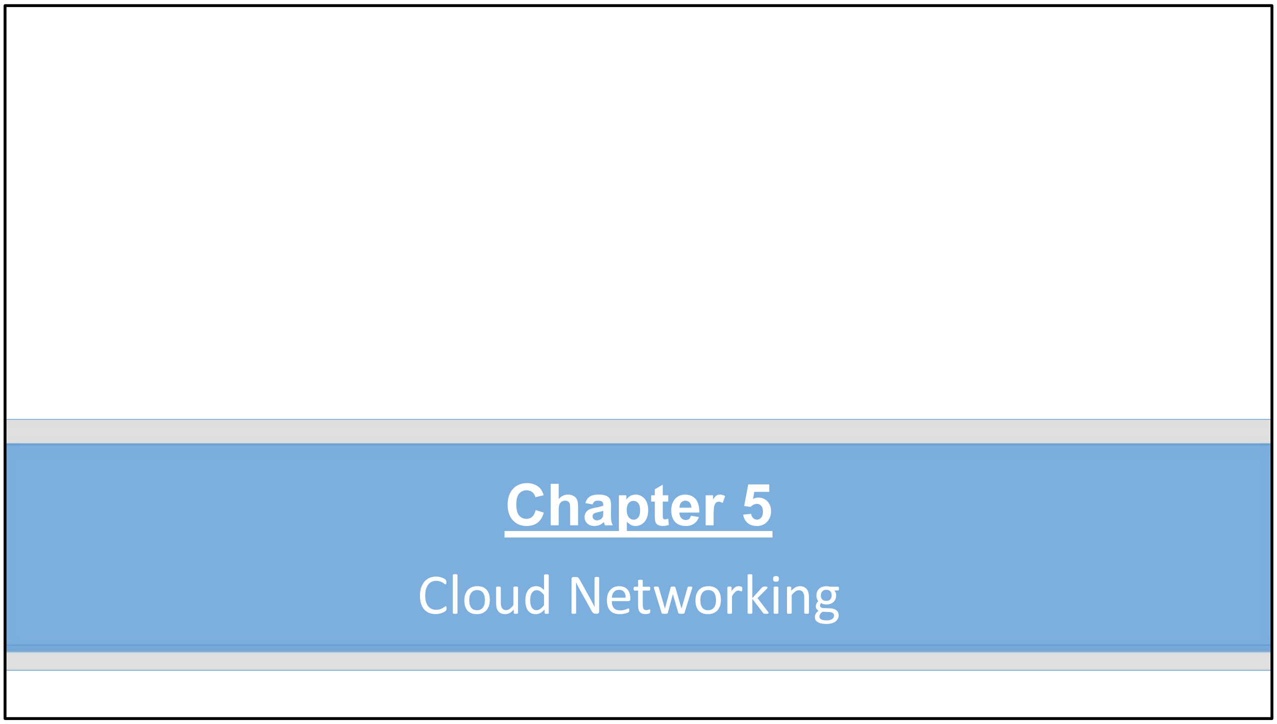
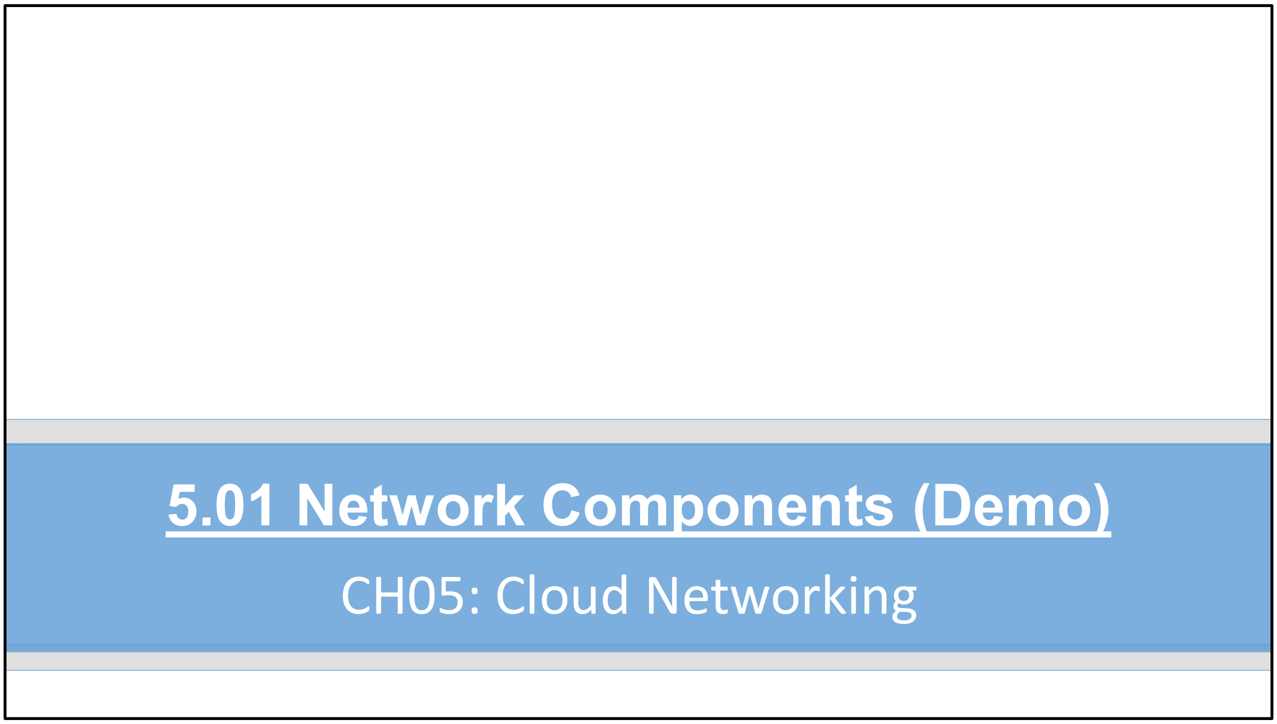


