ESTD 1845

QUEEN'S
UNIVERSITY
BELFAST

NAT, Tunneling and VPNs – Part 1

Dr. Sandra Scott-Hayward

CSC3064 Lecture 09

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- Network Address Translation (NAT)
- Tunneling
- Virtual Private Networks (VPNs)

References:

Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007.

QUEEN'S UNIVERSITY BELFAST

Basic Layer 2-3 Security Issues

Network packets pass by untrusted hosts

- Eavesdropping, packet sniffing
- Particularly easy when the attacker controls a machine close to the victim

IP addresses are public and no source authentication

- Enables spoofing

General Countermeasures

Since IP is so ingrained in the Internet, it is hard to provide security. There are a few general countermeasures:

- IP Filtering
- Network Address Translation (NAT)
- Virtual Private Network (VPN)
- Encrypted IPV4 & IPV6 (IPSec)

IP Filtering

Routers can be configured to filter out packets based on:

- IP Address (black listing)
    - Hard to keep list current
    - Hard to get off the list (DoS)
- Port numbers
    - Rogue protocols use multiple ports
- Protocol types (TCP, UDP, ICMP)
    - Course grain filtering

Turning Point - PRS

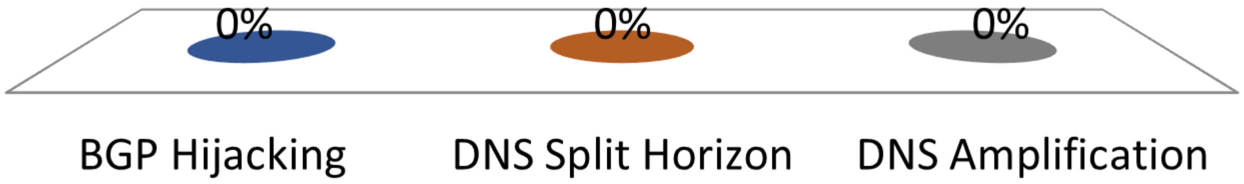
Go to:	https://qub.ac.uk/prs
Enter Session ID:	CSC306412Feb

Q: In what context have we already discussed IP filtering?

A. BGP Hijacking

✓ B. DNS Split Horizon

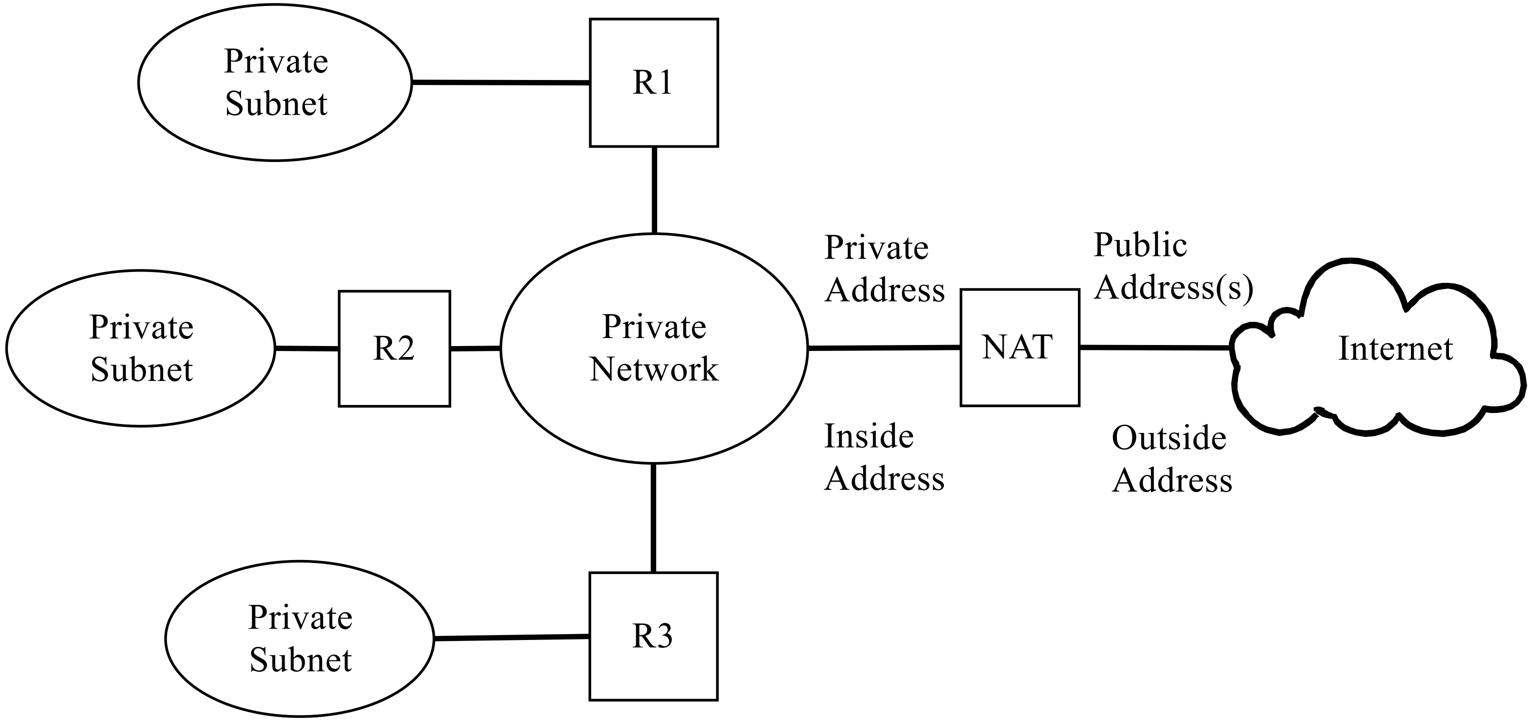
C. DNS Amplification



Network Address Translation (NAT)

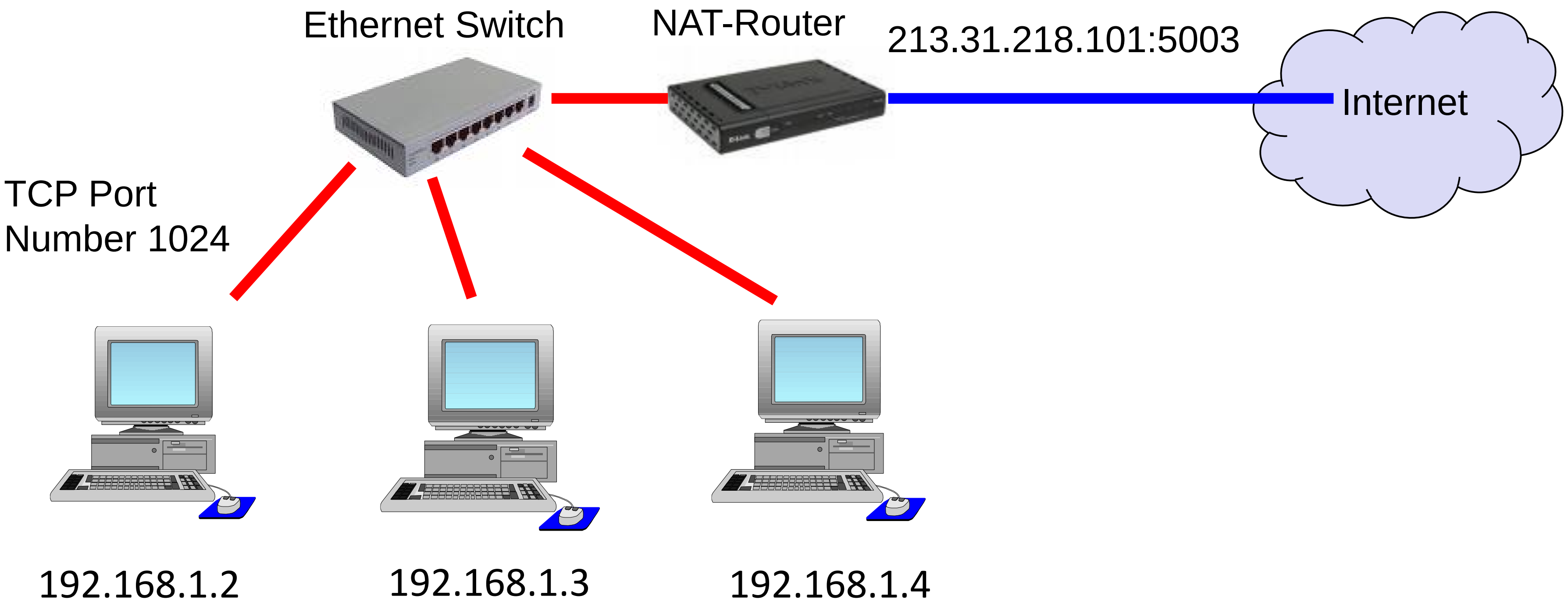
- Common problem nowadays: ISP provides only a single IP address, but multiple devices shall be connected
- Solution: A router is used to map several internal (private) addresses to a single external (public) address
- Most common approach (simplified):
  - For packets coming from the private side:
    - Router rewrites TCP/UDP source ports to unique value per IP flow
    - Stores the new source port in a table with the source address and old source port
    - Replaces source IP address with the external address
  - For packets coming from the public side:
    - Router looks up IP flow by TCP/UDP destination port
    - Replaces destination address and port to the old values

