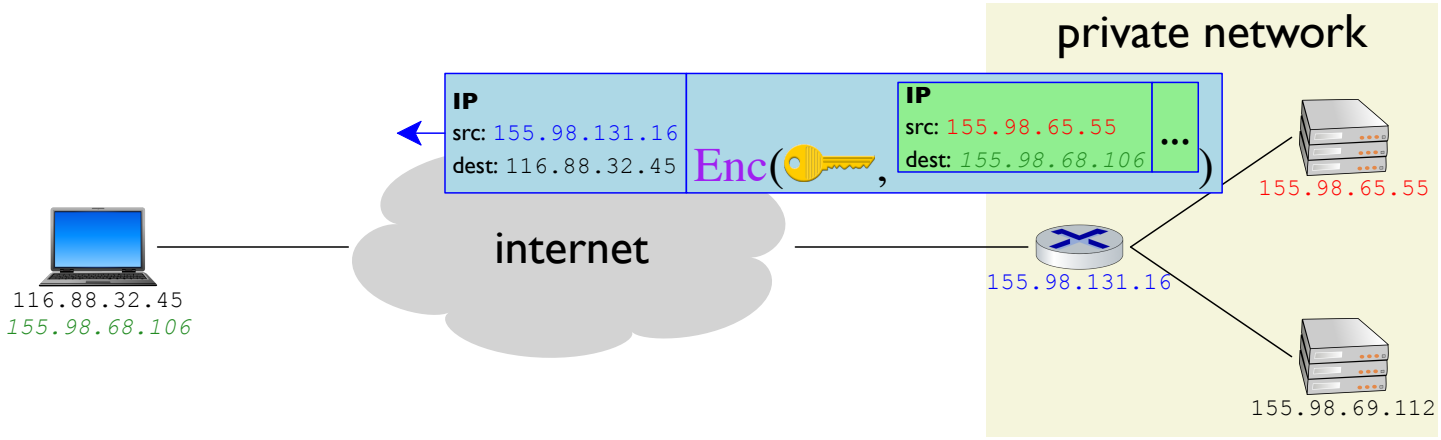
VPN using IPSec



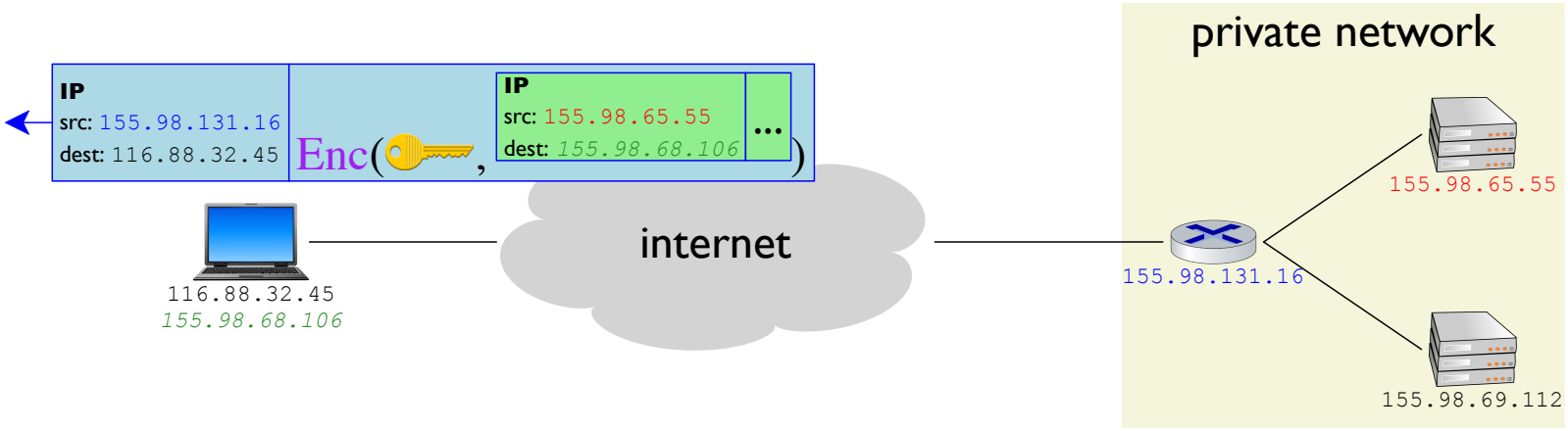
VPN using IPSec



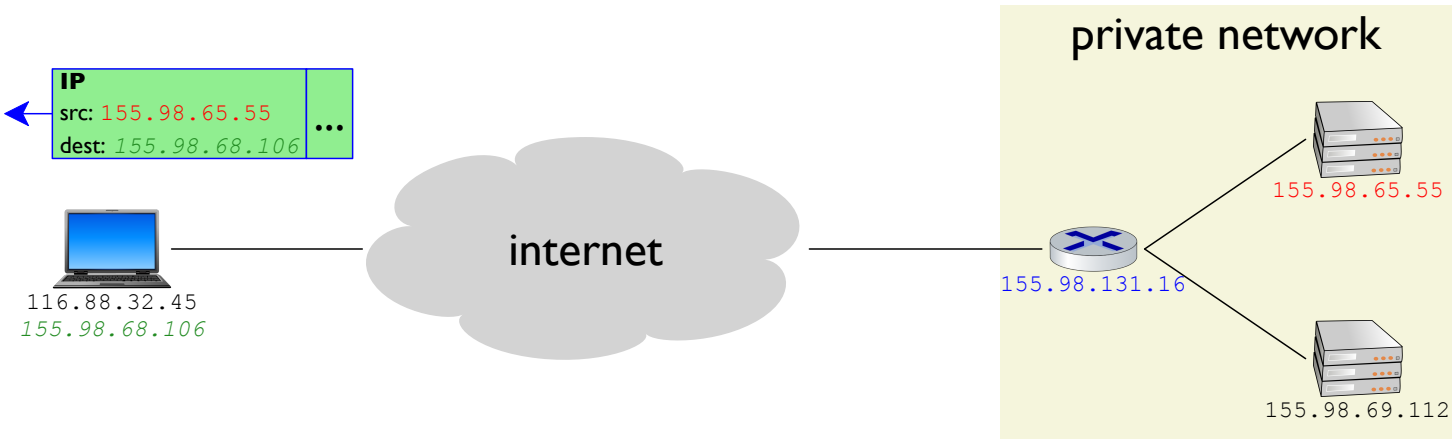
VPN using IPSec



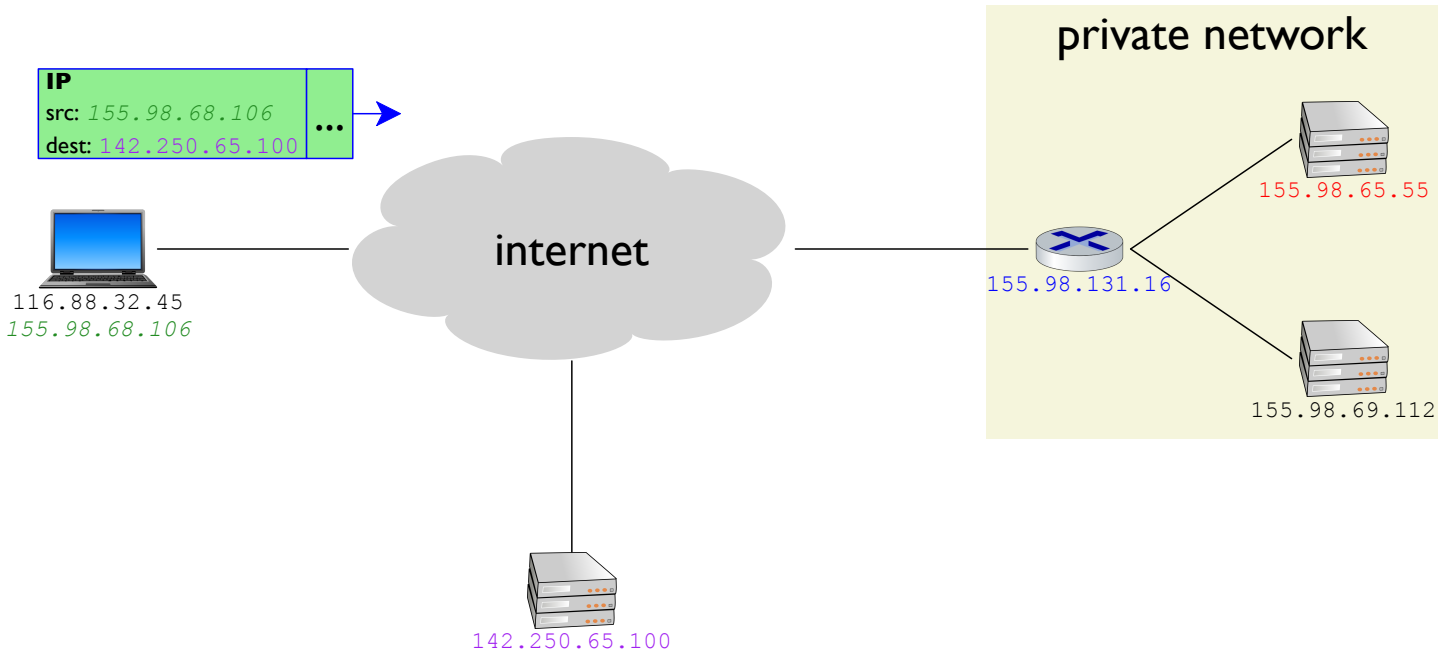
VPN using IPSec



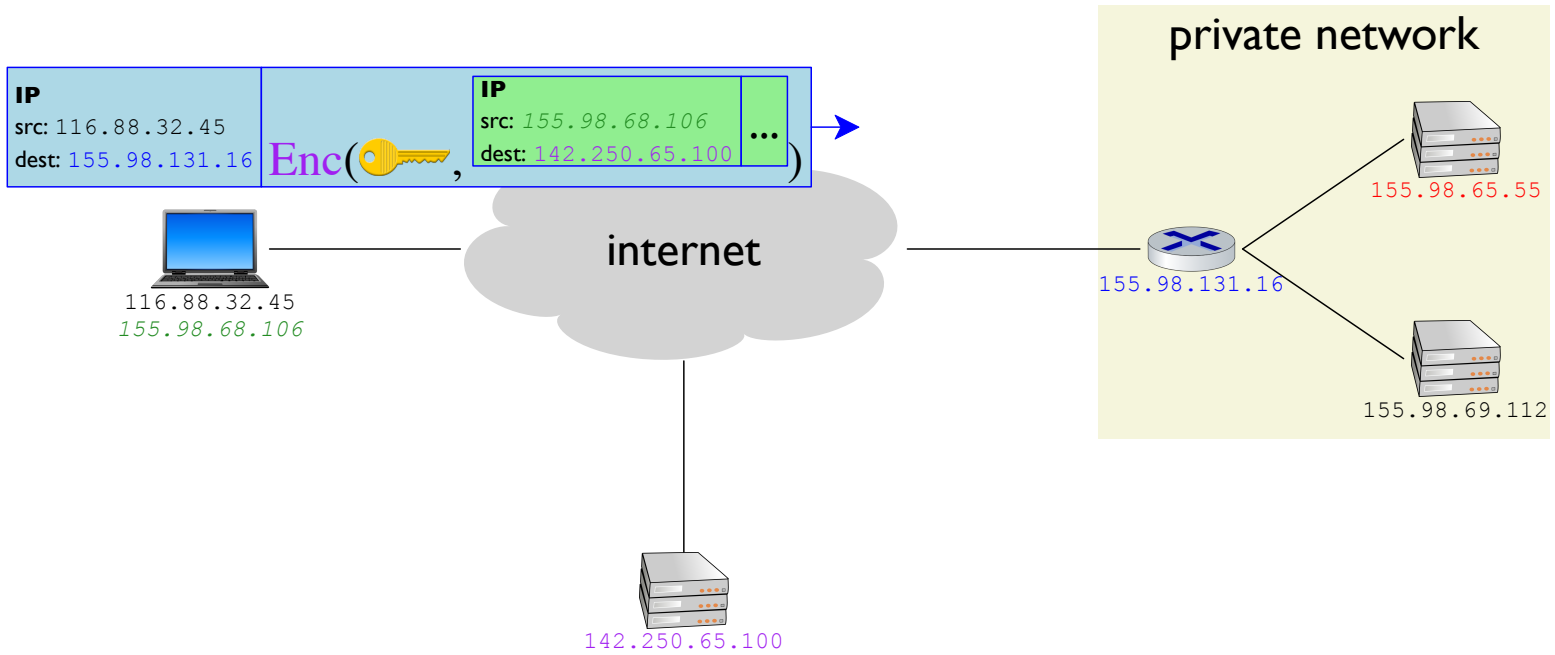
VPN using IPSec