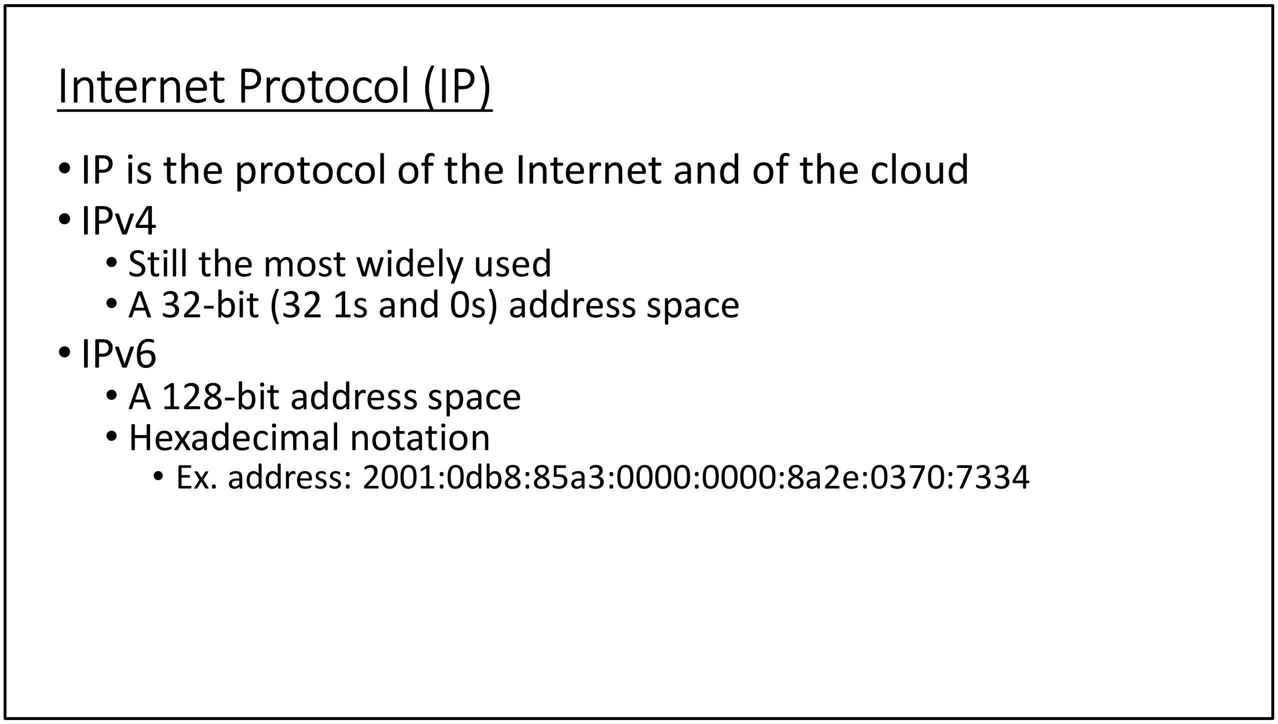
Chapter 5

Cloud Networking



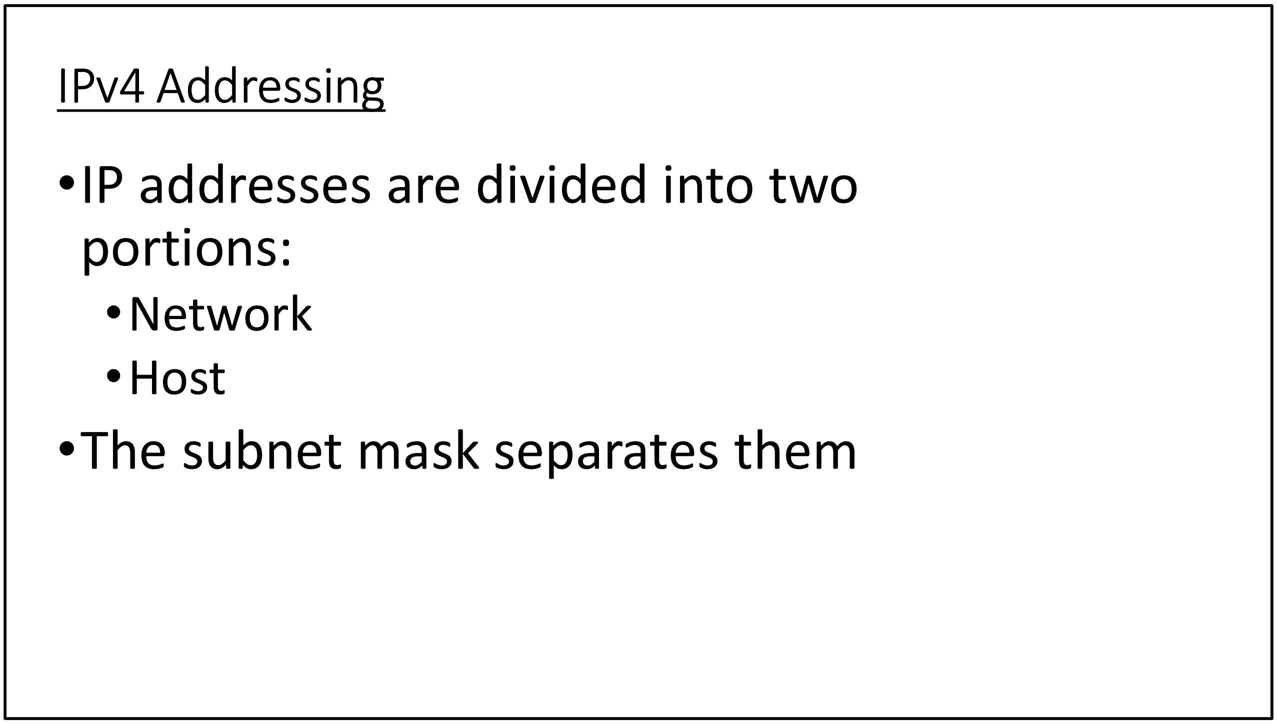
5.01 Network Components (Demo)

CH05: Cloud Networking



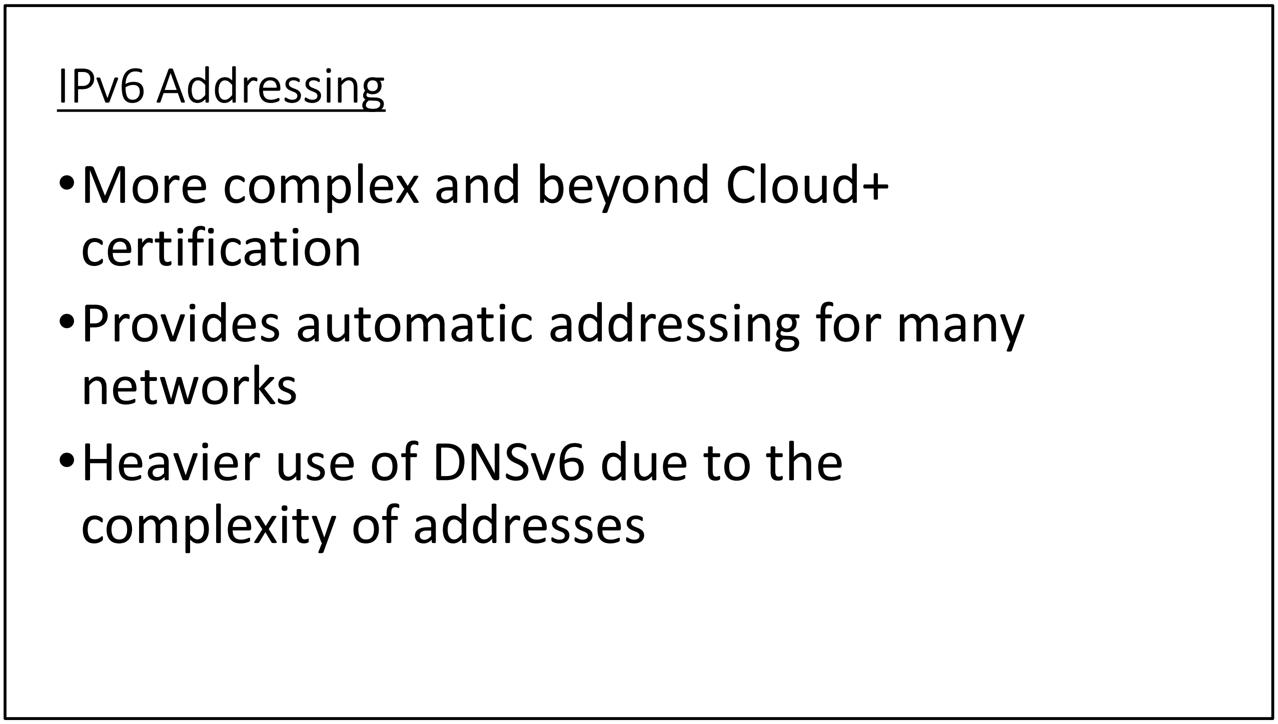
Internet Protocol (IP)

- IP is the protocol of the Internet and of the cloud
- IPv4
  - Still the most widely used
  - A 32-bit (32 1s and 0s) address space
- IPv6
  - A 128-bit address space
  - Hexadecimal notation
    - Ex. address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334



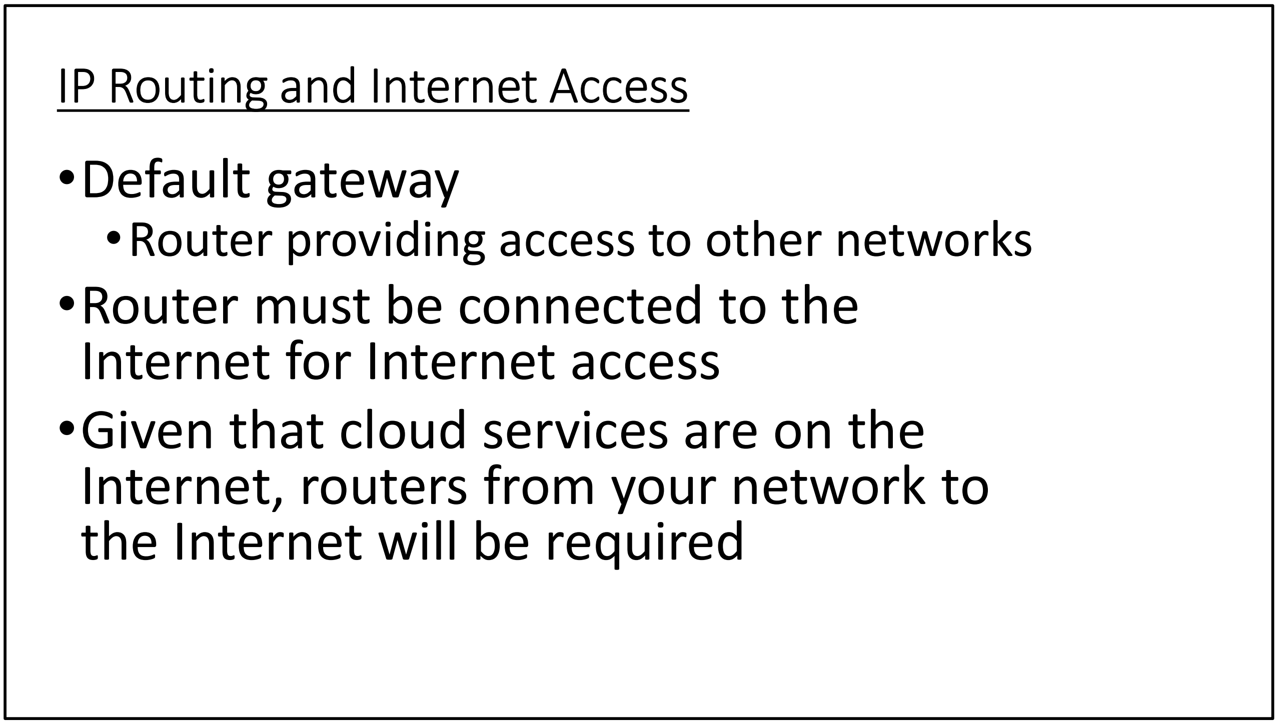
IPv4 Addressing

- IP addresses are divided into two portions:
  - Network
  - Host
- The subnet mask separates them