NAT Illustration



NAT Example

NAT changes the source address of each packet to a public IP address with different („rewritten“) source ports



213.31.218.101:5001

213.31.218.101:5002

213.31.218.101:5003

Ethernet Switch

NAT-Router

Internet

TCP Port
Number 1024

192.168.1.2

192.168.1.3

192.168.1.4

Private IP Addresses on Internal Network

NAT Usage

- Not really designed as a security device
- Does not provide security and is often coupled with a firewall

- Used to extend the address space

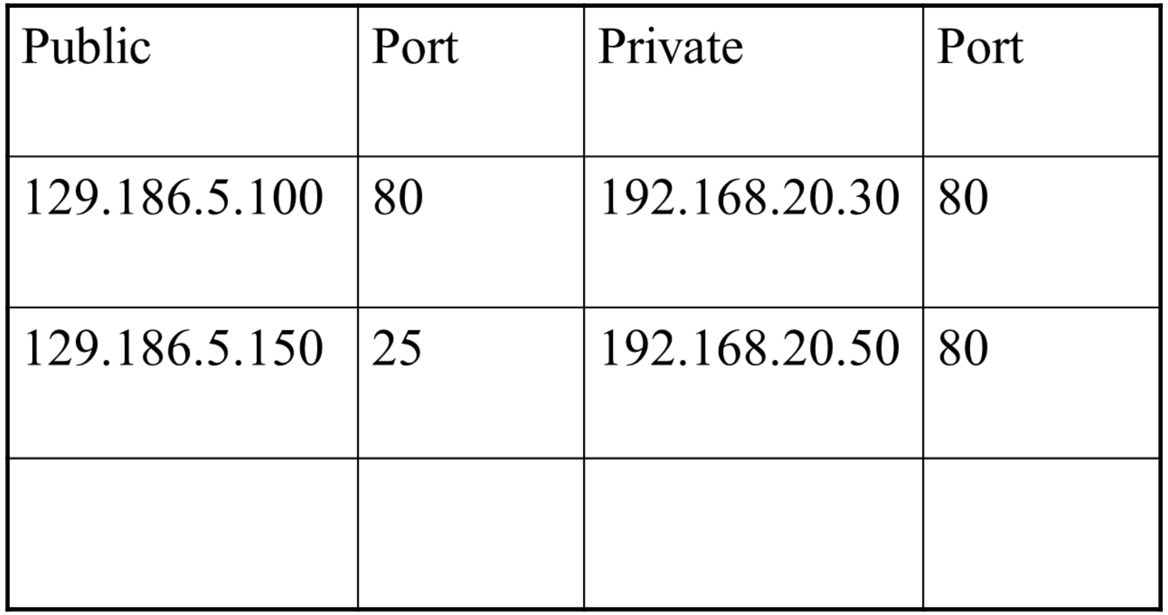
  Internal address ranges

10/8	10.0.0.0
172.16/12	172.16.0.0 (16 class B networks)
192.168/16	192.168.0.0 (class B network)

- Static NAT
- Dynamic NAT

Static NAT

- One to one mapping of external addresses to internal addresses
- Used when a small number of machines need Internet access.
- NAT looks like a router to the inside machines and the destination to outside machines

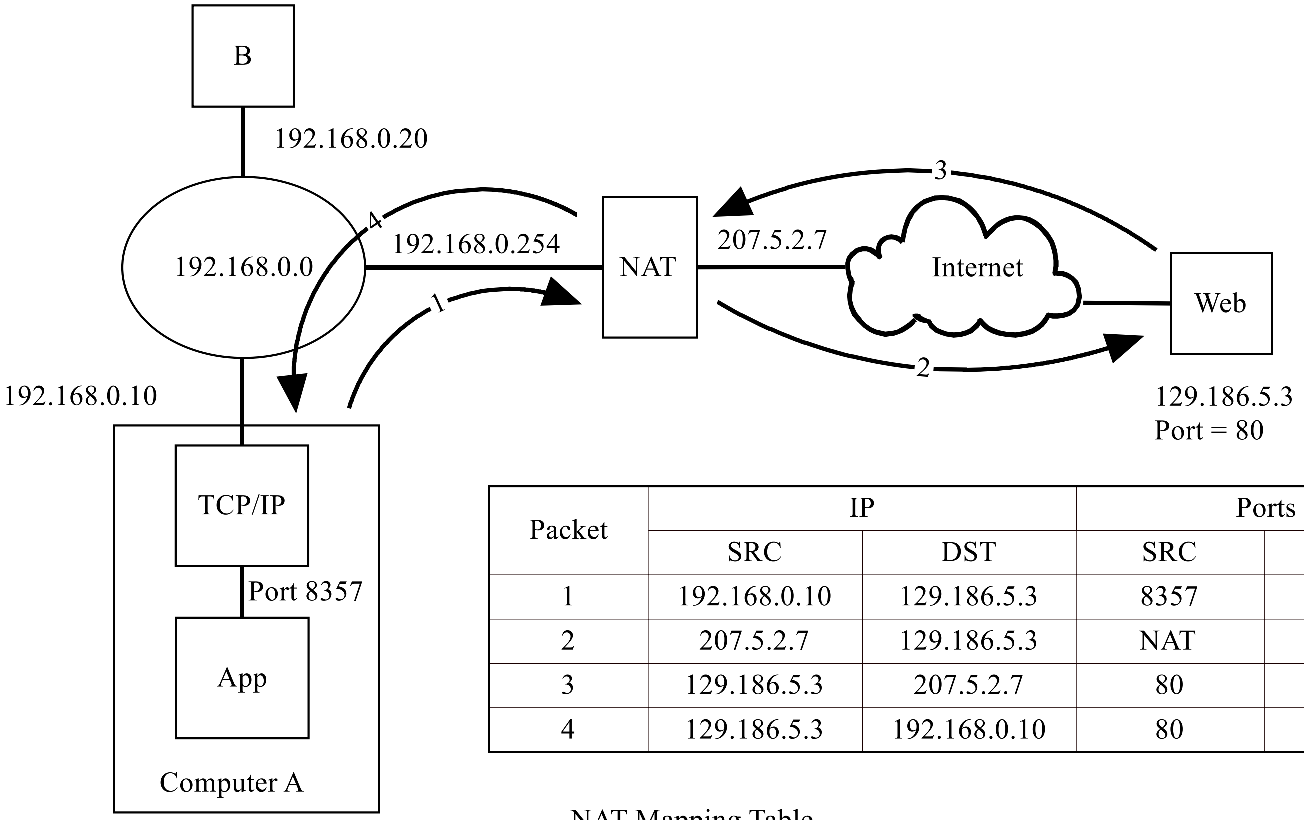


Public	Port	Private	Port
129.186.5.100	80	192.168.20.30	80
129.186.5.150	25	192.168.20.50	80

Dynamic NAT

- More machines on the inside than IP addresses on the outside.
- Used for outgoing access
- Inside can have same address range as a valid outside network (overlapping)

NAT (Port Mapping)



Packet	IP		Ports	
	SRC	DST	SRC	DST
1	192.168.0.10	129.186.5.3	8357	80
2	207.5.2.7	129.186.5.3	NAT	80
3	129.186.5.3	207.5.2.7	80	NAT
4	129.186.5.3	192.168.0.10	80	8357

NAT Mapping Table

Public IP	Ports		Private IP	Ports	
	SRC	DST		SRC	DST
129.186.5.3	NAT	80	192.168.0.10	8357	80

