Module Ten

CSG1105 Applied Communications

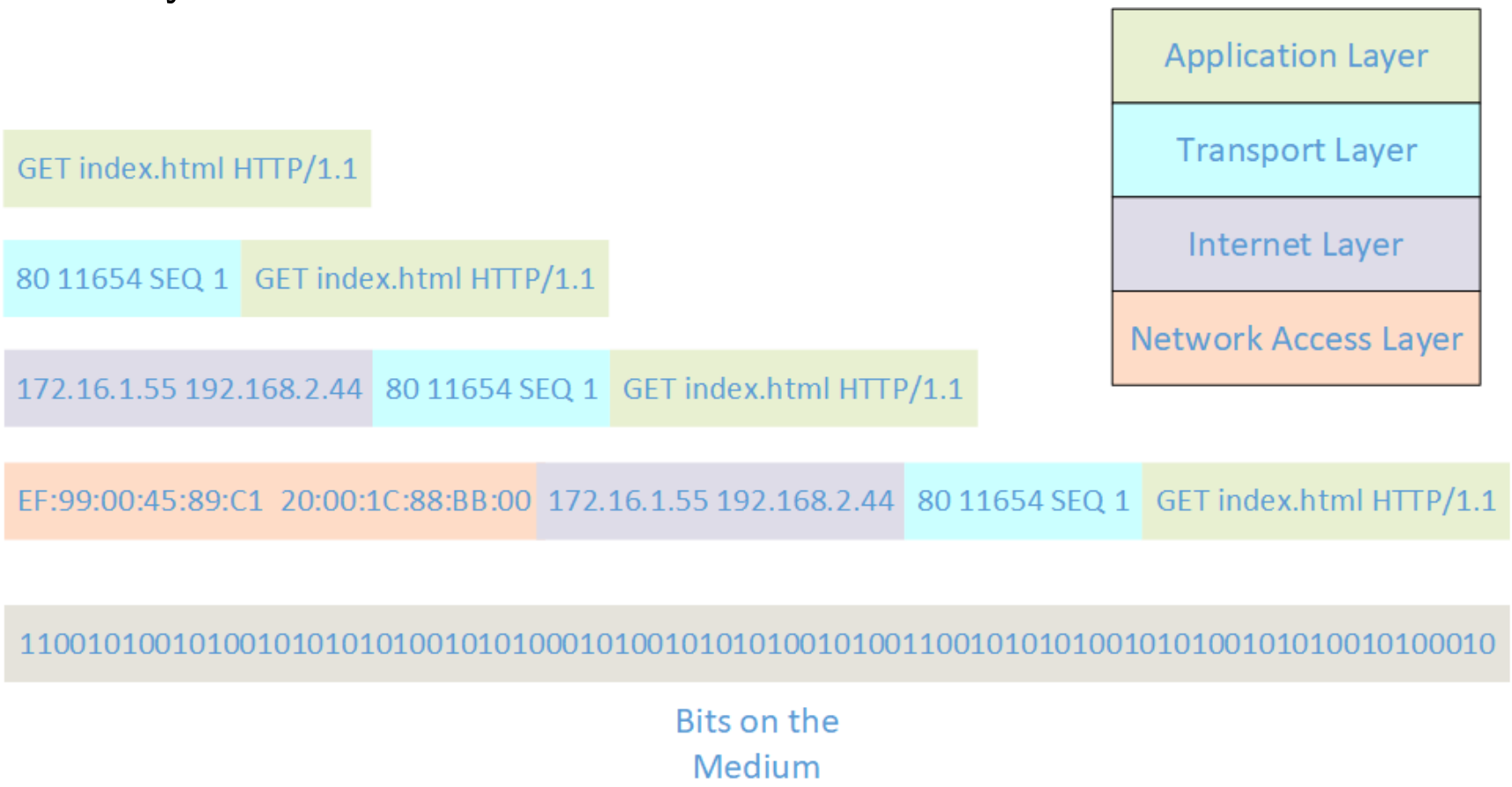
May 10, 2020

Network Tunnels

- Tunnelling is a **technique** used to transport traffic over an intermediary network by encapsulating packets within packets
- It has a long history of use in networks for
- It may be used for:
  - transporting non-IP traffic over an IP network (**Bridging**)
  - using a Public IP network as an encrypted WAN link (**VPNs**)
  - transporting incompatible traffic (**IPv6, Private IP addresses**) over an IP network
  - subverting restrictive Firewall rules (**ssh,HTTP tunnelling**)