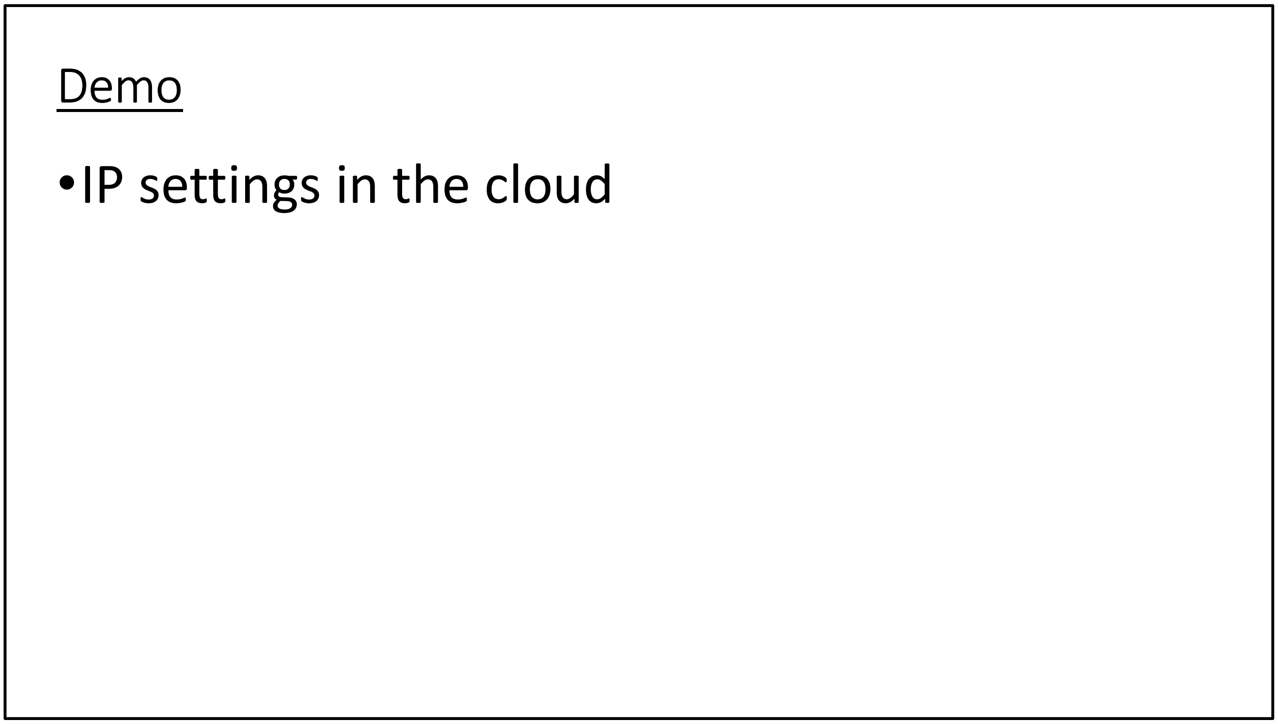
IPv6 Addressing

- More complex and beyond Cloud+ certification
- Provides automatic addressing for many networks
- Heavier use of DNSv6 due to the complexity of addresses



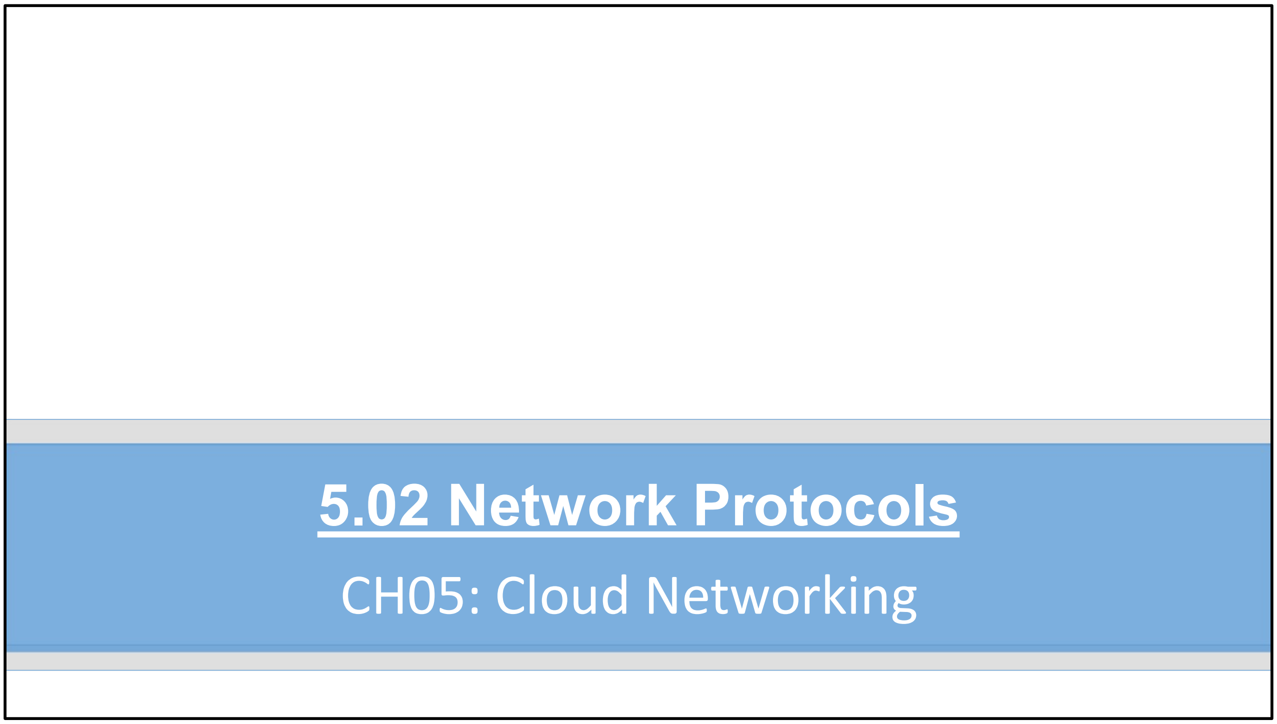
IP Routing and Internet Access

- Default gateway
  - Router providing access to other networks
- Router must be connected to the Internet for Internet access
- Given that cloud services are on the Internet, routers from your network to the Internet will be required