QUEEN'S UNIVERSITY BELFAST

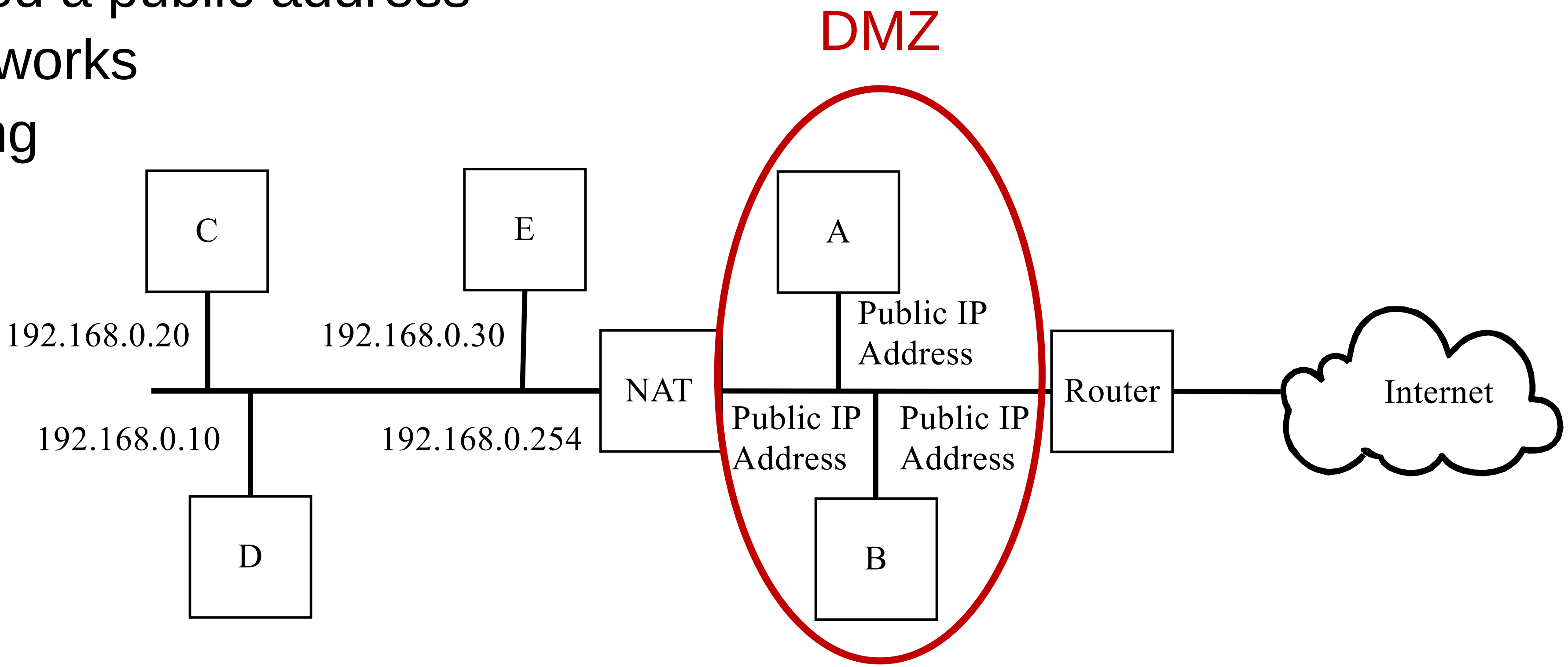
NAT is used to map several external (public) addresses to a single internal (private) address.

A. True

[✓ B. False]

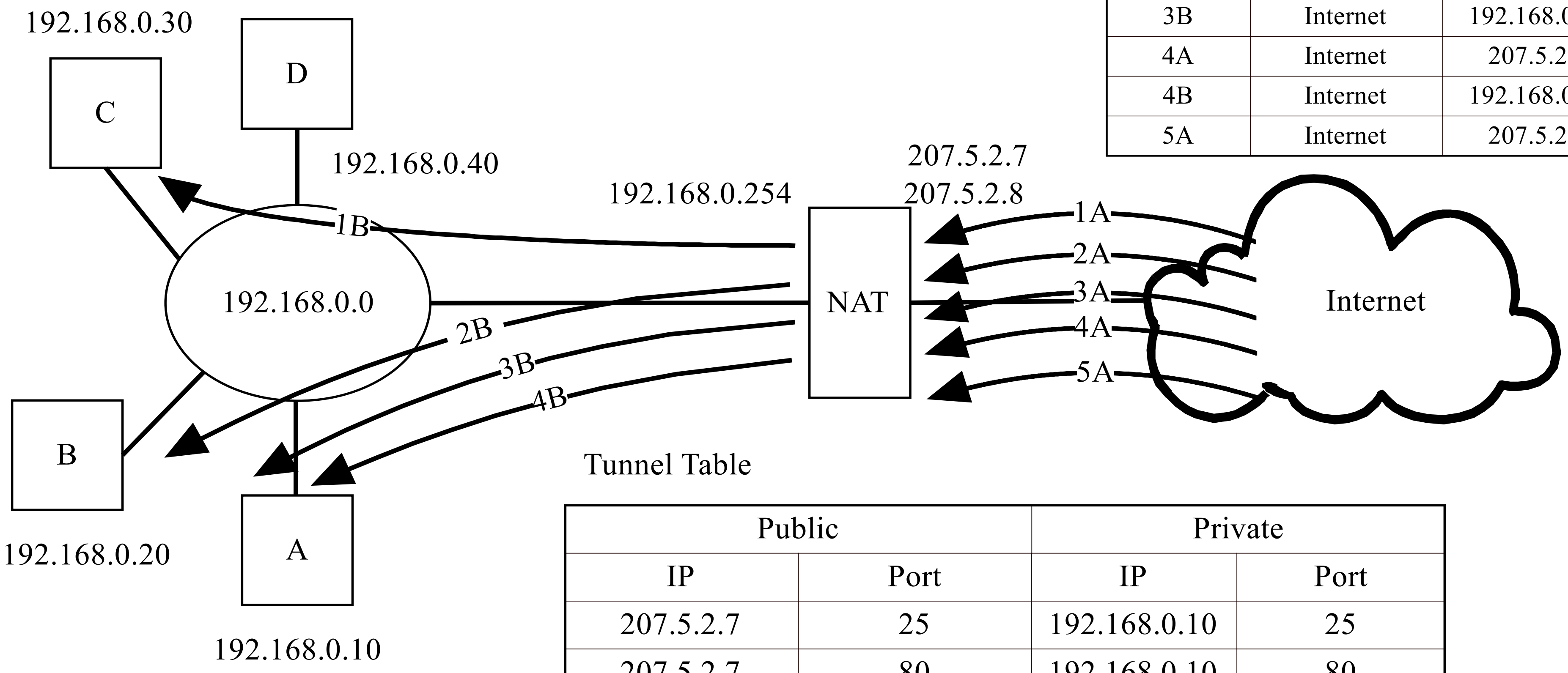
Handling inbound connections e.g. public servers

- Servers need a public address
  - Two networks
  - Tunneling



Tunneling through a NAT

Packet	IP		Ports	
	SRC	DST	SRC	DST
1A	Internet	207.5.2.8	8357	100
1B	Internet	192.168.0.30	8357	80
2A	Internet	207.5.2.8	7384	80
2B	Internet	192.168.0.20	7384	80
3A	Internet	207.5.2.7	2345	80
3B	Internet	192.168.0.10	2345	80
4A	Internet	207.5.2.7	2554	25
4B	Internet	192.168.0.10	2554	25
5A	Internet	207.5.2.7	6623	22



Tunnel Table

Public		Private	
IP	Port	IP	Port
207.5.2.7	25	192.168.0.10	25
207.5.2.7	80	192.168.0.10	80
207.5.2.8	80	192.168.0.20	80
207.5.2.8	100	192.168.0.30	80

Tunneling through a NAT

- Note Packets 2 and 3
  - Public port matches private port
  - Typical – most applications use predefined port numbers e.g. port 80 (web/http)
  - Tunneling limitation – only one private device per public IP address and port number combination
- Note Packet 5
  - Destination address of the NAT and destination port not in the tunnel table
  - NAT either drops the packet or sends back ICMP destination unreachable packet