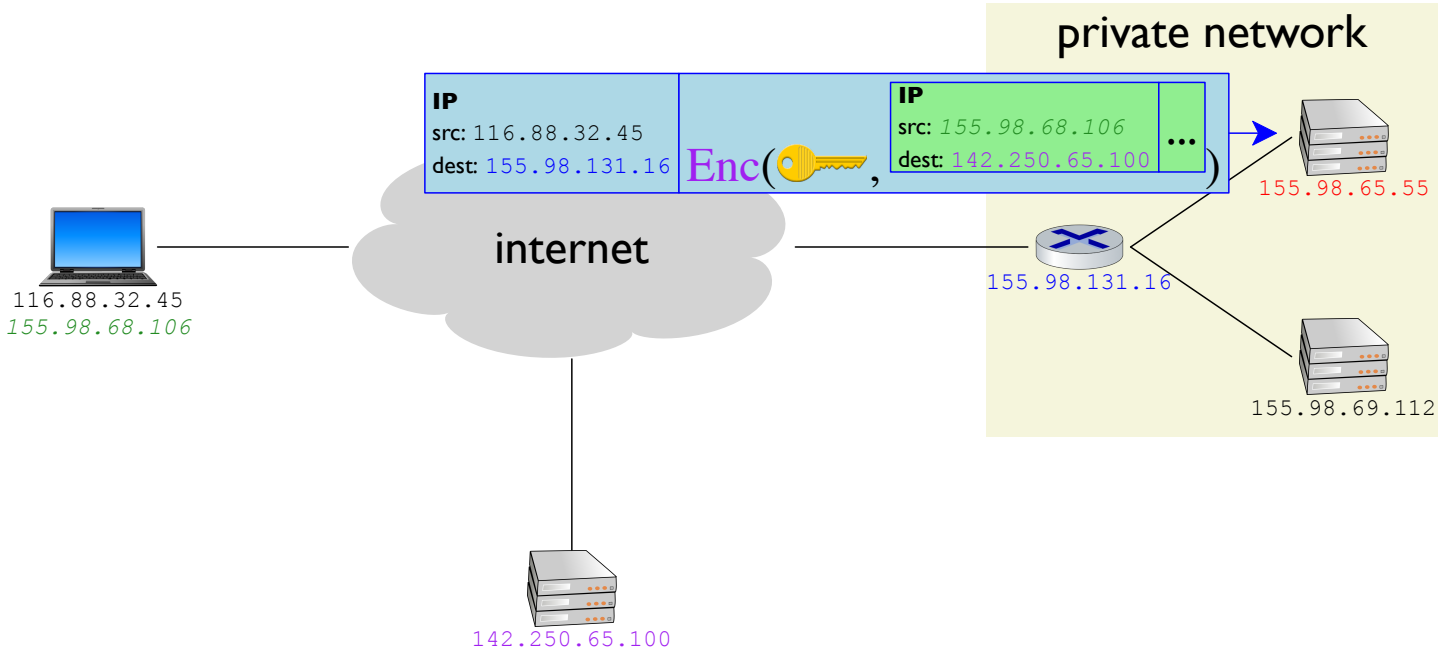
VPN using IPSec



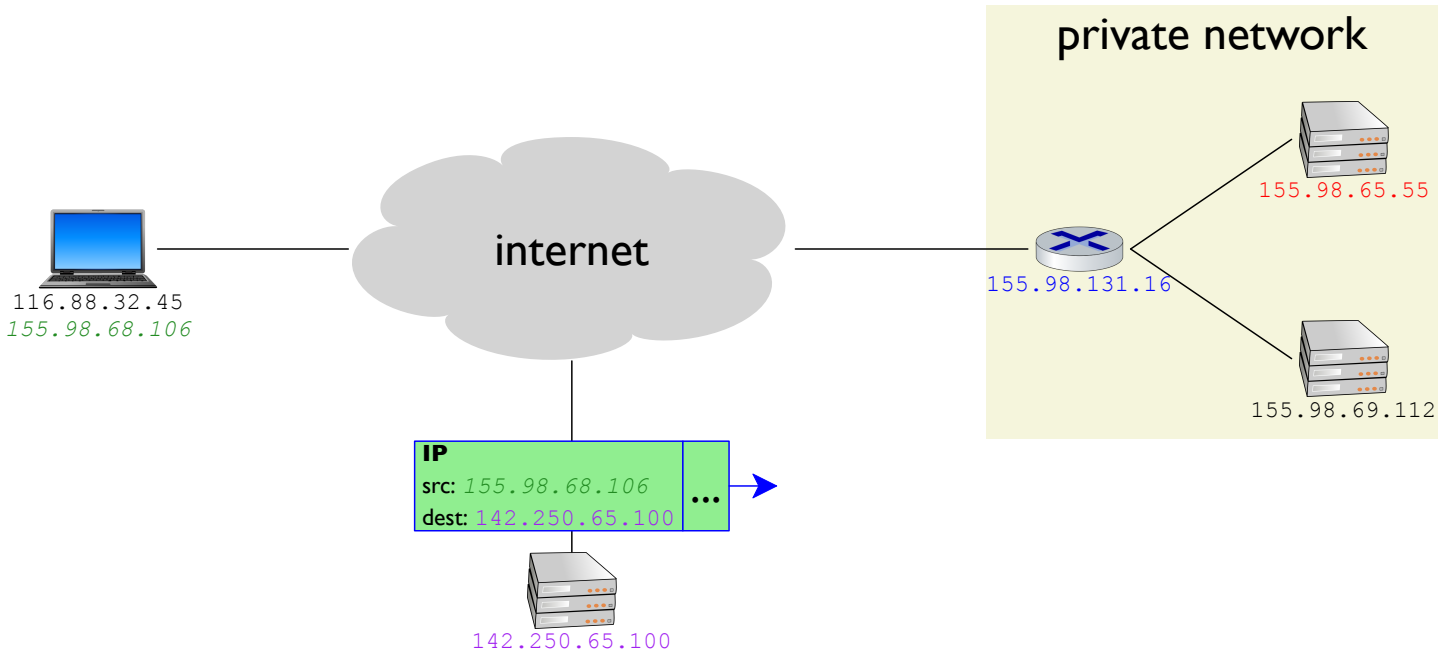
VPN using IPSec



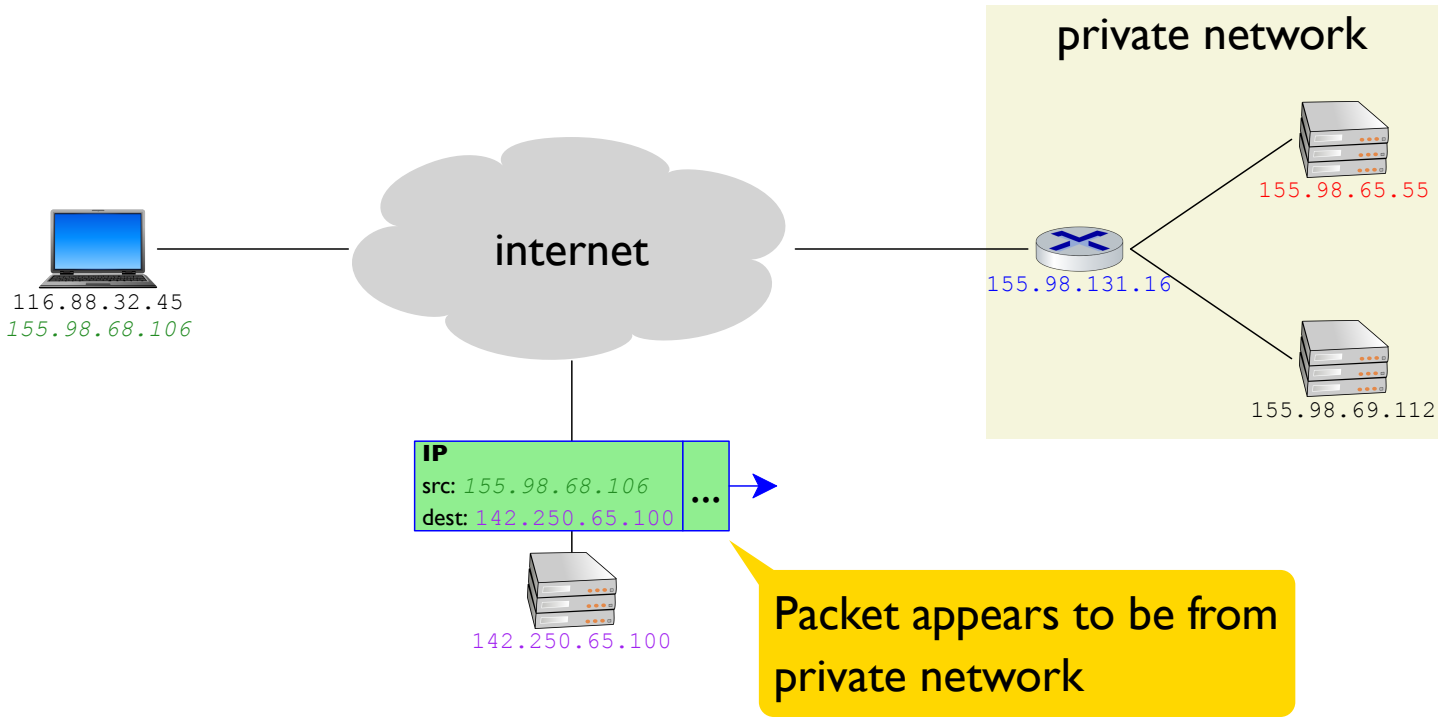
VPN using IPSec



VPN using IPSec



VPN using IPSec



IPSec

IPSec uses a cryptography combination similar to TLS:

- negotiated cipher suite