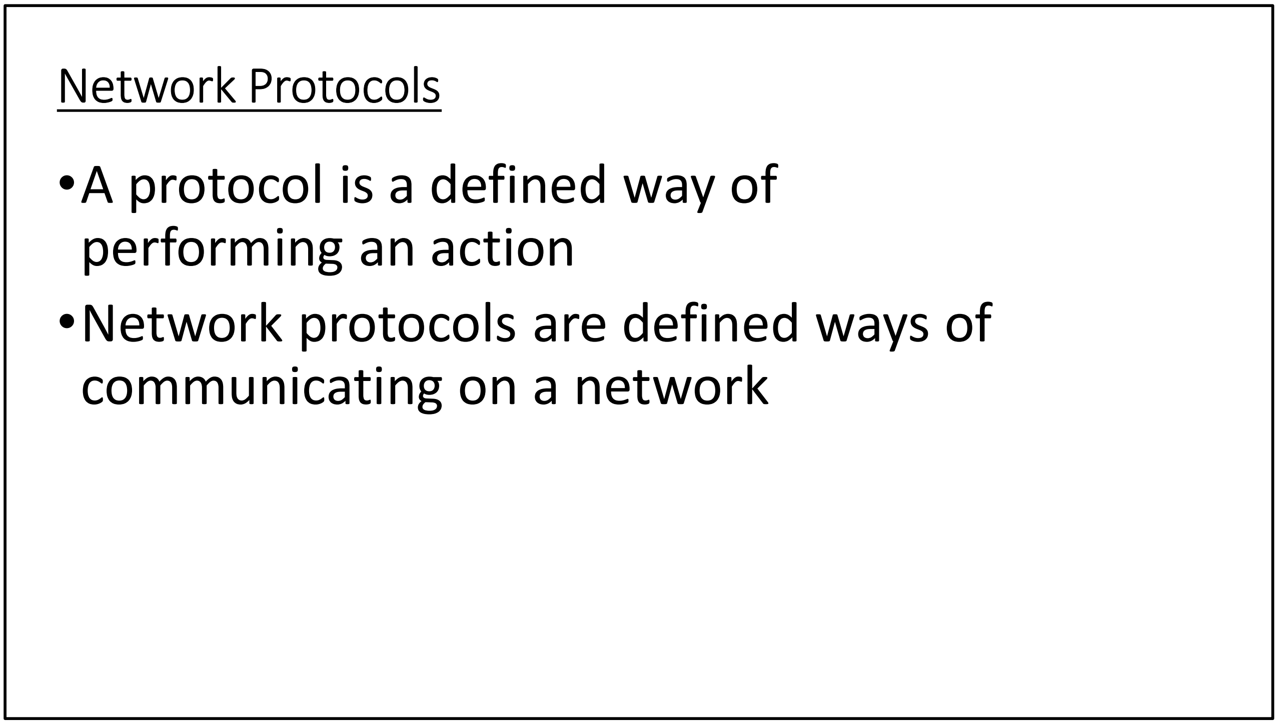
Demo

- IP settings in the cloud



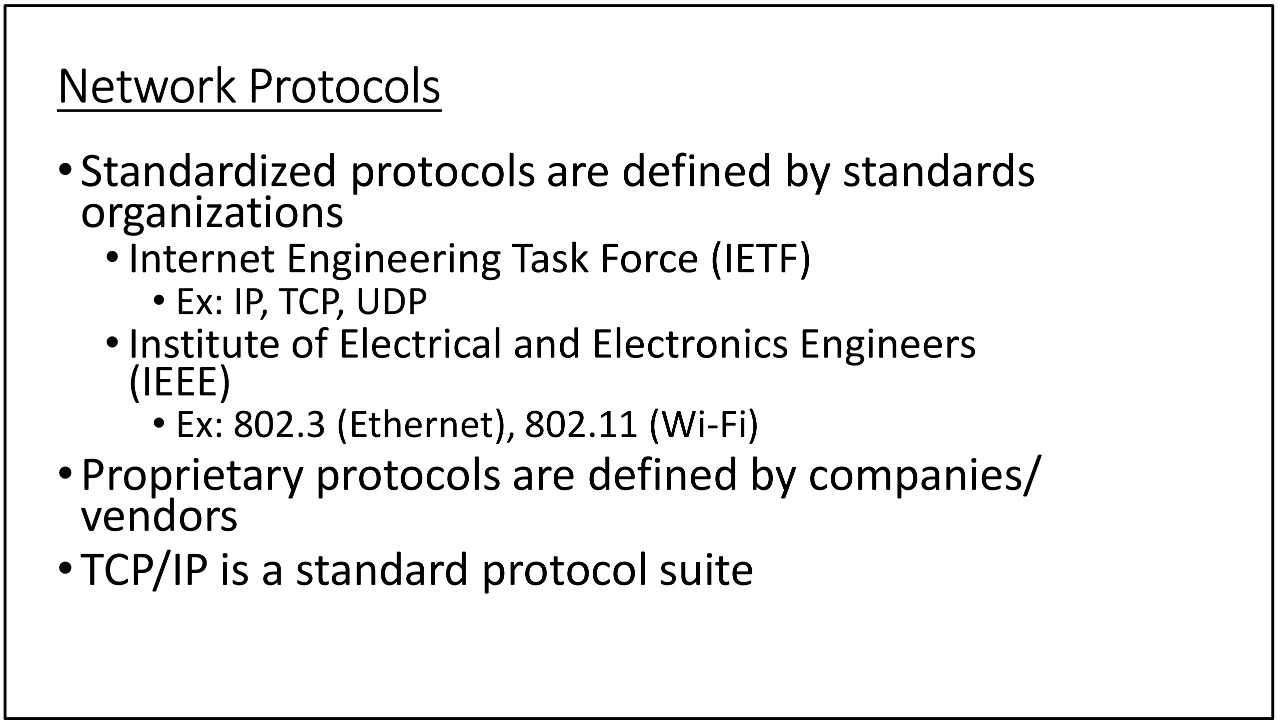
5.02 Network Protocols

CH05: Cloud Networking



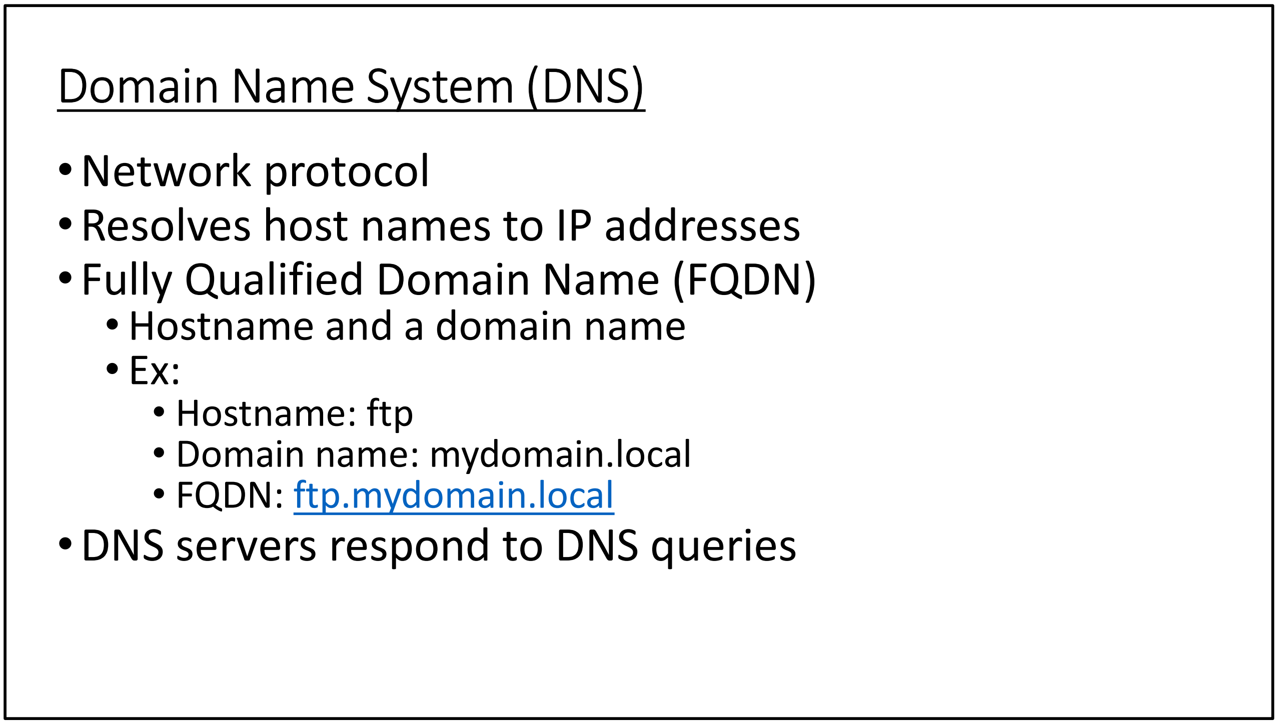
Network Protocols

- A protocol is a defined way of performing an action
- Network protocols are defined ways of communicating on a network



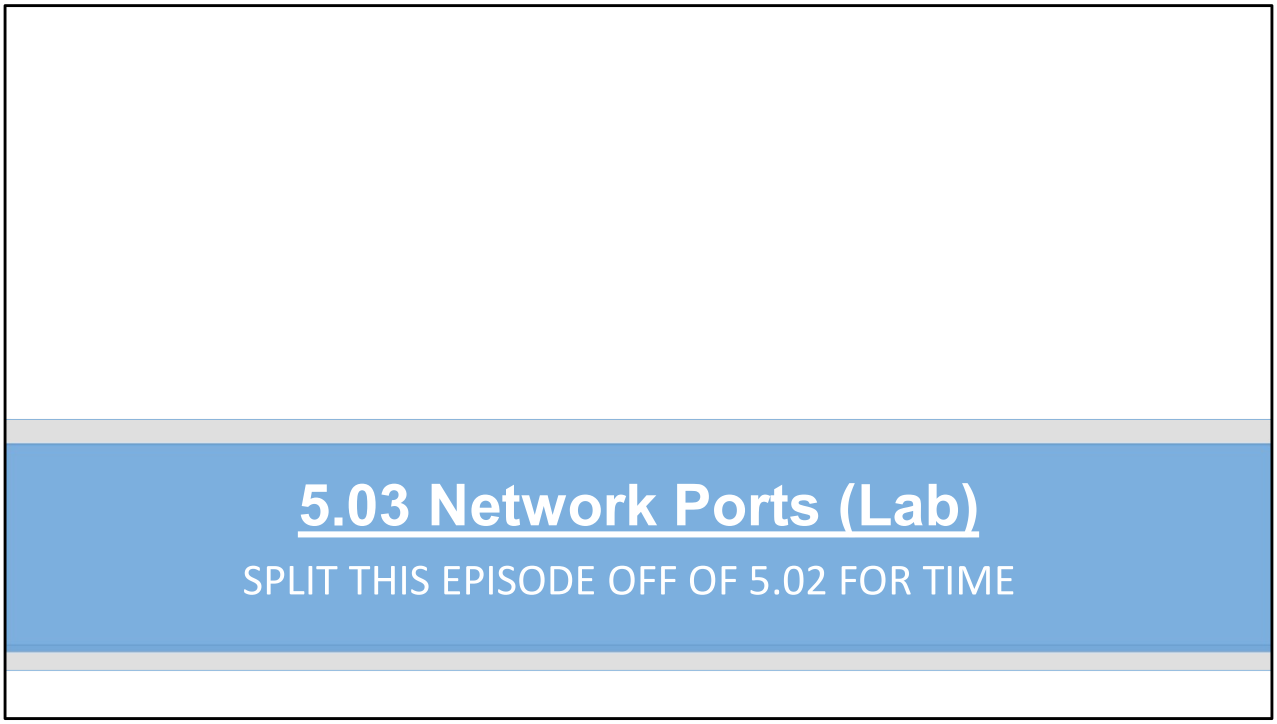
Network Protocols

- Standardized protocols are defined by standards organizations
  - Internet Engineering Task Force (IETF)
    - Ex: IP, TCP, UDP
  - Institute of Electrical and Electronics Engineers (IEEE)
    - Ex: 802.3 (Ethernet), 802.11 (Wi-Fi)
- Proprietary protocols are defined by companies/ vendors
- TCP/IP is a standard protocol suite