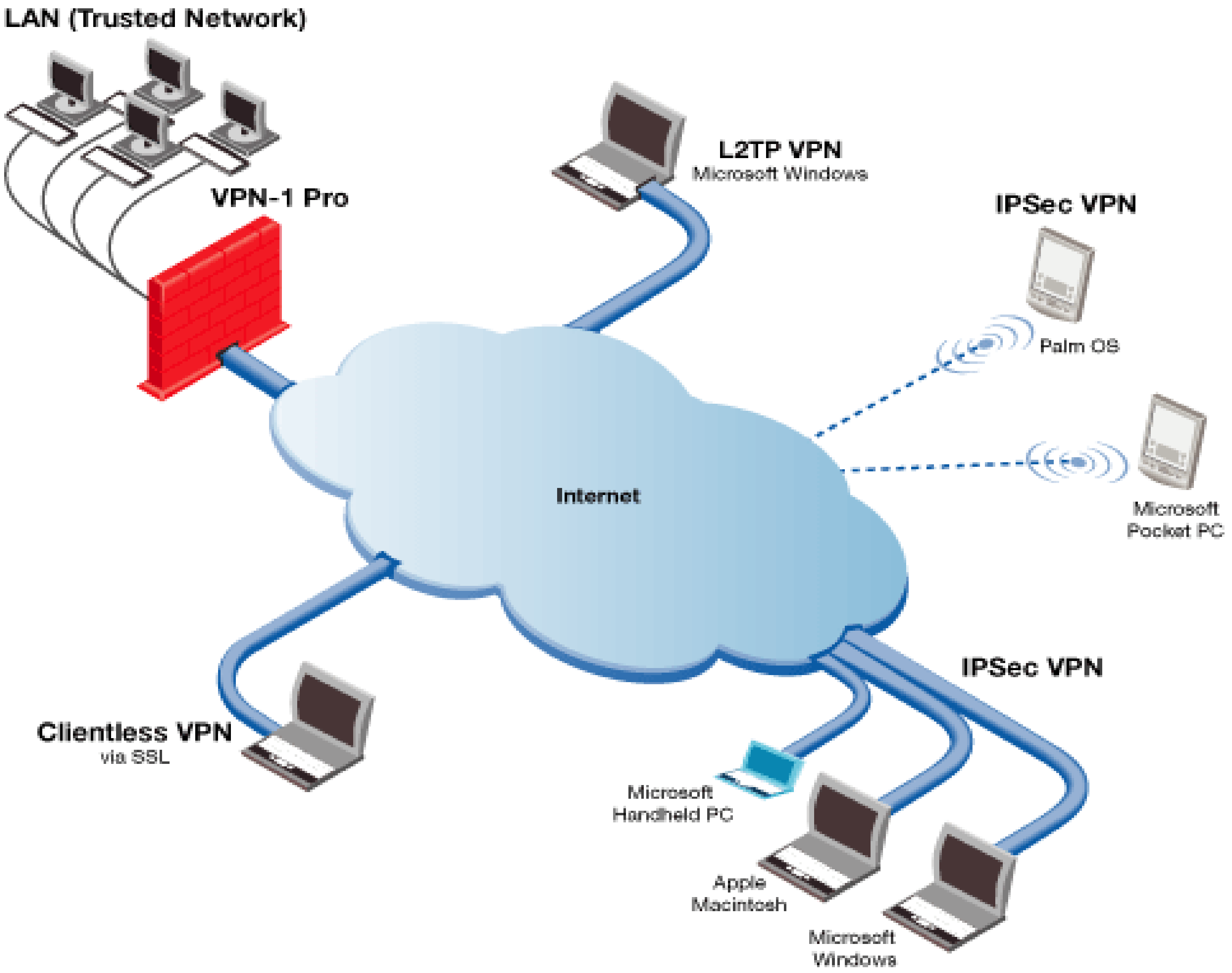
Virtual Private Networks

- Used to create encrypted and authenticated communication channels (tunnels) between devices
- Three different modes of use:
  - Remote access client connections
  - LAN-to-LAN internetworking
  - Controlled access within an intranet
- Several different protocols
  - PPTP – Point-to-point tunneling protocol
  - L2TP – Layer-2 tunneling protocol
  - Generic Routing Encapsulation (GRE)
  - IPsec

Data layer

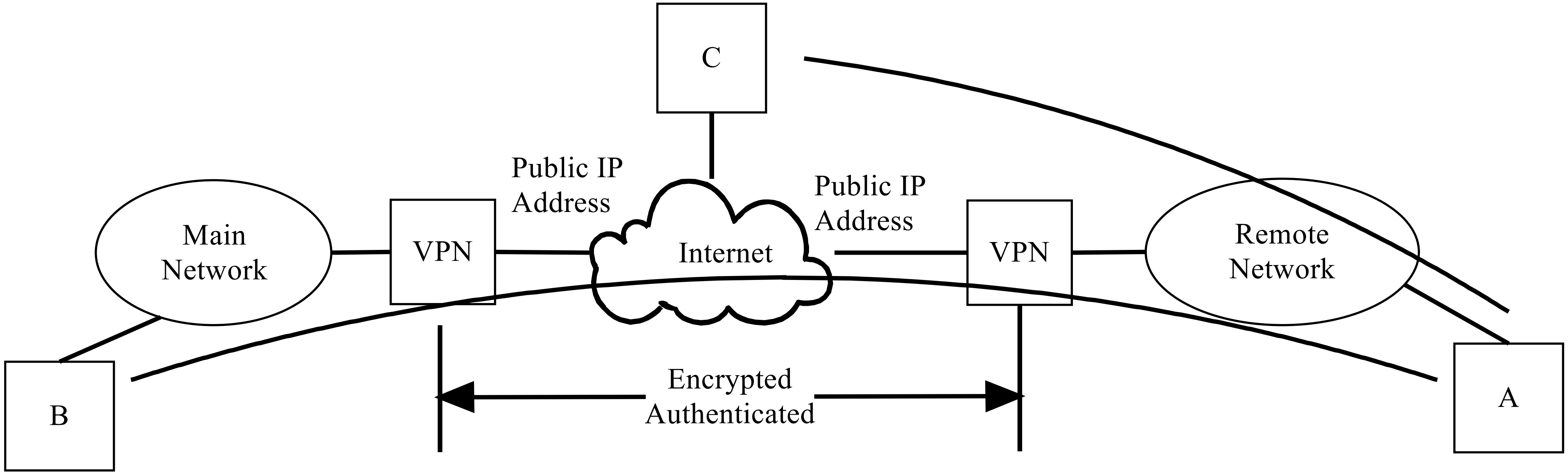
Network layer

Virtual Private Networks



Network to Network VPN

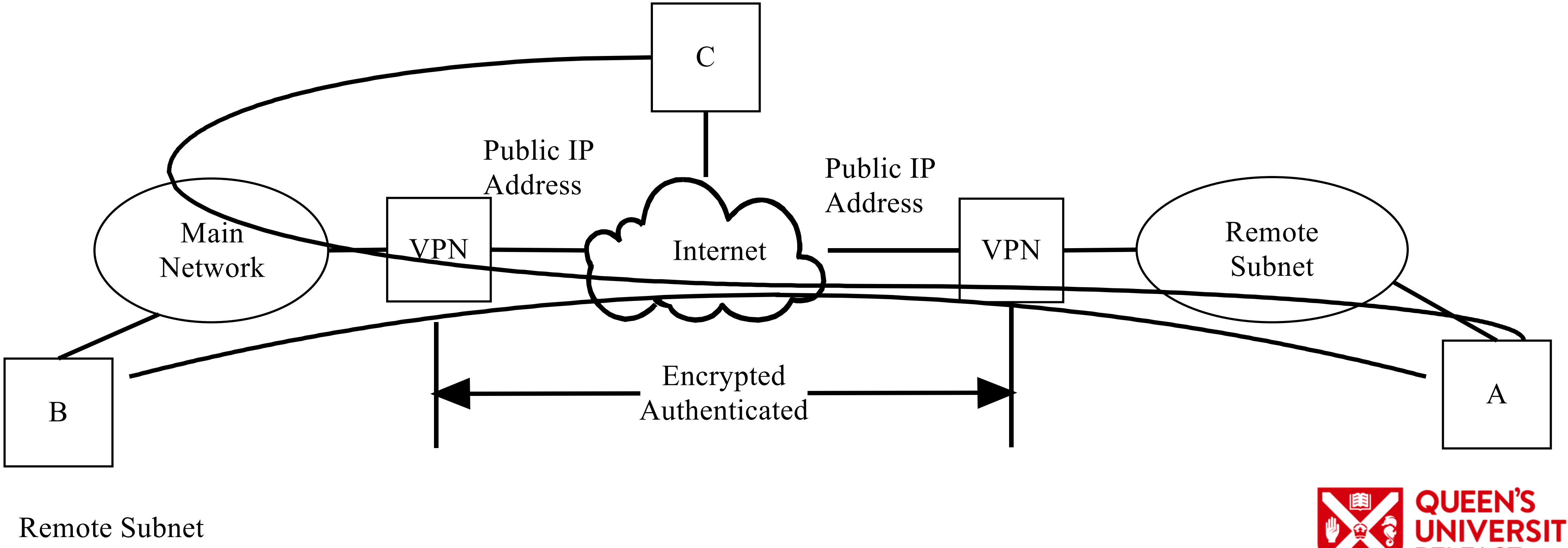
- VPN only when talking to target (main) network
- Other traffic goes directly to destination