- usually a certificate with public key (at least for one end)
- session key(s) for encryption
- MAC for integrity checking

... but without the benefit of a TCP *connection*

A 32-bit **security parameter index (SPI)** is included in every packet and effectively represents an IPSec connection

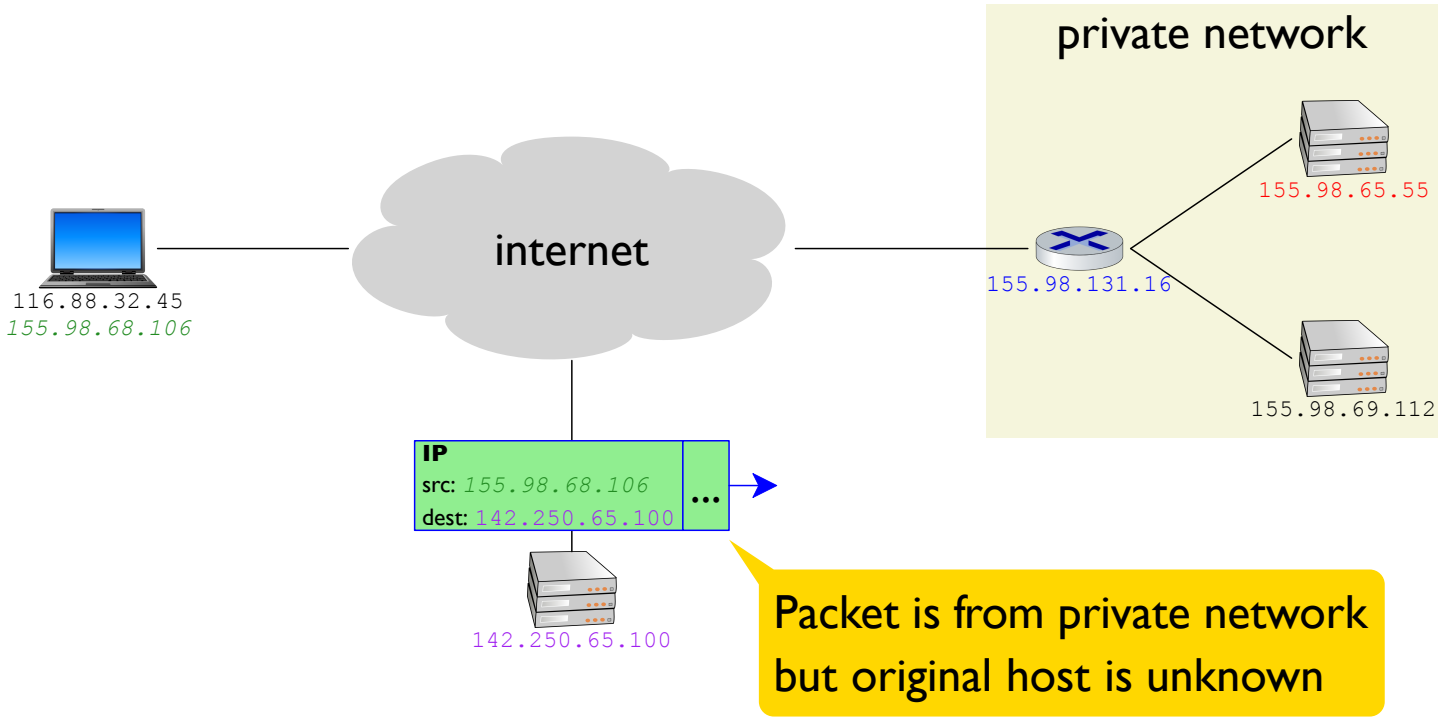
... in combination with the src and dest addresses

Some SPI Details

- An SPI is one way, so a VPN connection has two SPIs
- SPI key setup protocol in IPSec has its own name:
  Internet Key Exchange (IKE)
- SPIs timeout if unused, so IPSec includes keepalive messages