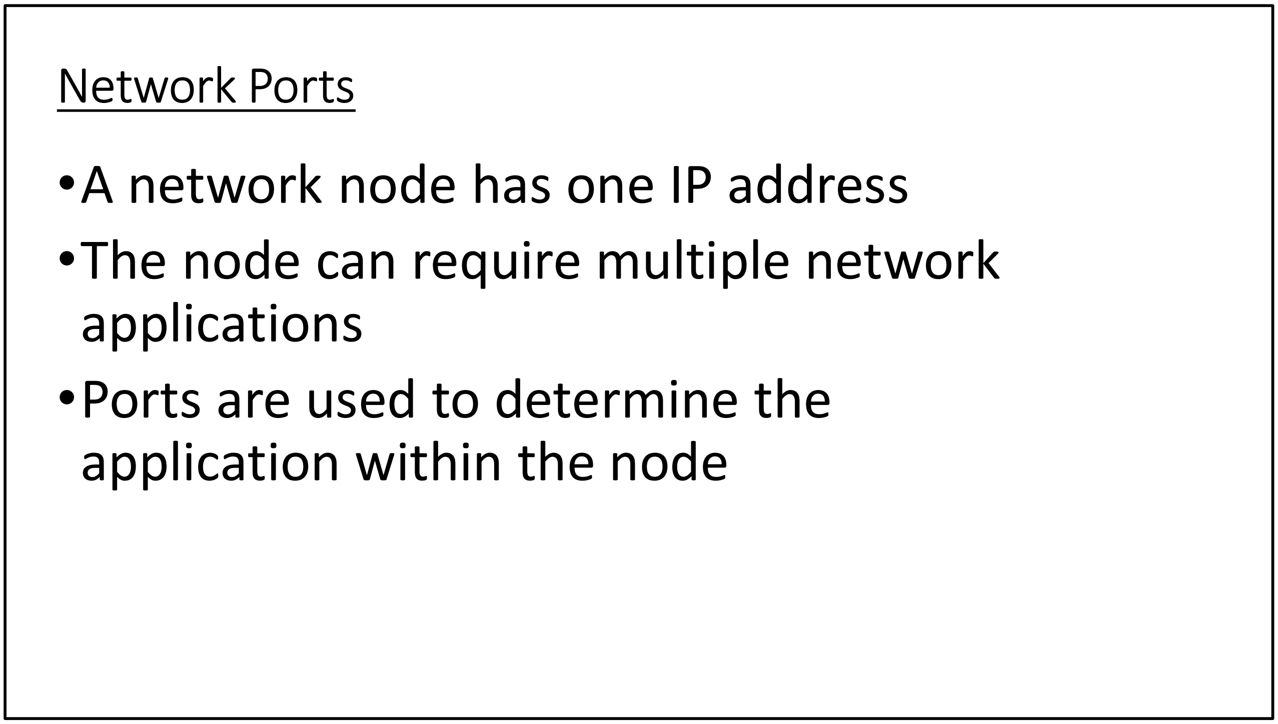
Domain Name System (DNS)

- Network protocol
- Resolves host names to IP addresses
- Fully Qualified Domain Name (FQDN)
  - Hostname and a domain name
  - Ex:
    - Hostname: ftp
    - Domain name: mydomain.local
    - FQDN: ftp.mydomain.local
- DNS servers respond to DNS queries



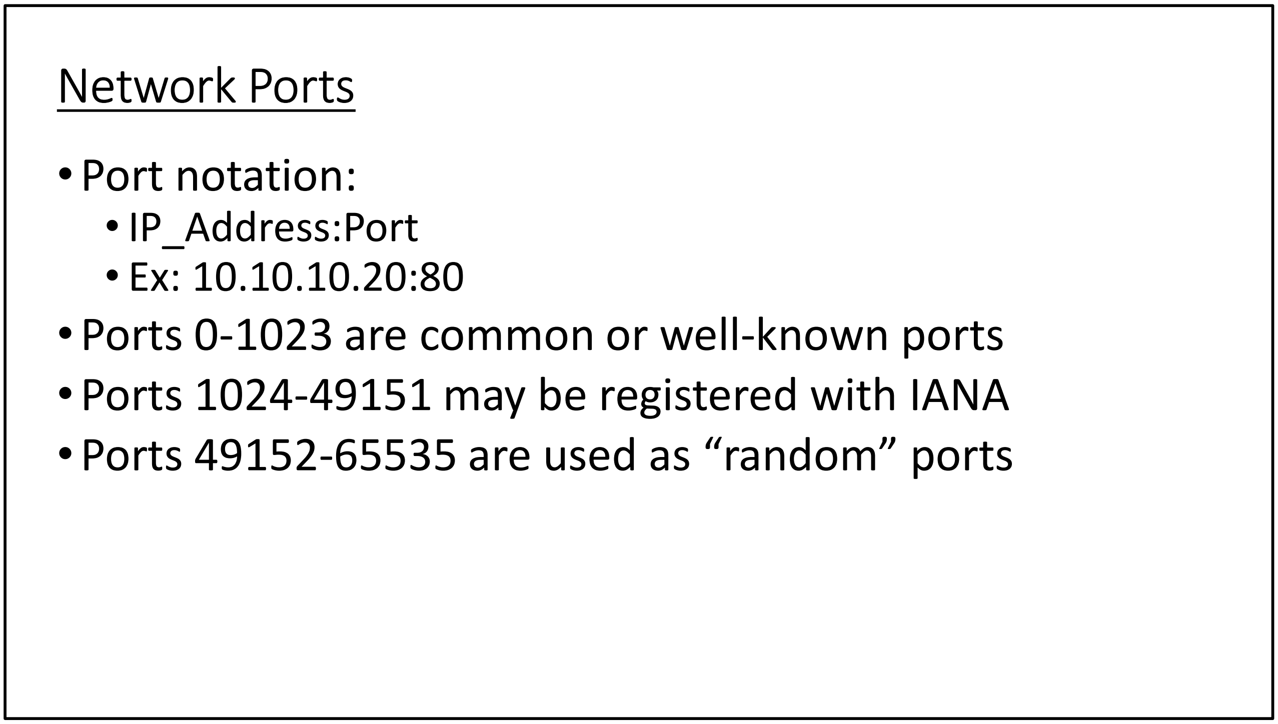
5.03 Network Ports (Lab)