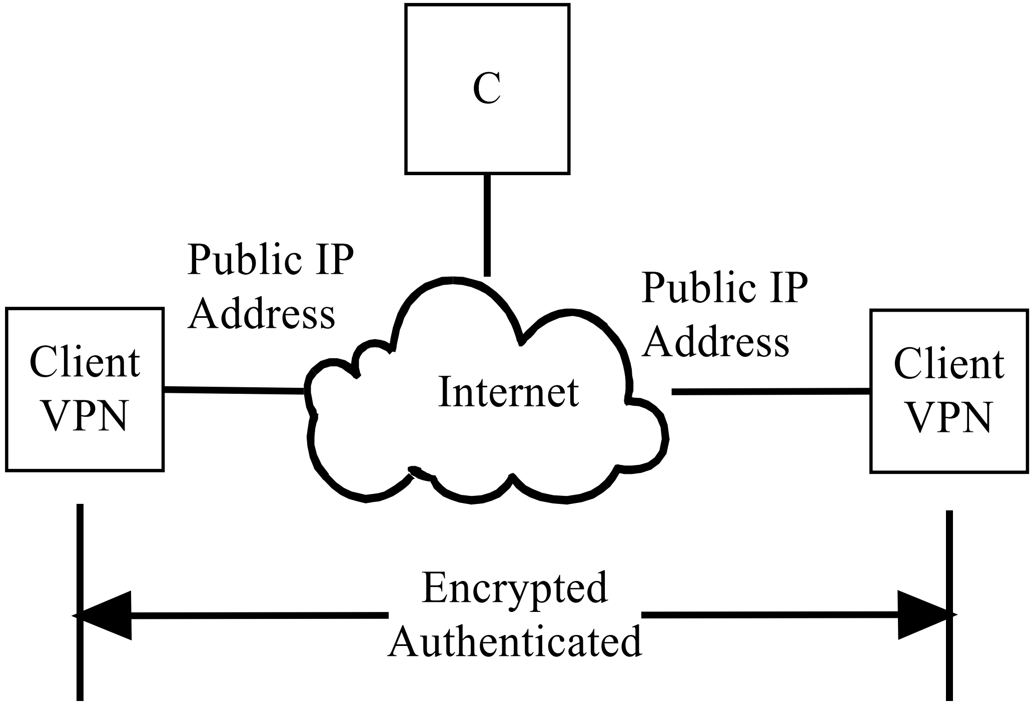
Remote Network

Network to Network VPN

- Always uses VPN
- All traffic is routed through target (main) network

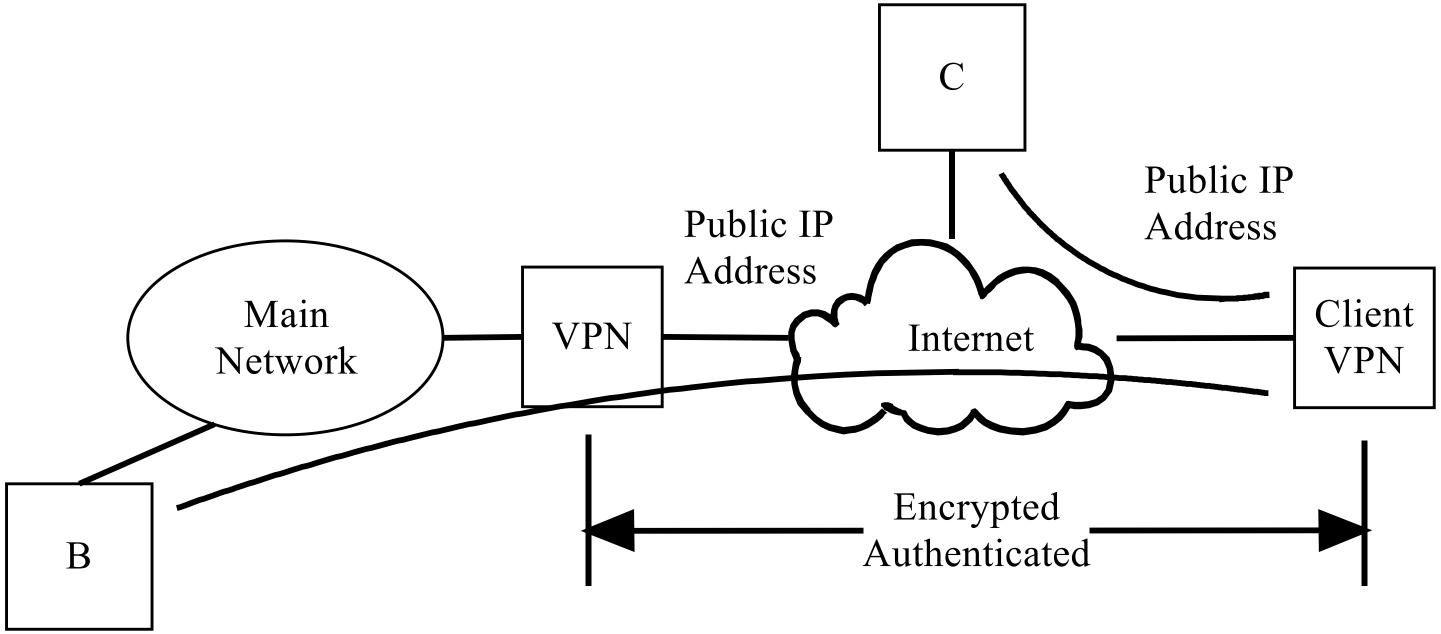


Client-to-Client VPN



Client to Network VPN

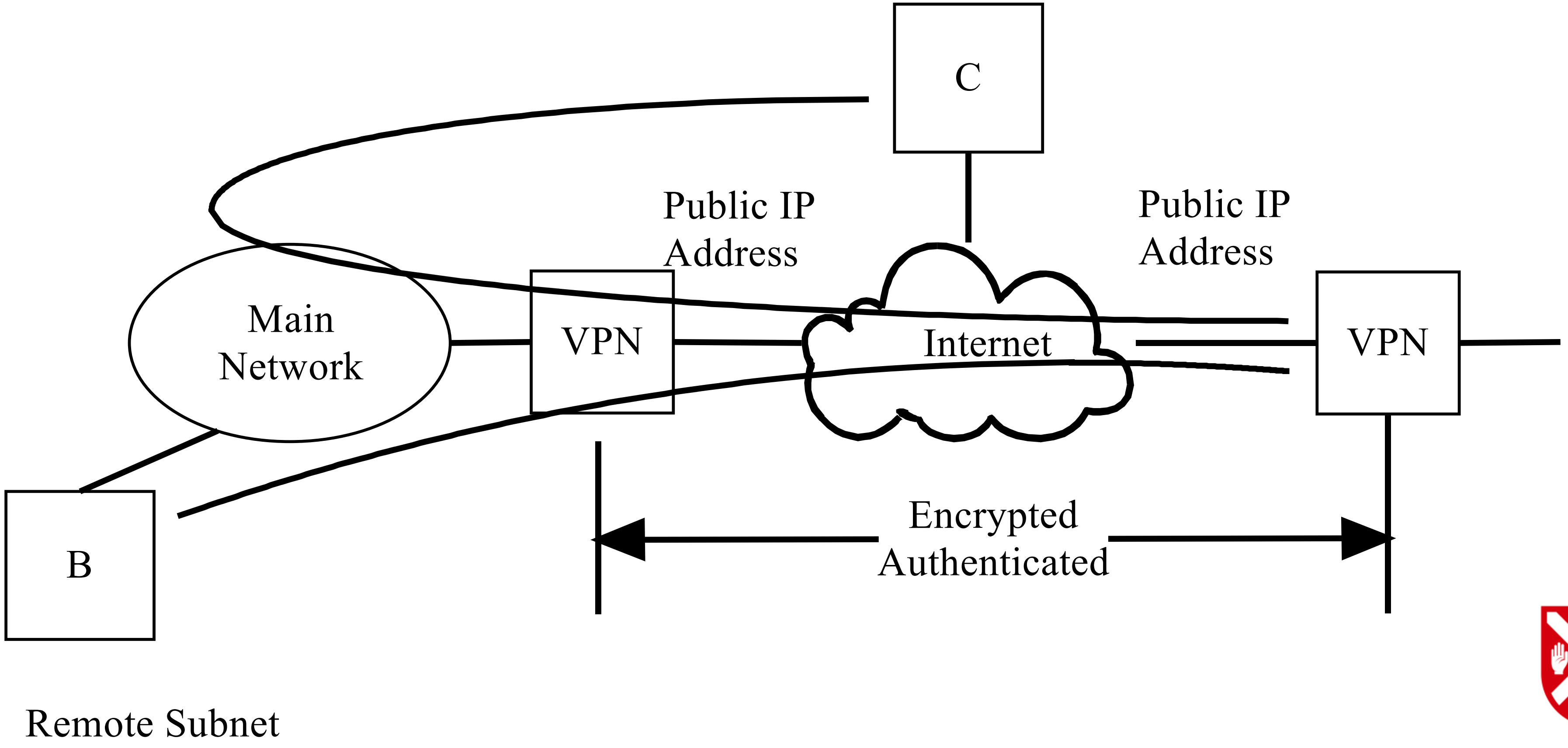
- VPN only when talking to target (main) network
- Other traffic goes directly to destination