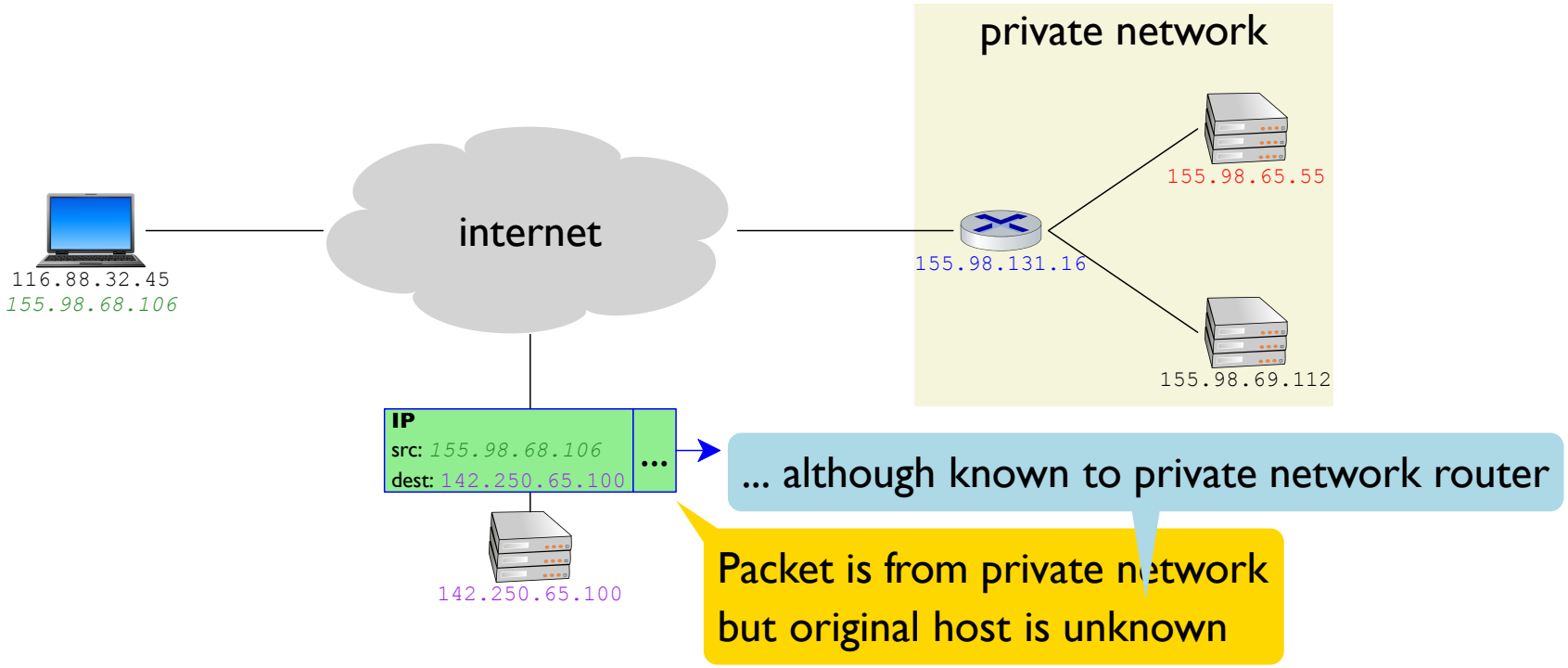
Anonymity

A VPN provides a limited form of **anonymity**



Anonymity

A VPN provides a limited form of **anonymity**



Who Needs Anonimity?

Everyday people
for identity protection

Journalists and citizens
to circumvent censorship

Activists and whistleblowers
to avoid retaliation

Based in part on https://2019.www.torproject.org/about/torusers.html.en

Who Needs Anonimity?

Everyday people
for identity protection

Journalists and citizens
to circumvent censorship

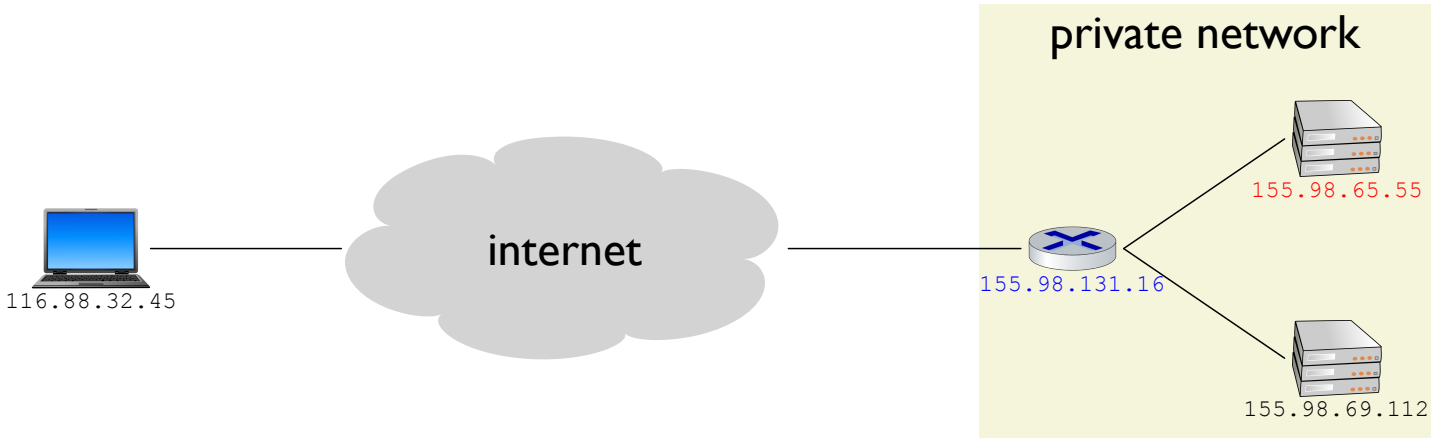
Activists and whistleblowers
to avoid retaliation

and, yes,

Unscrupulous people
to avoid getting caught

Based in part on https://2019.www.torproject.org/about/torusers.html.en

Anonymity

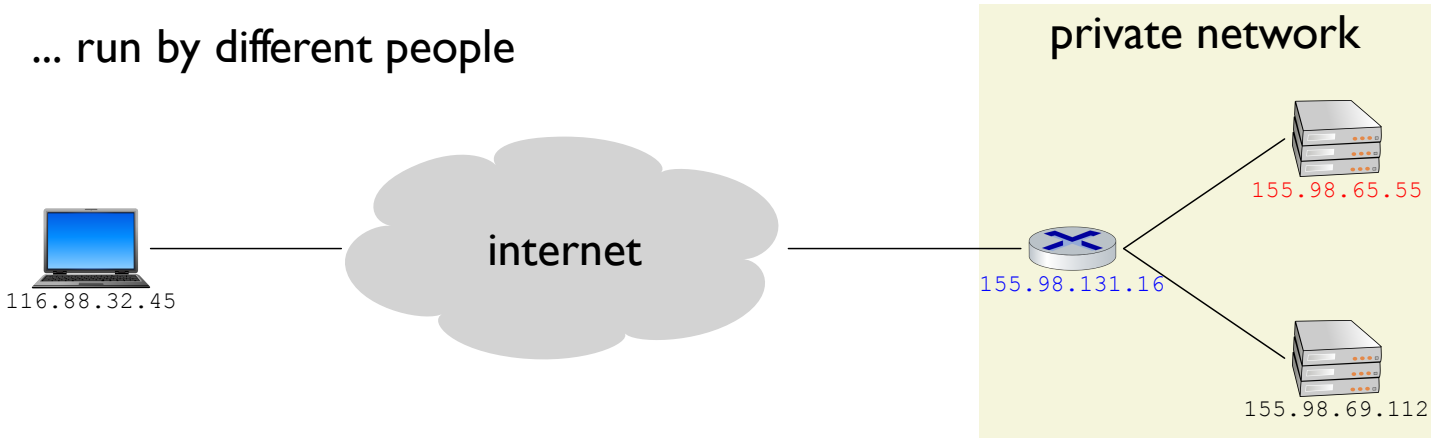

private network
internet
116.88.32.45
155.98.131.16
155.98.65.55
155.98.69.112

Anonymity

What if...