SPLIT THIS EPISODE OFF OF 5.02 FOR TIME



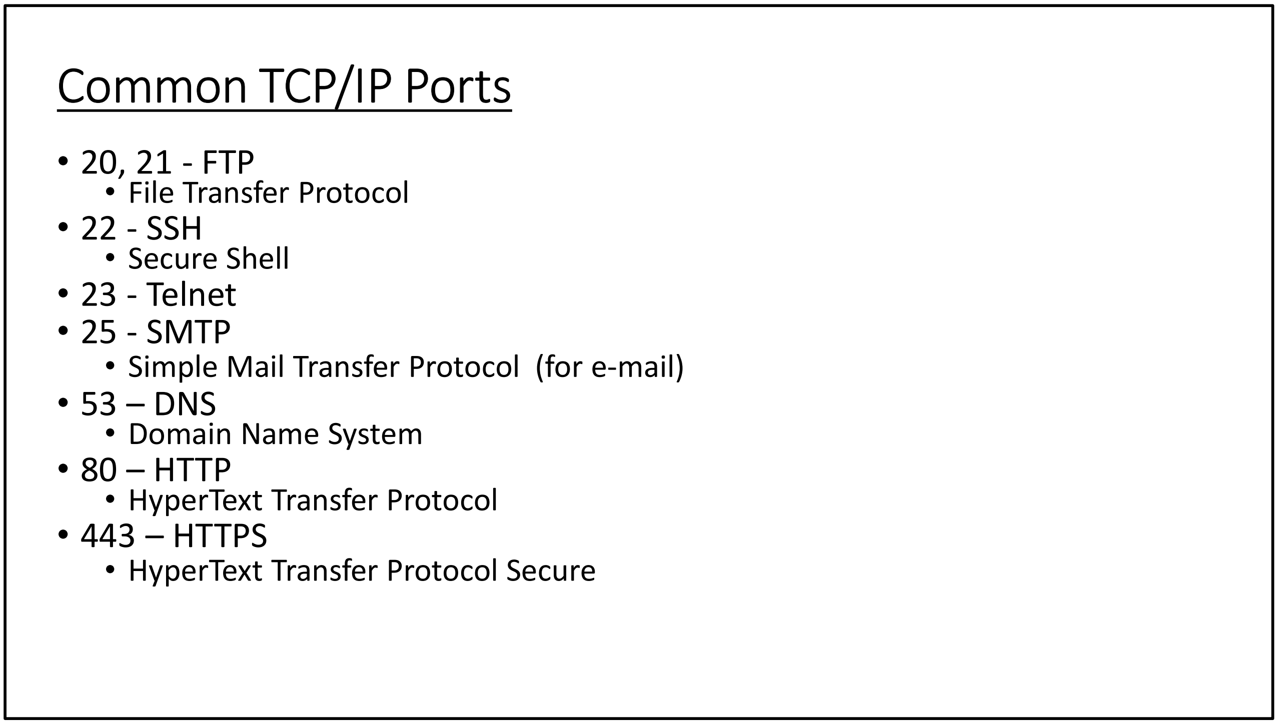
Network Ports

- A network node has one IP address
- The node can require multiple network applications
- Ports are used to determine the application within the node



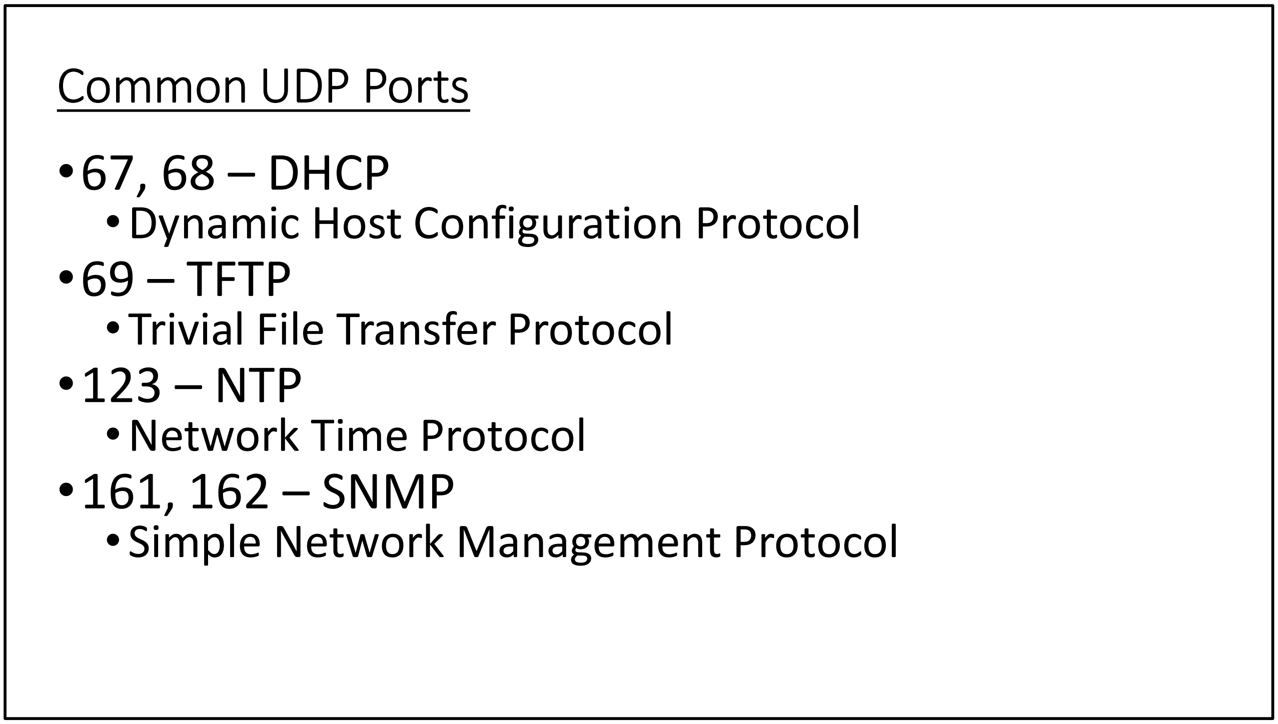
Network Ports

- Port notation:
  - IP_Address:Port
  - Ex: 10.10.10.20:80
- Ports 0-1023 are common or well-known ports
- Ports 1024-49151 may be registered with IANA
- Ports 49152-65535 are used as “random” ports



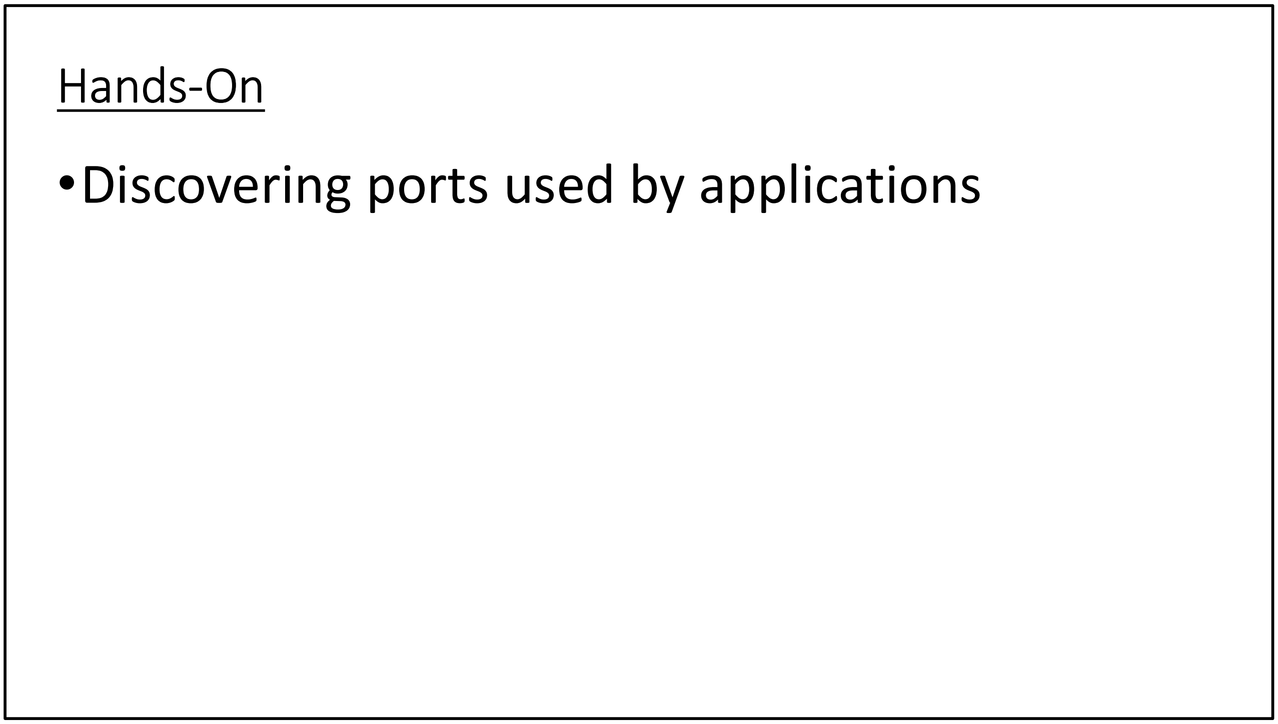
Common TCP/IP Ports

- 20, 21 - FTP
  - File Transfer Protocol
- 22 - SSH
  - Secure Shell
- 23 - Telnet
- 25 - SMTP
  - Simple Mail Transfer Protocol (for e-mail)
- 53 – DNS
  - Domain Name System
- 80 – HTTP
  - HyperText Transfer Protocol
- 443 – HTTPS
  - HyperText Transfer Protocol Secure