Remote Access

Client to Network VPN

- Always uses VPN
- All traffic is routed through target (main) network



Point-to-Point Protocol

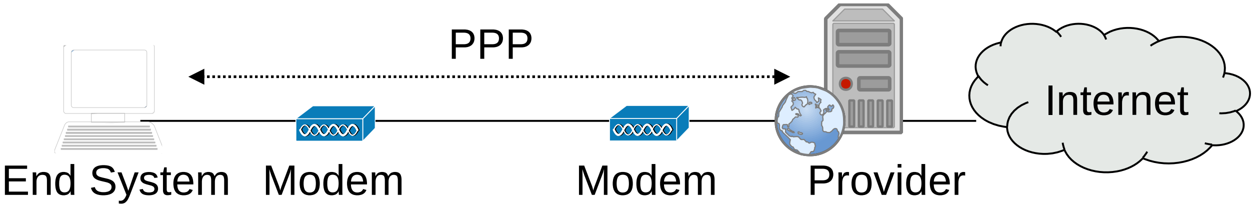
Background

Large parts of the Internet rely on point-to-point connections:

- Wide area network (WAN) connections between routers
- Dial-up connections of hosts using modems and telephone lines

Point-to-Point Protocol (PPP) [RFC 1661/1662]:

- Layer-2 frame format with frame delimitation and error detection
- Control protocol *(Link Control Protocol, LCP)* for connection establishment, -test, -negotiation, and -release
- Separate *Network Control Protocols (NCP)* for supported Layer-3 protocols



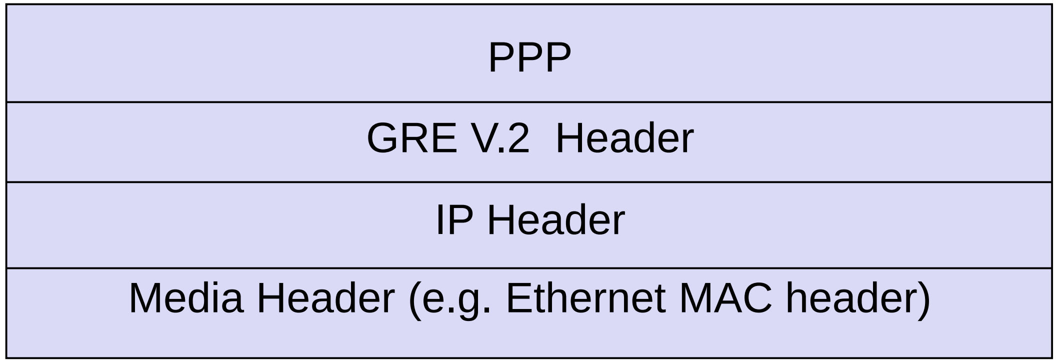
Point-to-Point Tunneling Protocol

- PPP was originally designed to be run between “directly” connected entities, that is entities which share a layer-2 connection
    - Example: a PC and a dialup-router of an Internet service provider connected over the telephone network using modems
- PPP has optional security services of authentication and encryption
- The basic idea of PPTP is to extend the protocol’s reach over the entire Internet by defining transport of PPP PDUs in IP packets

Point-to-Point Tunneling Protocol

- The payload of PPTP PDUs are PPP packets

- PPP packets are encapsulated in GRE packets (generic routing encapsulation) that themselves are encapsulated in IP packets:



PPP

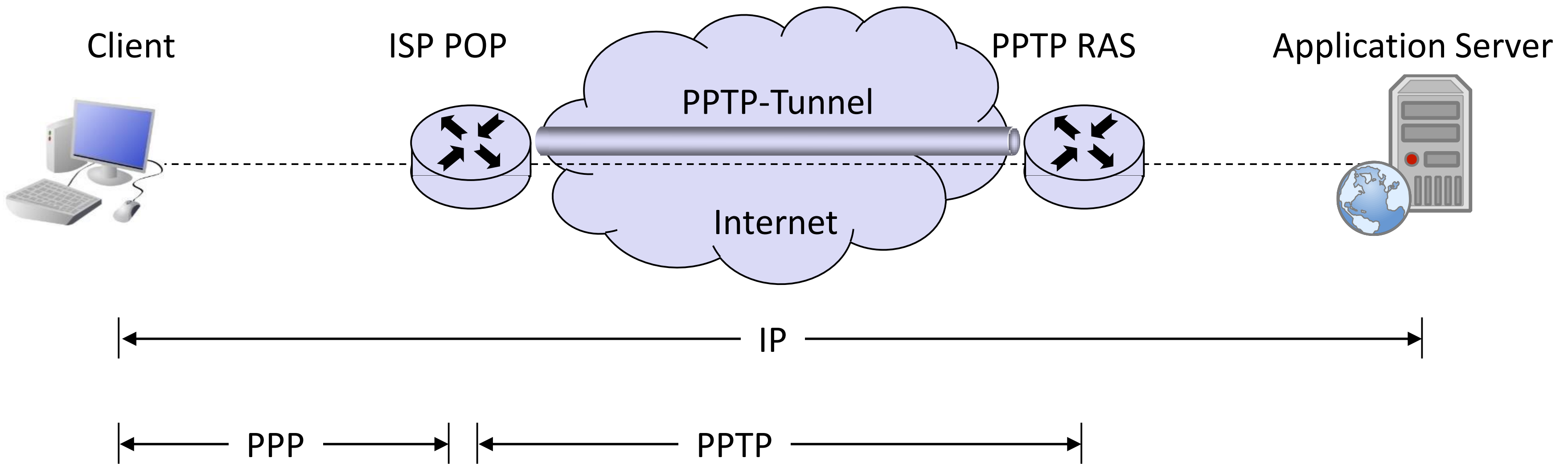
GRE V.2 Header

IP Header

Media Header (e.g. Ethernet MAC header)

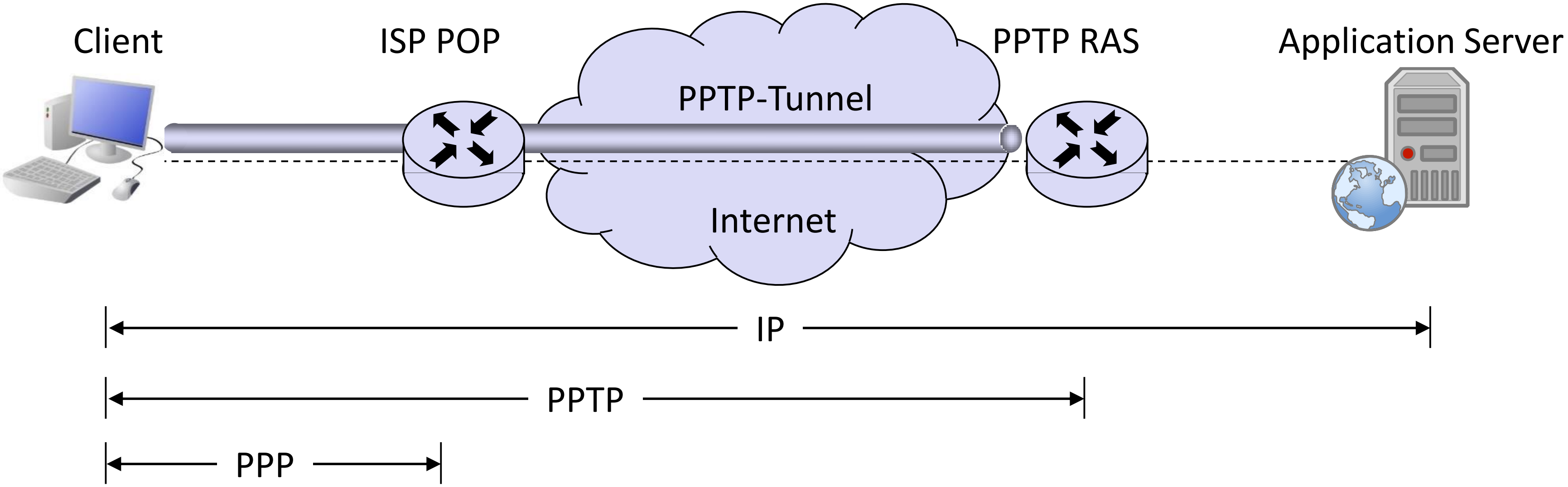
- PPTP realizes a “tunnel” over the Internet that carries PPP packets

PPTP: Compulsory Tunneling Protocol Layers



IP	IP	IP
PPP	PPP	Layer 2 (e.g. 802.x)
PPP Framing (e.g. HDLC)	GRE Version 2	
	IP	
	Layer 2	
Physical Layer	Physical Layer	Physical Layer