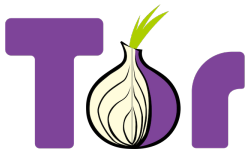
... there are multiple entry and exit routers

... run by different people

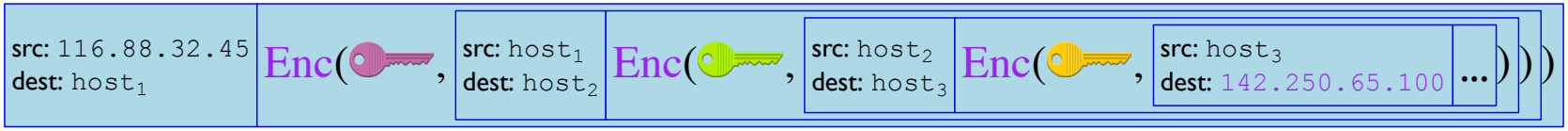


... and messages bounce around a while

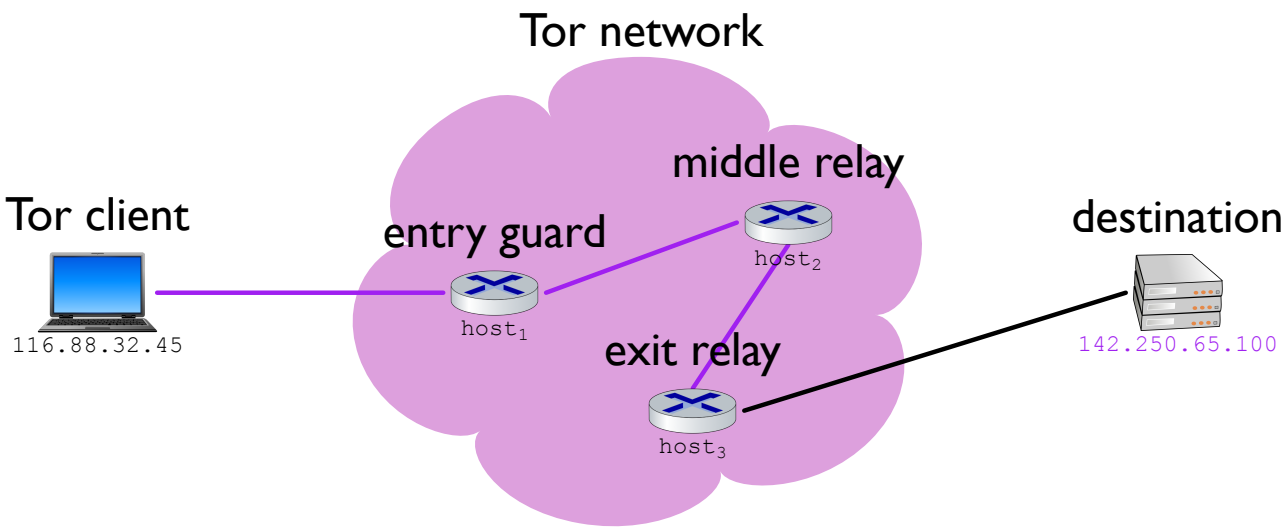
... and each router knows only the next step?