Encapsulation 1

- Encapsulation was covered in Module Two.
- This diagram shows the PDUs from the higher layer encapsulated in a lower layer PDU



Encapsulation 2

- Tunnelling uses the same concept of encapsulation, but not as a layer.
- In this example, a LAN packet (Internetwork Layer) is encapsulated in a WAN packet (also Internetwork layer)

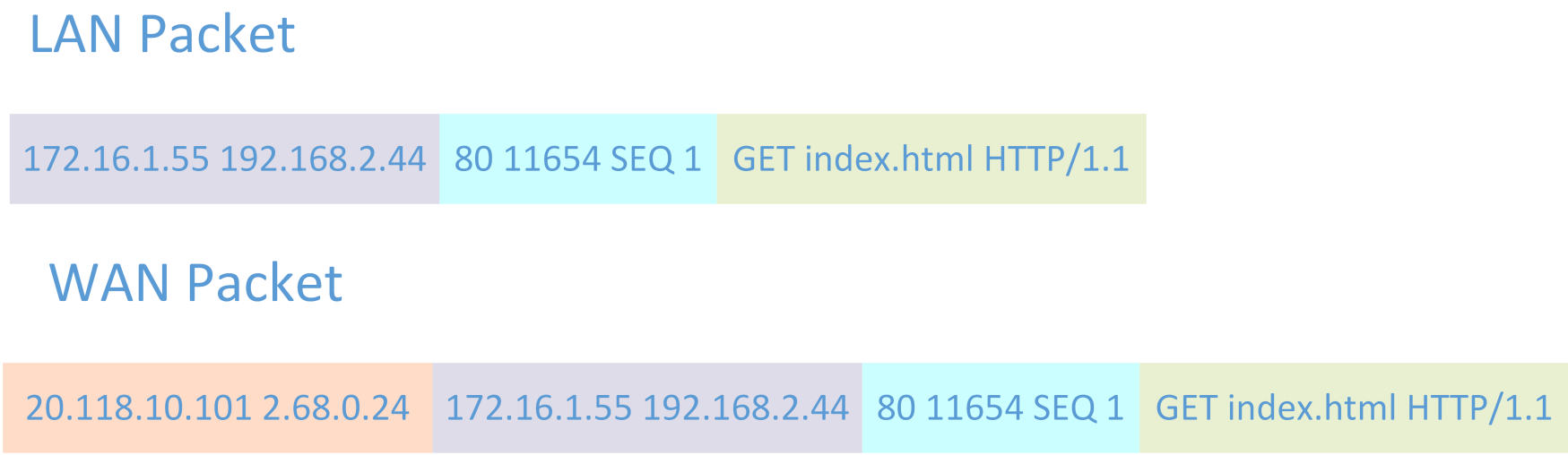


Figure 1: Tunnelling Encapsulation

How is this different from NAT?

- We have previously seen how private IPs can be used in a LAN to access public IP sites
- The NAT gateway **re-writes** the IP addresses dynamically
- With tunnelling, **we are *not* accessing the Public Internet**
- In this example, tunnelling uses the Public Internet as a transport medium
- Tunnelling allows us to use the Internet as a **WAN medium**, like those seen in Module Nine (MPLS etc)