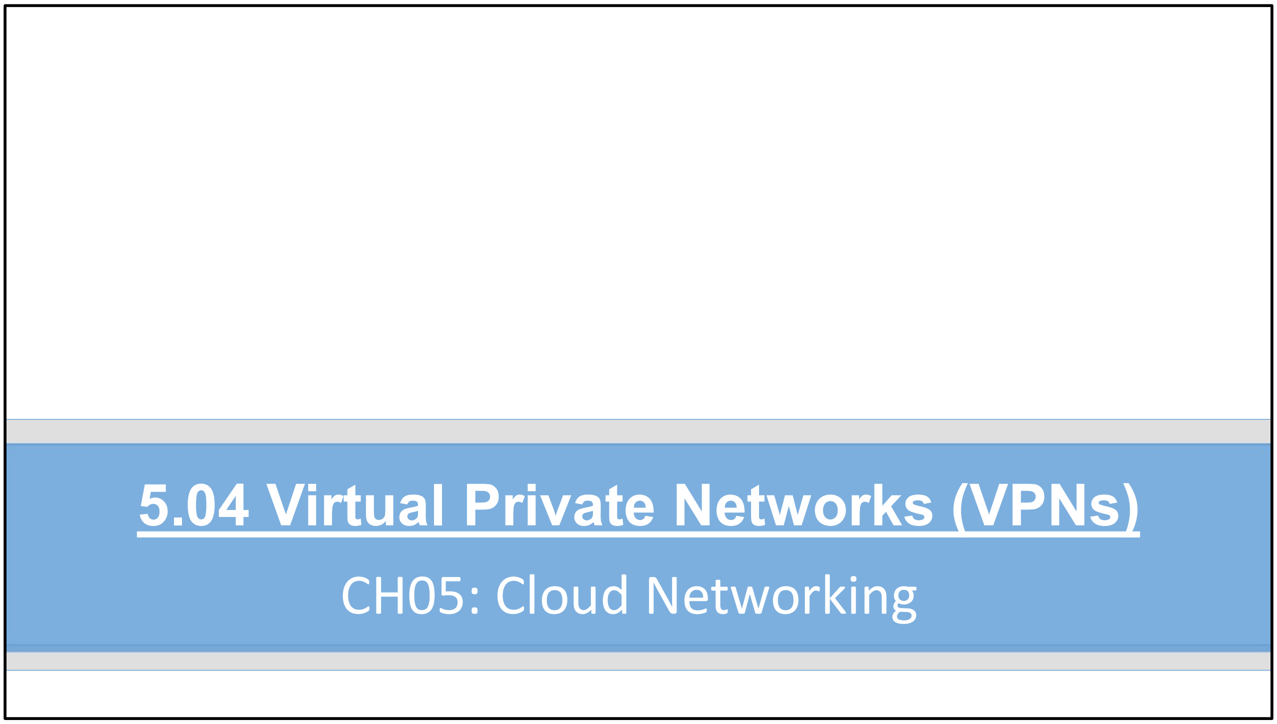
Common UDP Ports

- 67, 68 – DHCP
  - Dynamic Host Configuration Protocol
- 69 – TFTP
  - Trivial File Transfer Protocol
- 123 – NTP
  - Network Time Protocol
- 161, 162 – SNMP
  - Simple Network Management Protocol



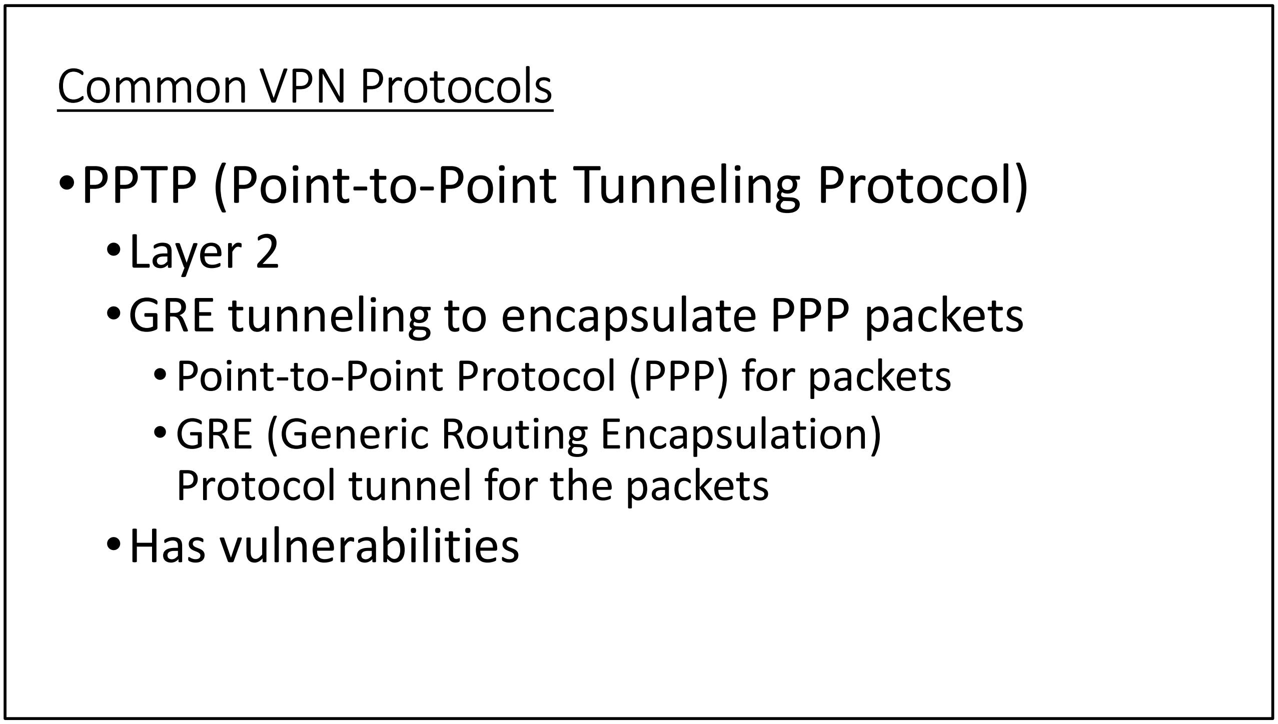
Hands-On

- Discovering ports used by applications



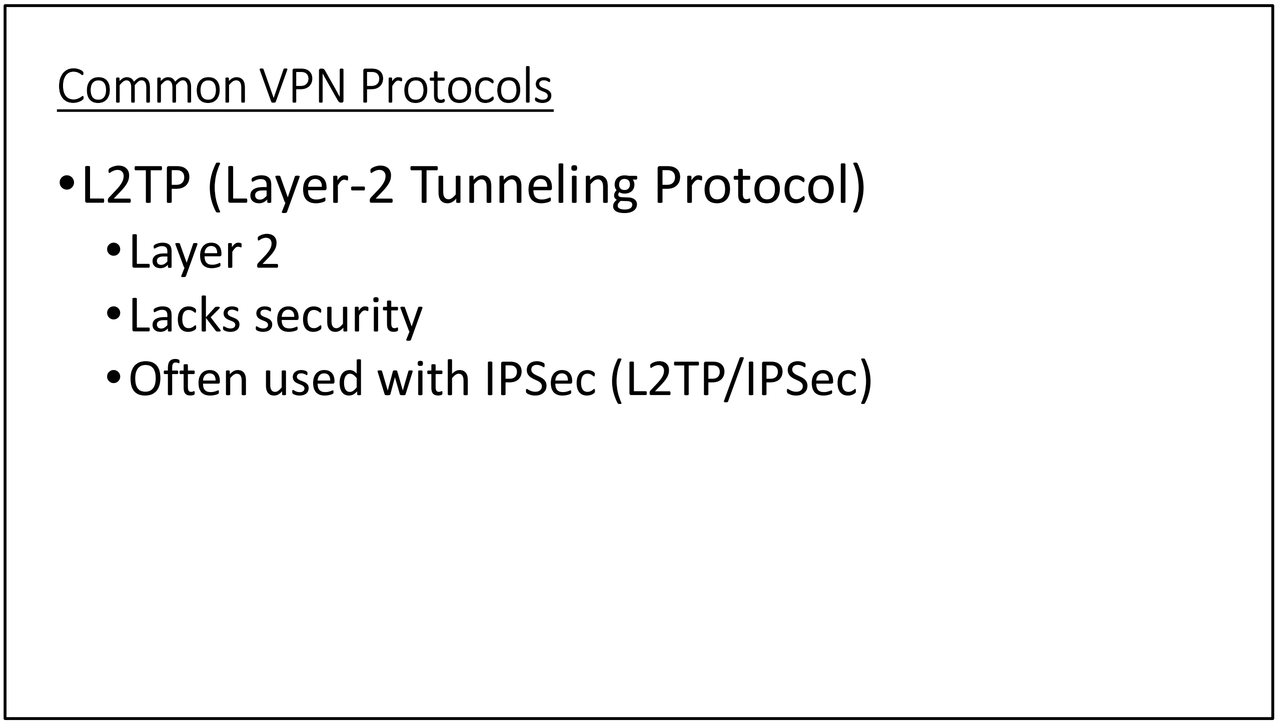
5.04 Virtual Private Networks (VPNs)