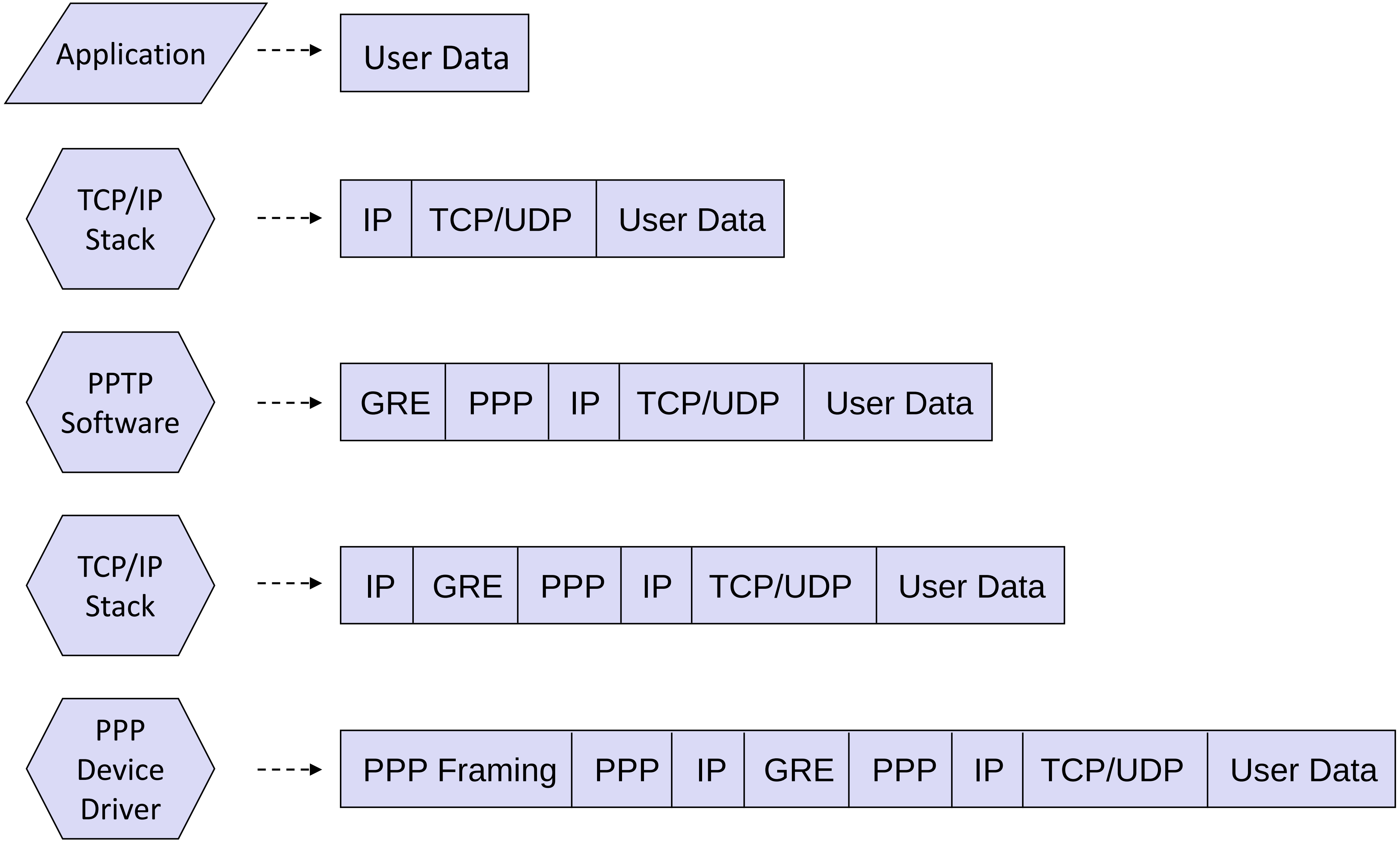
PPTP: Voluntary Tunneling Protocol Layers



IP	IP	IP
PPP	PPP	Layer 2 (e.g. 802.x)
GRE Version 2	GRE Version 2	
IP	IP	
PPP	Layer 2	
PPP Framing (HDLC)		
Physical Layer	Physical Layer	Physical Layer

PPTP: Voluntary Tunneling Packet Construction at Client

Background



Application → User Data

TCP/IP Stack → IP | TCP/UDP | User Data

PPTP Software → GRE | PPP | IP | TCP/UDP | User Data

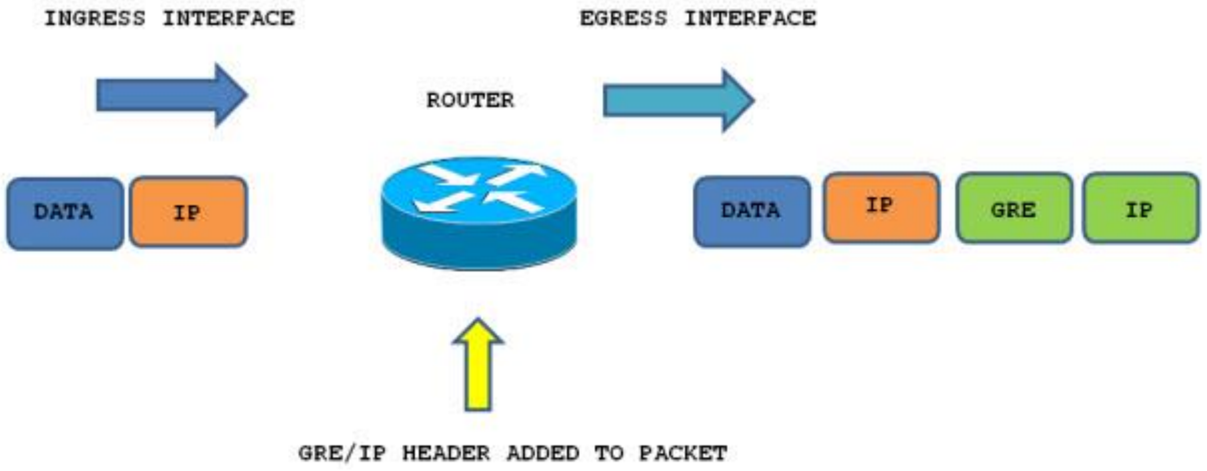
TCP/IP Stack → IP | GRE | PPP | IP | TCP/UDP | User Data

PPP Device Driver → PPP Framing | PPP | IP | GRE | PPP | IP | TCP/UDP | User Data

Generic Routing Encapsulation (GRE)

Background

- Basic, non-secure (no encryption) site-to-site VPN tunneling protocol developed by Cisco
- Encapsulates a wide variety of protocol packet types inside IP tunnels
- Creates a virtual point-to-point link to routers at remote points, over an IP internetwork
- For data protection, IPSec must be configured



Generic Routing Encapsulation (GRE)

Background

Encapsulation—A switch operating as a tunnel source router encapsulates and forwards GRE packets as follows:

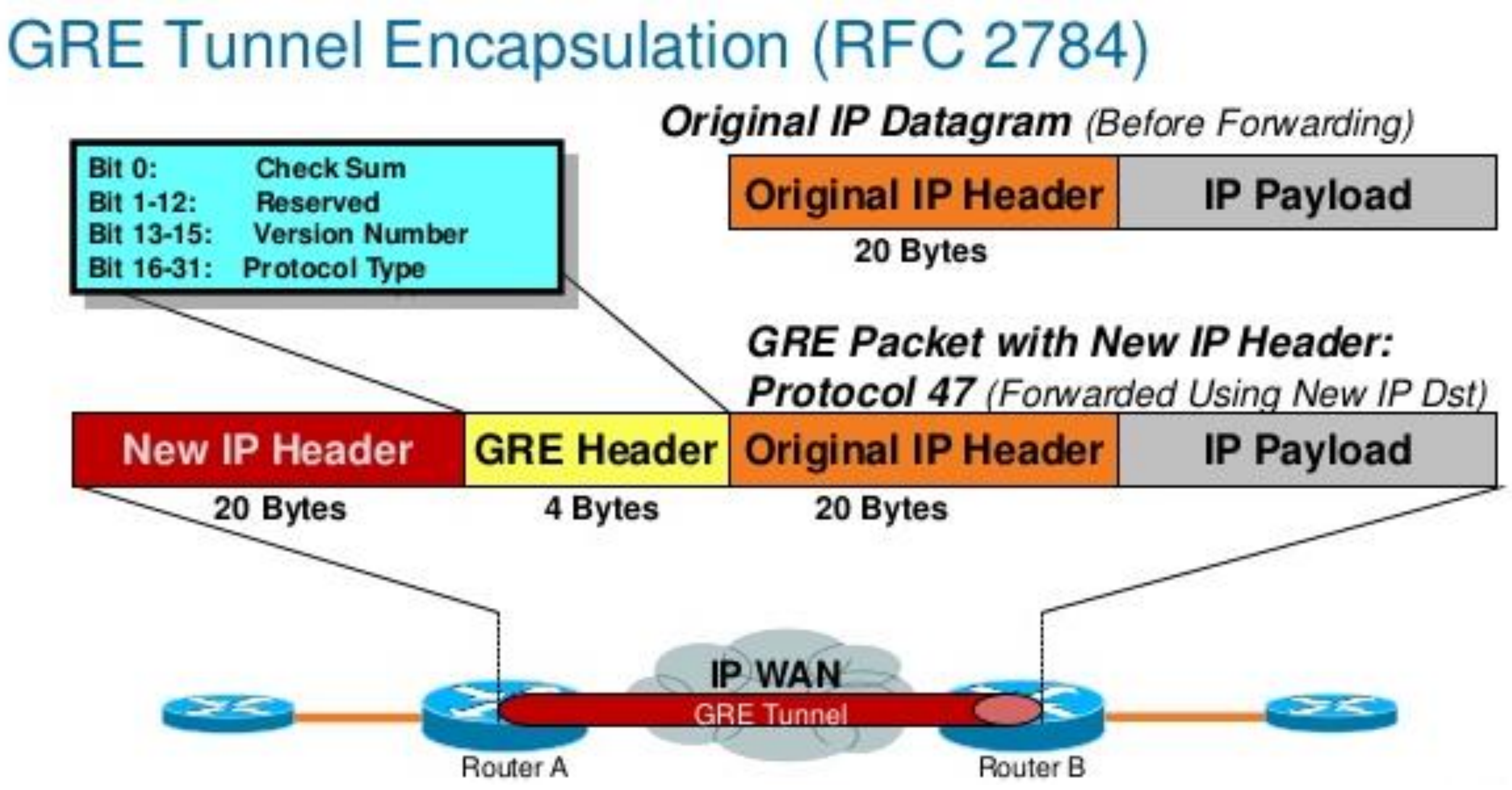
1. When a switch receives a data packet (payload) to be tunneled, it sends the packet to the tunnel interface.
2. The tunnel interface encapsulates the data in a GRE packet and adds an outer IP header.
3. The IP packet is forwarded on the basis of the destination address in the outer IP header.