IP Tunnel

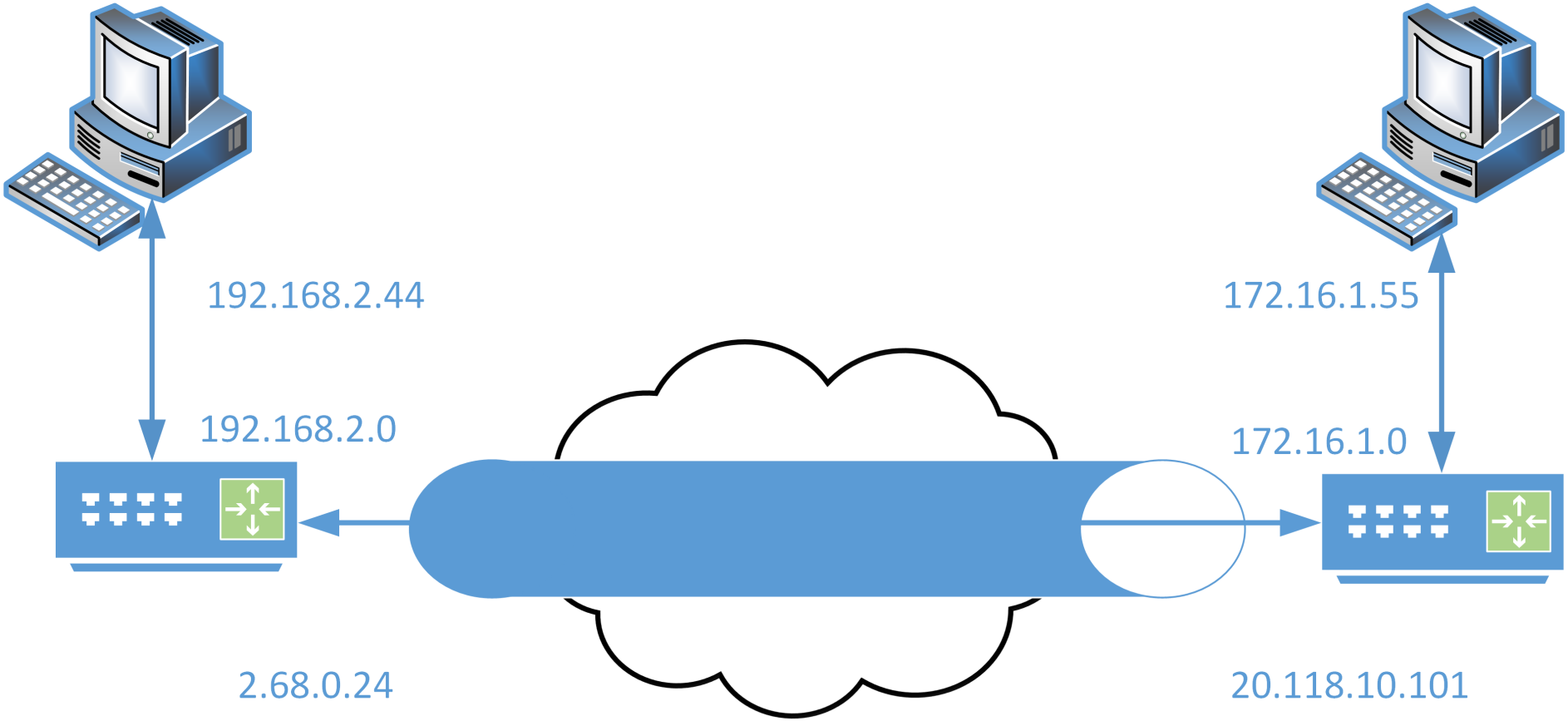


Figure 2: IP Tunnel

Tunnelling

- Tunnelling is a generic technique of encapsulating a PDU inside another PDU
- In the late 1980's, MS-DOS based **LAN** gaming used a networking protocol from **Novell** (now part of Micro Focus) called **SPX/IPX** which was roughly equivalent to TCP/IP but used a different addressing scheme
- Enthusiasts developed a method of encapsulating IPX packets inside of IP packets to allow LAN gaming to be done over Internet connections

802.1Q Tunnelling (Q-in-Q)

- In Module Six on VLANs, the topic of double-tagging was introduced
- In Module Nine on WANs, the topic of Carrier Ethernet was introduced
- 802.1Q Tunnelling is a **Layer Two** tunnelling technique using VLAN concepts
- A customer designates a VLAN for inter-site traffic and a **router** connected to a carrier controlled switch tags the traffic
- The carrier will allocate a VLAN in it's network for that customer and will add the second VLAN tag to direct the traffic on it's internal network