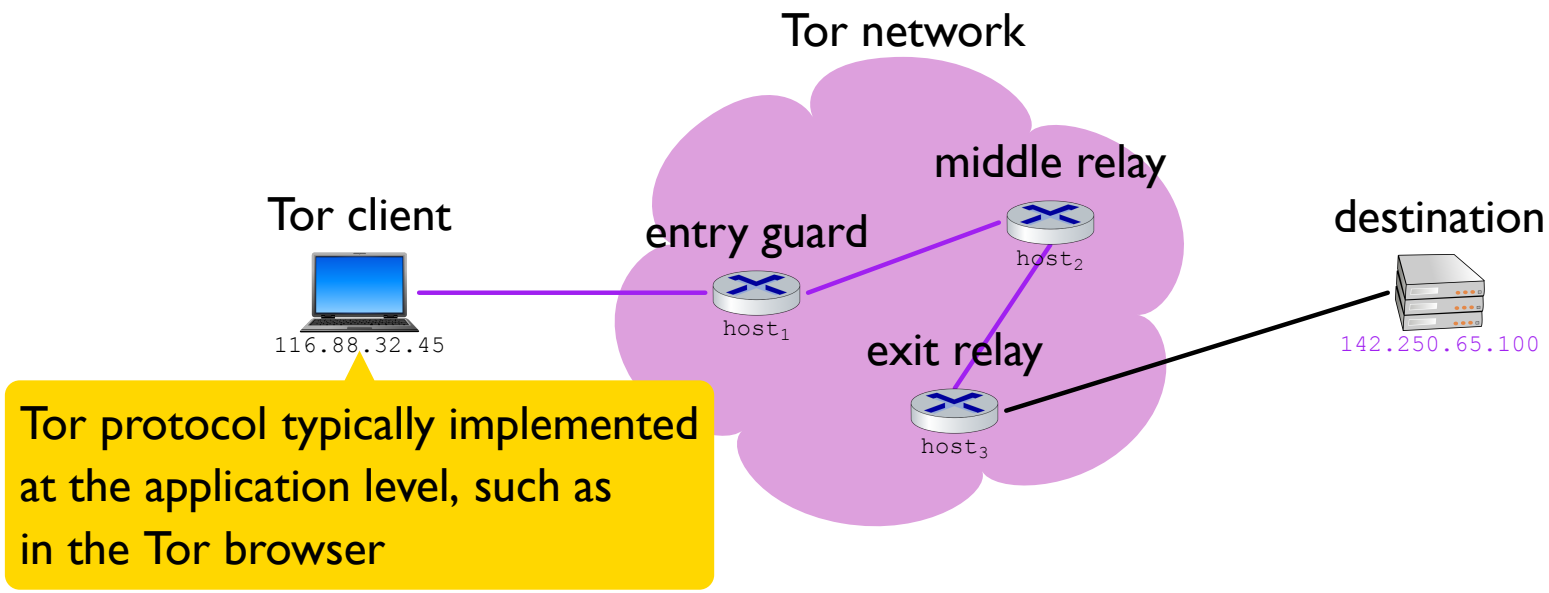
Tor (the onion router) is for anonymity



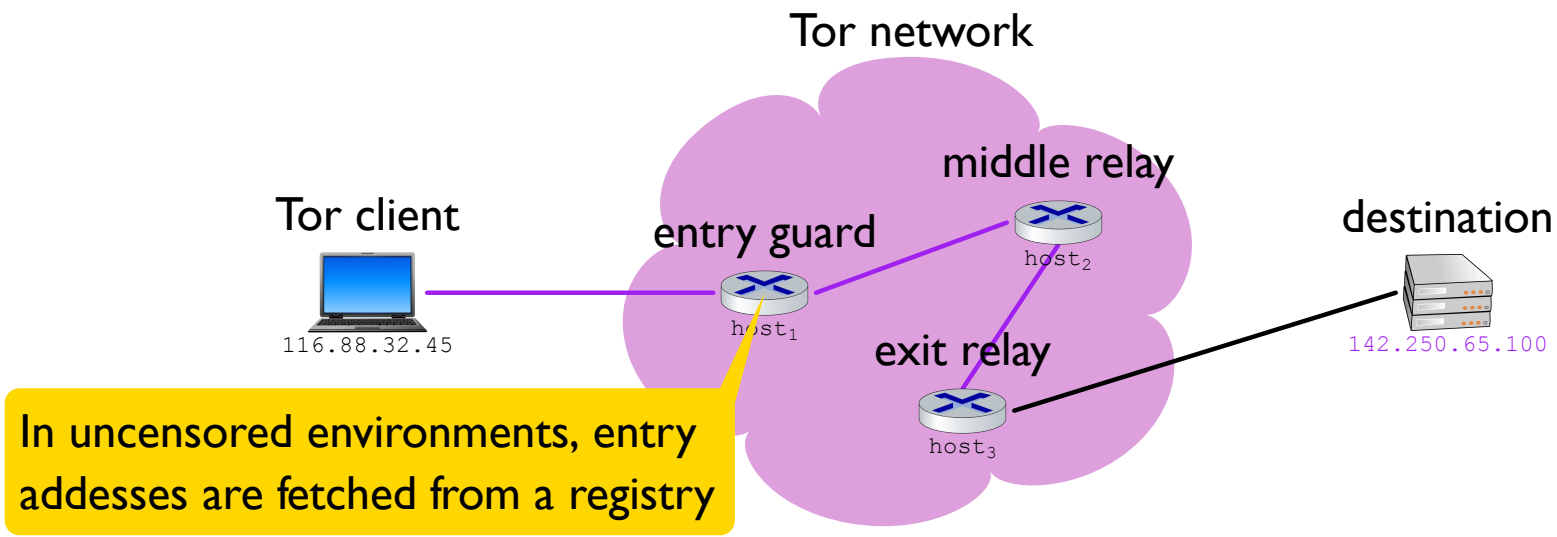
Onion Routing



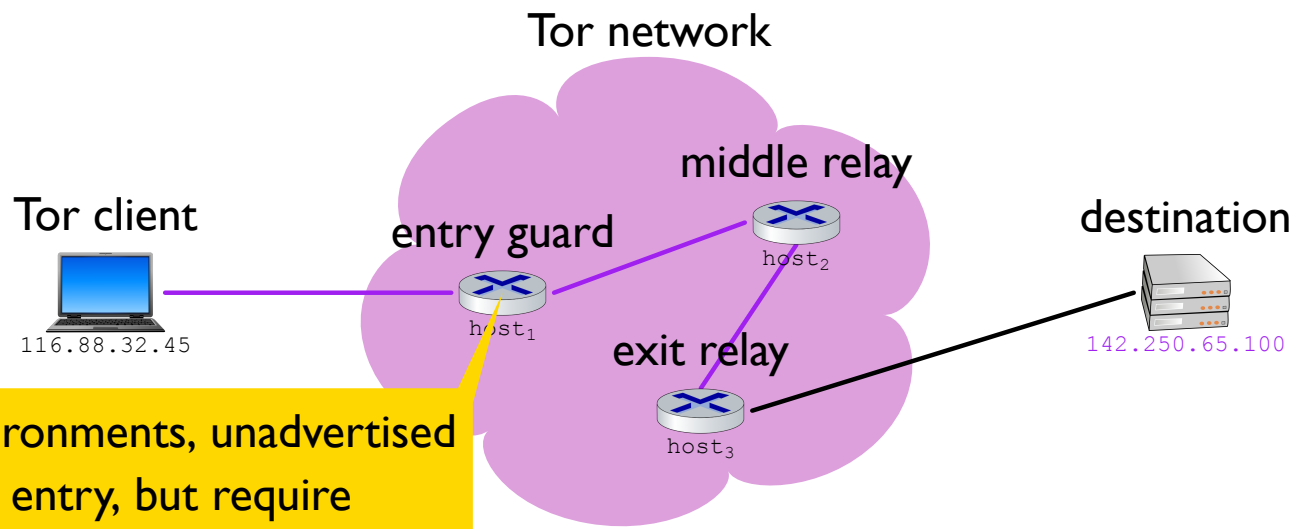
Onion Routing



Onion Routing

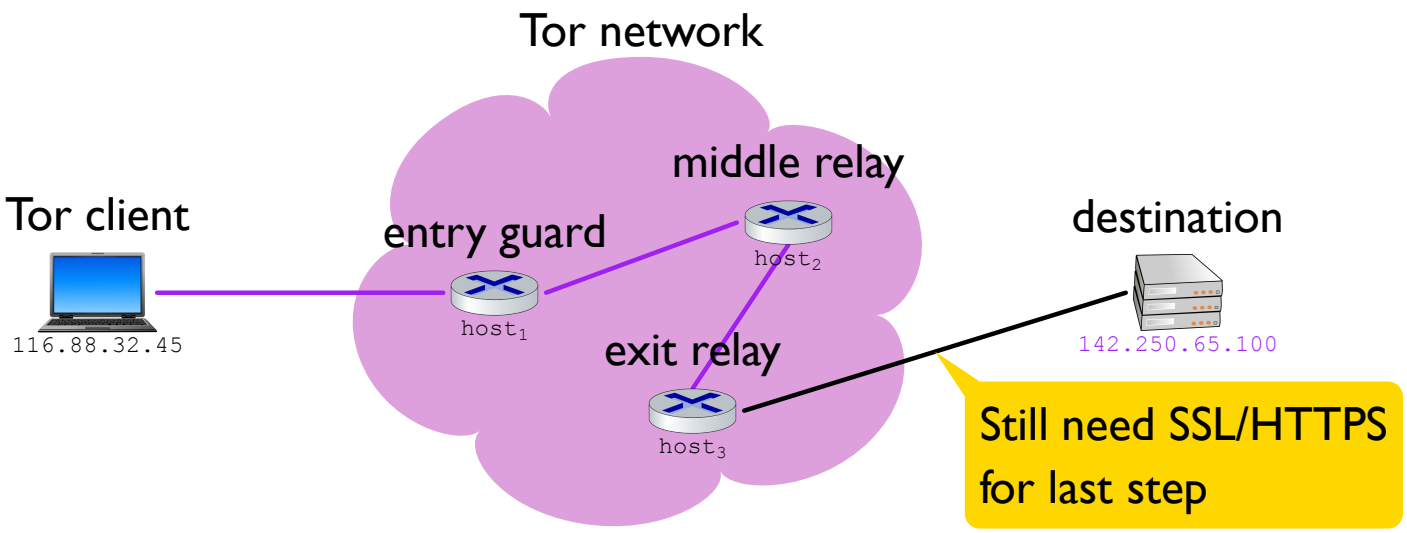


Onion Routing

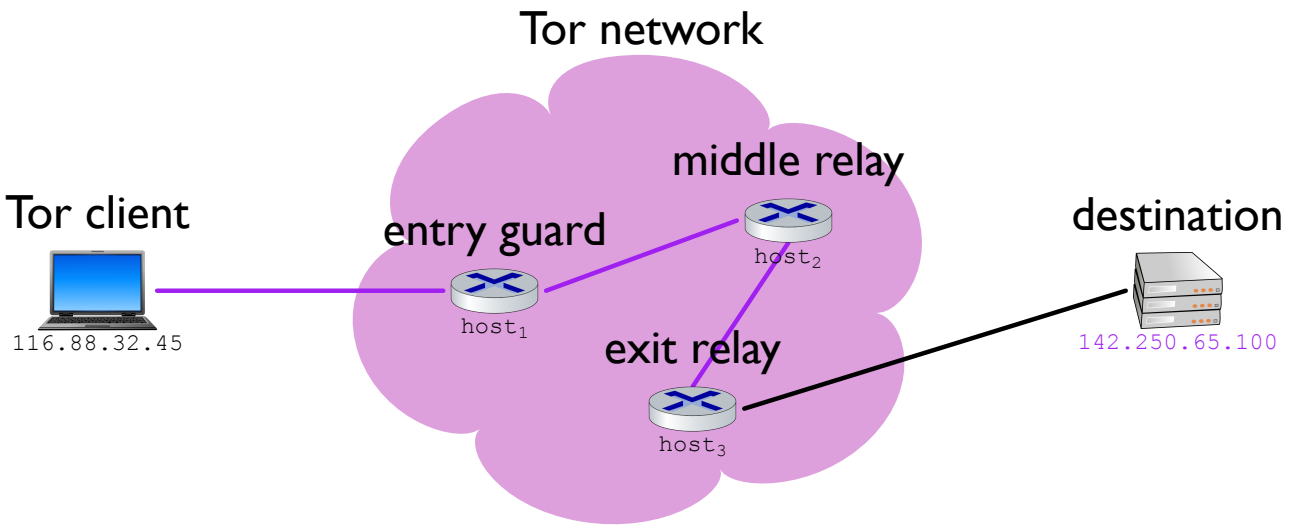


In censored environments, unadvertised **bridges** enable entry, but require explicit configuation (e.g., an address posted on Telegram)

Onion Routing

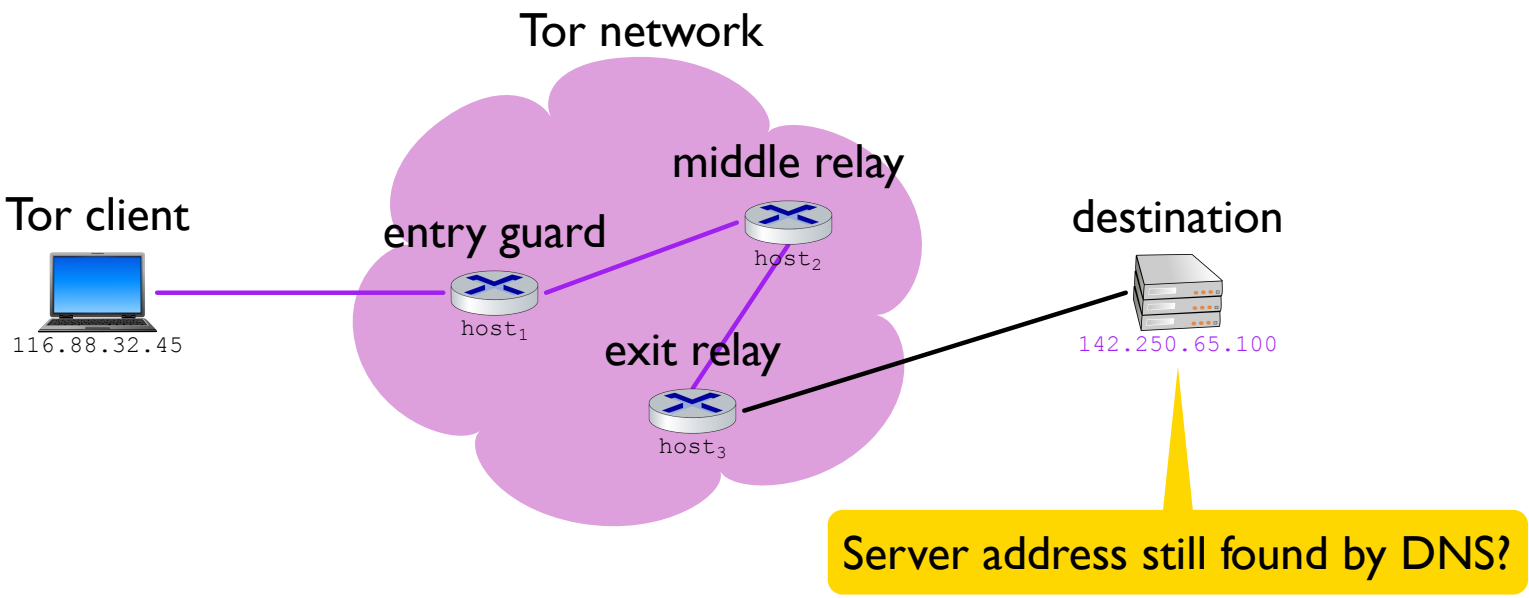


Onion Routing

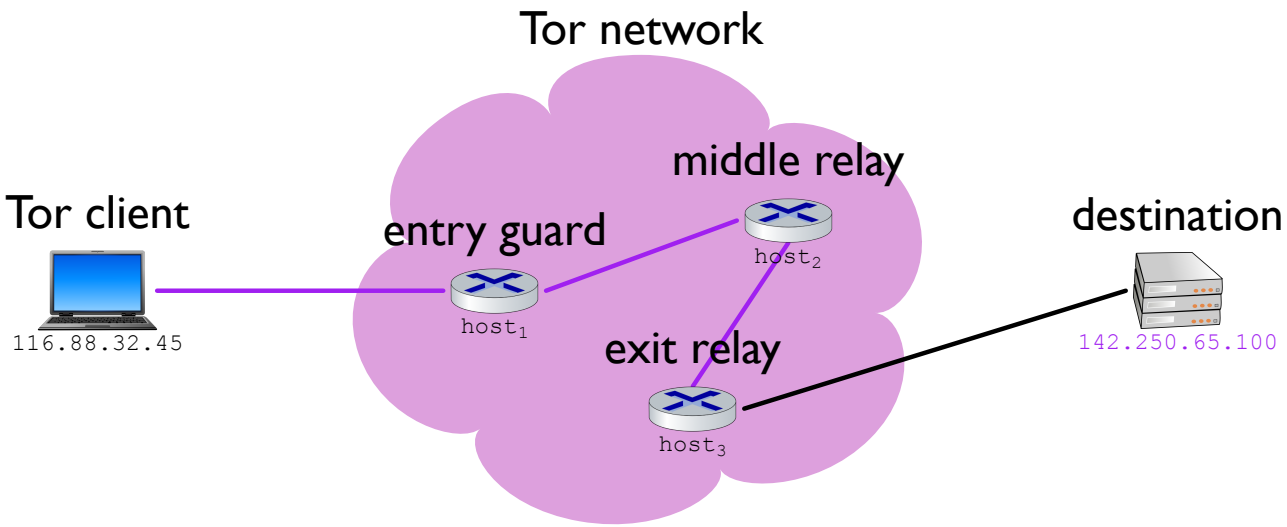


As of 2016: about 2,000 entry nodes, 7,000 relay nodes, 1,000 exit nodes

Onion Routing



Onion Routing



Severs can have `.onion` addresses, which are resolved within Tor

⇒ anonymity for servers

Secure DNS

DoT is DNS over TLS on port 853

DoH is DNS over HTTPS on port 443

Cloudflare's public DNS that supports both:

`1.1.1.1`

Summary

Tunneling and layering TLS are general strategies for adding security over existing networking layers

VPNs use **IPSec**, which uses **IKE**

similar to TLS, but at the network layer

Tor adds **onion routing** to TLS-like encryption to implement anonimity