De-encapsulation—A switch operating as a tunnel remote router handles GRE packets as follows:

1. When the destination switch receives the IP packet from the tunnel interface, the outer IP header and GRE header are removed.
2. The packet is routed based on the inner IP header.

Generic Routing Encapsulation (GRE)

Background



PPTP Compulsory Tunneling provides end-to-end security between the client PC and the remote access server.

A. True

[✓ B. False]

PPTP/PPP Proprietary Extensions - History

Background

- PPTP has been largely deployed as a consequence of Microsoft’s support for it:
  - It has been developed with Microsoft’s active involvement and is documented in [RFC2637]
  - Microsoft implemented it as a part of its *Remote Access Service (RAS)*
- Microsoft further specified “proprietary” extensions for PPP:
  - Microsoft PPP CHAP Extensions [RFC2433]
  - Microsoft Point to Point Encryption Protocol [RFC3078]
- However, a series of vulnerabilities were discovered in PPTP version 1 and also in an improved version 2:
  - A general consensus to adopt PPTP as a standard protocol could not be reached in the IETF working groups
  - Furthermore, a similar protocol *(Layer 2 Forwarding, L2F)* had been proposed by Cisco as a competing approach
  - As a consequence, a compromise was found to merge the advantages of both proposals into one single protocol *Layer 2 Tunneling Protocol (L2TP)*

Comparison of PPTP and L2TP

Both protocols:

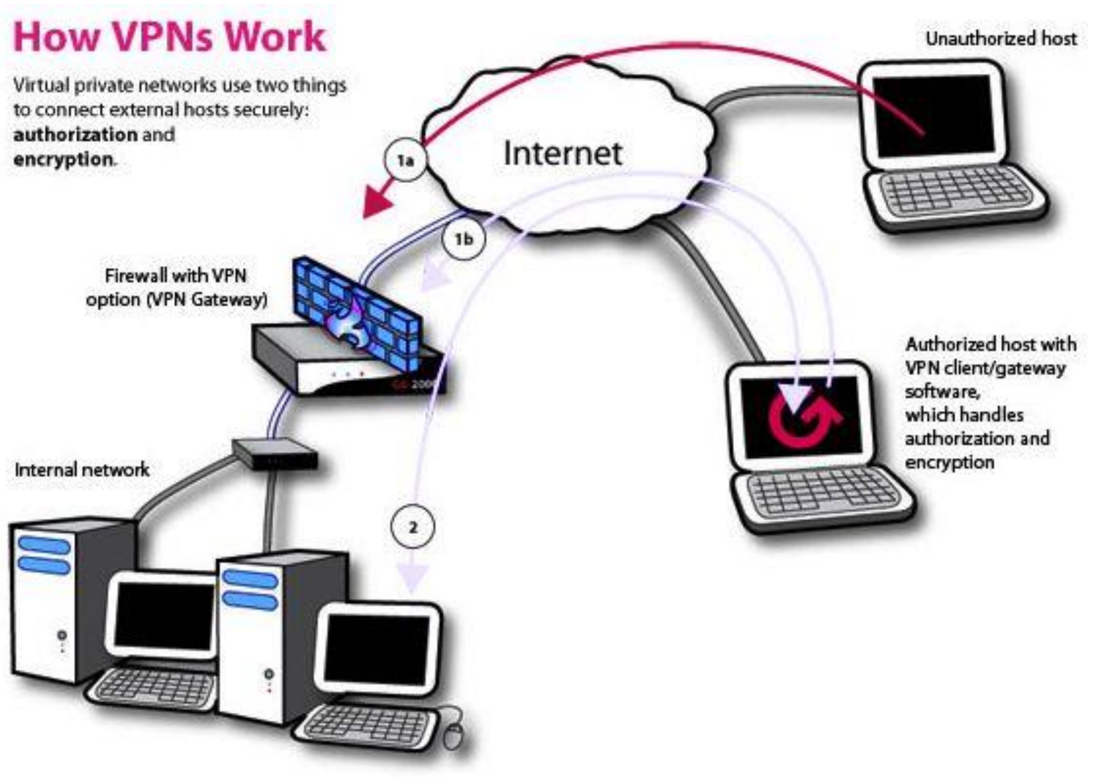
- use PPP to provide an initial envelope for user packets
- extend the PPP model by allowing the layer-2 and the PPP endpoints to reside on different devices (i.e. extend across the Internet)
- support voluntary and compulsory tunneling
- provide for header compression

- PPTP is considered easy to setup, compatible with most systems but has security issues e.g. weak encryption

- L2TP (with IPSec for encryption) offers stronger security -> we look at IPSec next …

Virtual Private Networks

A restricted-use, logical computer network that is constructed from the system resources of a relatively public, physical network (such as the Internet), often by using encryption, and often by tunneling links of the virtual network across the real network [RFC2828]



How VPNs Work
Virtual private networks use two things to connect external hosts securely: **authorization** and **encryption**.
Unauthorized host
Internet
1a
1b
Firewall with VPN option (VPN Gateway)
Authorized host with VPN client/gateway software, which handles authorization and encryption
Internal network
2

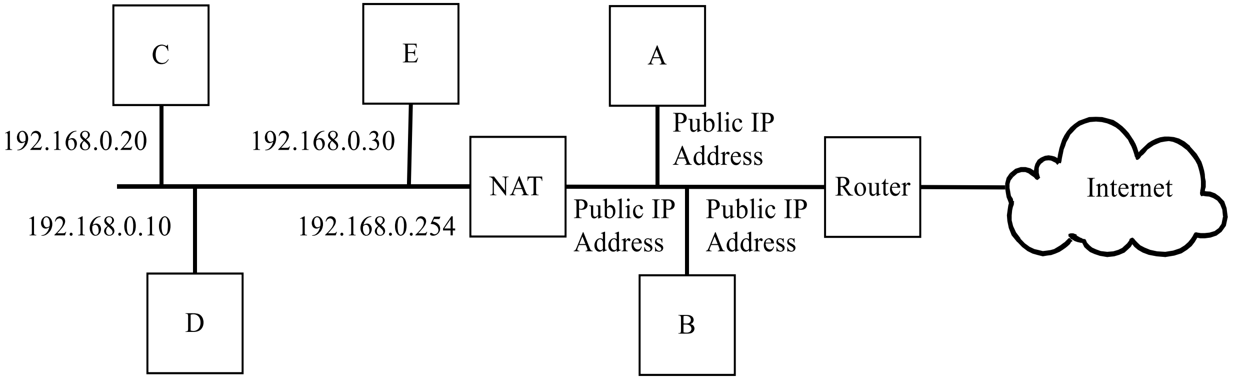
What is illustrated in the diagram?

A. VPN

B. Tunnel

C. PPP

✓ D. DMZ



Summary

- IP Filtering
- Network Address Translation – Static, Dynamic
- Virtual Private Networks
  - Types e.g. Network-to-network etc.
  - Point-to Point Tunneling Protocol
  - PPTP vs. L2TP

Questions?

Next Session: Tuesday, 19 February 2019

Tunneling and VPNs – Part 2