IPv6 Tunnelling

- The dominant Internetwork layer protocol is currently IPv4
- ISPs are increasingly providing IPv6 access, but end-to-end IPv6 across the Internet is not guaranteed
- There are several IPv6 over IPv4 tunnelling protocols available which allow IPv6 LANs to communicate over an IPv4 backbone
- There also exists protocols to tunnel IPv4 over a IPv6 network
- There are many issues to confront including NAT/PAT gateways and further details are beyond the scope of this unit

VPNs

- Tunnelling allows private WAN connections to be established over a public IP network
- The tunnelling techniques described above provide a mechanism for establishing one or more point to point connections between locations
- What has not yet been considered is the security of these connections
- Any entity who has access to the network infrastructure in the public IP network would be able to tap the connection (in a similar fashion to how we used Wireshark) and view the contents of the packets
- In order to be secure, VPN connections need to be **Encrypted**.
- Full details of the encryption methods are beyond the scope of this unit.

Varieties of VPN

- Remote Access - Device to Router/Host
- Site to Site - Router to Router

Remote Access VPNs

- A remote access VNP allows encrypted access to resources for users from anywhere on the Internet
- The remote computer requires a VPN Client to be installed (eg ECU uses CISCO Anyconnect client)
- A common approach on the OS is to create a **Virtual NIC** with an associated IP address.
- Depending on the client,
  - The default gateway is reset to the Virtual NIC IP address and all traffic is directed there
  - It may intercept DNS requests and direct site specific traffic to the Virtual NIC
- There are a number of VPN providers that allow the selection of the termination end point to allow circumvention of Geographic content restrictions and to conceal the IP of the computer establishing the connection

Site to Site VPNs

- Site to site VPNs provide an encrypted IP tunnel through the Internet
- Routers at each end provide the end point for the VPNs although for SOHO users, vendors provide VPN appliances that use the ISP router for transport
- Subnets and routes are configured to use VPN tunnels between each location
- Avoids the requirement for all PCs at a branch office to run Remote access VPN client

PPP - Point-to-Point Protocol

- PPP is a Network Access Layer (OSI Datalink Layer) that operates over duplex links
- It can carry a wide variety of Internetwork layer protocols such as IP, IPX and others
- It replaces SLIP (Serial Line IP) for serial and dial-up connections
- It handles encapsulation, Link negotiation and Network Control negotiation
- Variants operate over Ethernet (PPPoE) and ATM (PPPoA), the later used over DSL links
- Authentication may be performed using CHAP (Challenge Handshake Authentication Protocol)* and EAP (Extensible Authentication Protocol)

IPSec

- Internetwork Layer Protocol
- Transport Mode - just the payload encrypted
- Tunnel Mode - VPN tunnel, all traffic encrypted
- Multiple choices for encryption and authentication
- IPSec is an open standard documented in multiple RFCs

PPTP (obsolete)

- Point to Point Tunnelling Protocol
- Developed by Microsoft, Ascend and 3COM
- Uses GRE (Generic Routing Encapsulation)
- Basic Encryption , easy to break
- TCP port 1723
- Insecure, Avoid

L2TP

- Improved version of PPTP
- Used features of CISCO's L2F and PPTP
- A number of RFCs codify and extend L2TPs features
- L2TP permits the tunnelling of any protocol supported by PPP
- No built in encryption, needs to use IPSec
- UDP Port 500

SSTP - SSL/TLS

- Internetwork Layer Protocol
- Transports PPP traffic over SSL/TLS connection
- Microsoft Proprietary protocol
- Uses SSL 3.0 Encryption (more in a later lecture)
- Runs over TCP Port 443
- Firewall friendly

OpenVPN

- Open Source Commercial Software
- AES Encryption
- Runs over TCP Port 443
- Best cross platform security
- Firewall friendly

SSH - Secure Shell

- Designed for remote shell access
- Uses SSL 3.0 Encryption
- Has a setting which allows X11 or TCP tunnelling
- Runs over TCP Port 22

Downsides of Tunnelling

- Firewall subversion
  - Insider employee can establish a tunnel through a firewall
  - Use of permitted protocols such as HTTP and HTTPS (ports 80 and 443)
  - The insider installs a proxy client (RAT, remote access trojan) and establishes a connection to a remote server
  - Remote server is able to view and exfiltrate data from the network