CH05: Cloud Networking



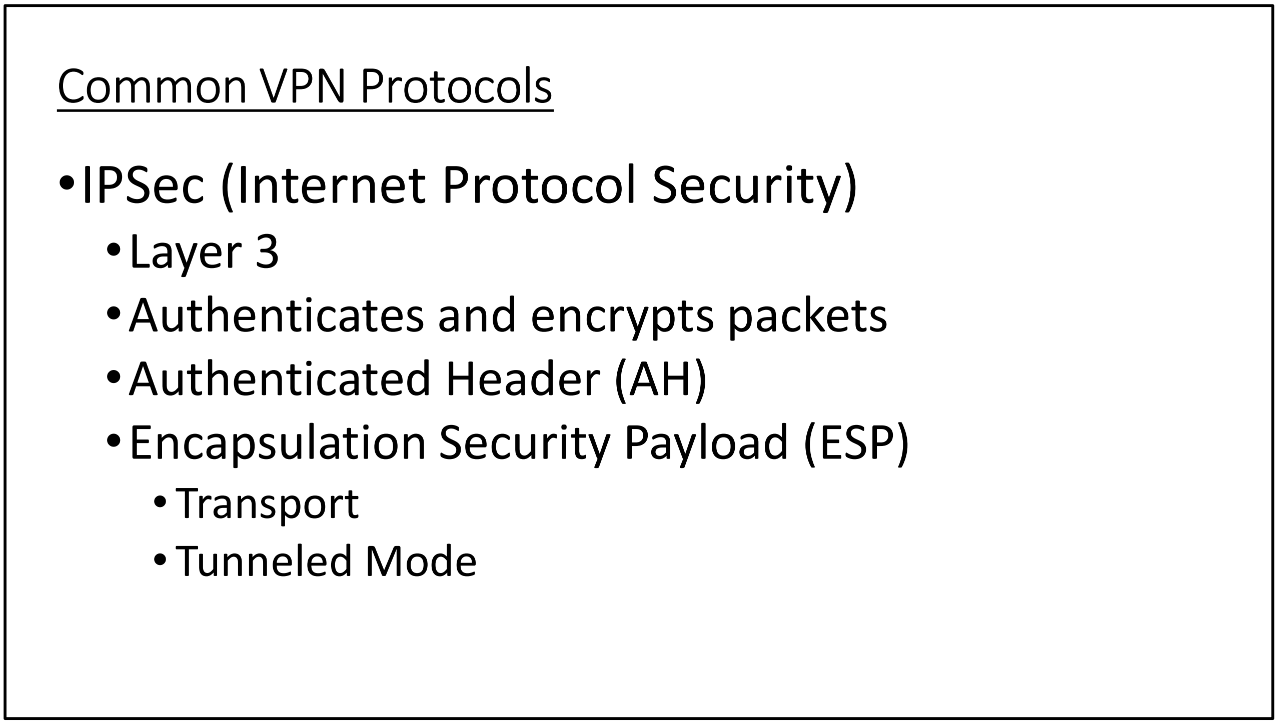
Common VPN Protocols

- PPTP (Point-to-Point Tunneling Protocol)
  - Layer 2
  - GRE tunneling to encapsulate PPP packets
    - Point-to-Point Protocol (PPP) for packets
    - GRE (Generic Routing Encapsulation) Protocol tunnel for the packets
  - Has vulnerabilities



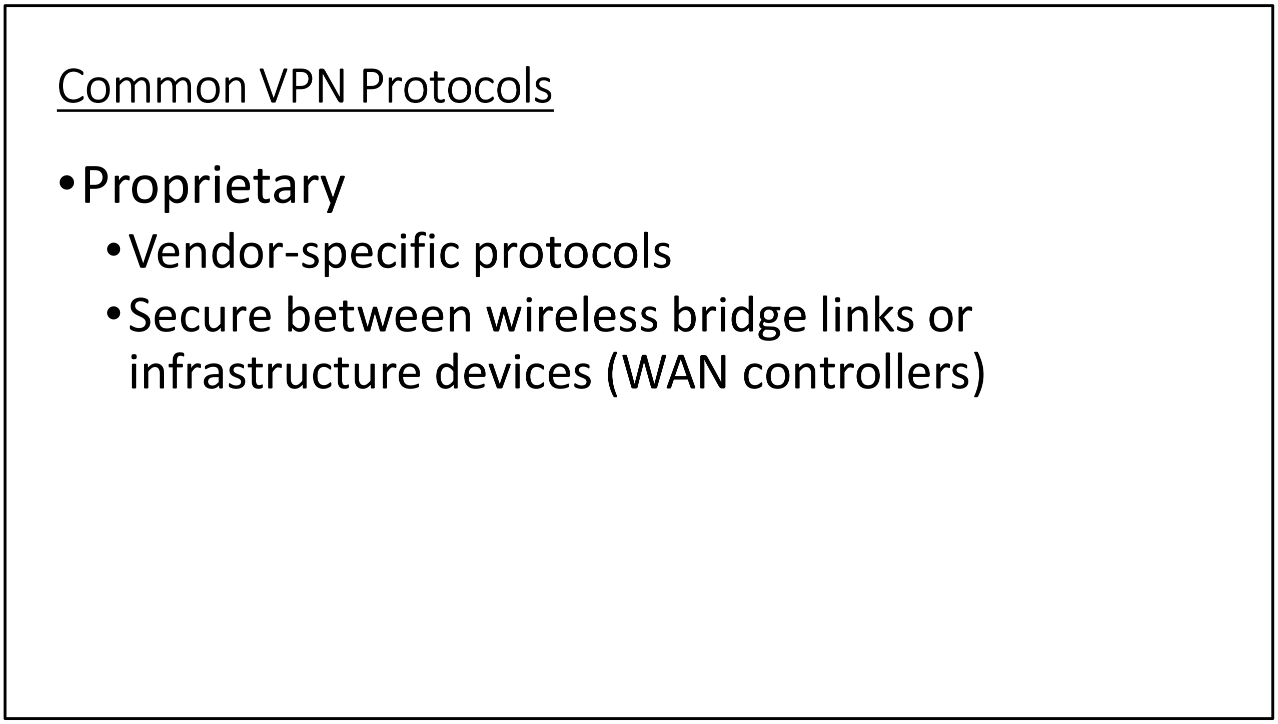
Common VPN Protocols

- L2TP (Layer-2 Tunneling Protocol)
  - Layer 2
  - Lacks security
  - Often used with IPSec (L2TP/IPSec)



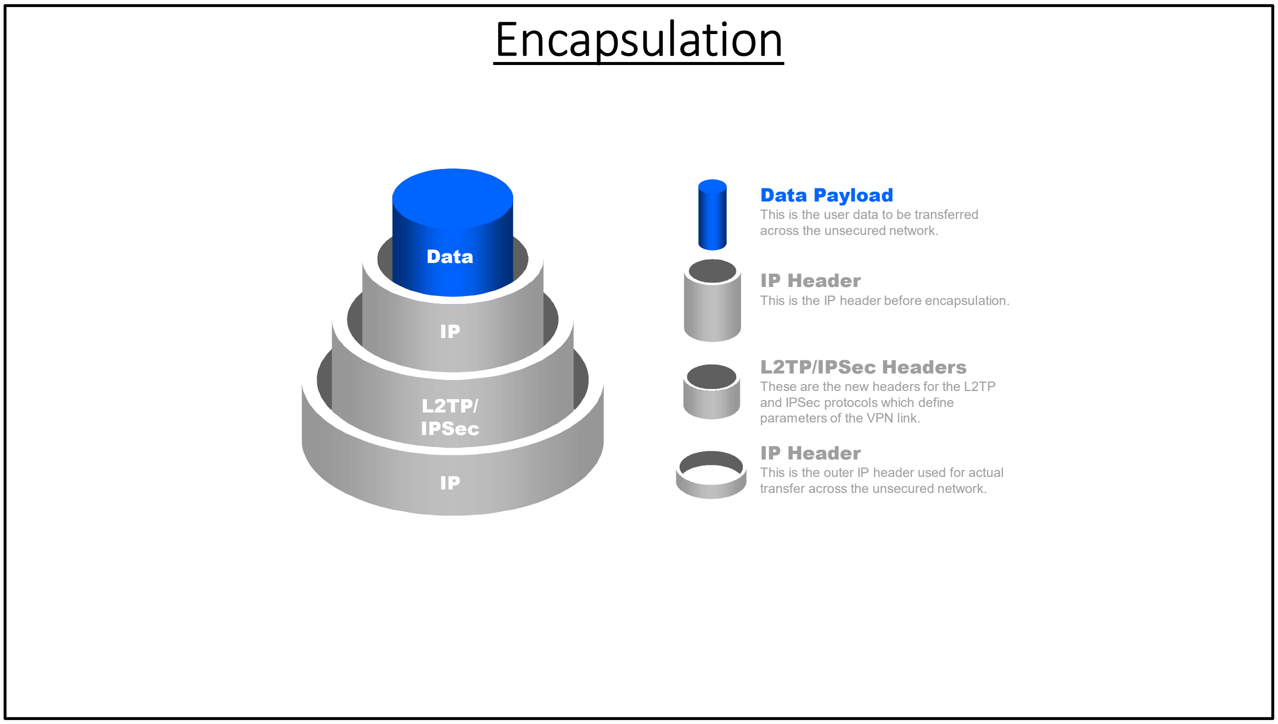
Common VPN Protocols

- IPSec (Internet Protocol Security)
  - Layer 3
  - Authenticates and encrypts packets
  - Authenticated Header (AH)
  - Encapsulation Security Payload (ESP)
    - Transport
    - Tunneled Mode



Common VPN Protocols

- Proprietary
  - Vendor-specific protocols
  - Secure between wireless bridge links or infrastructure devices (WAN controllers)



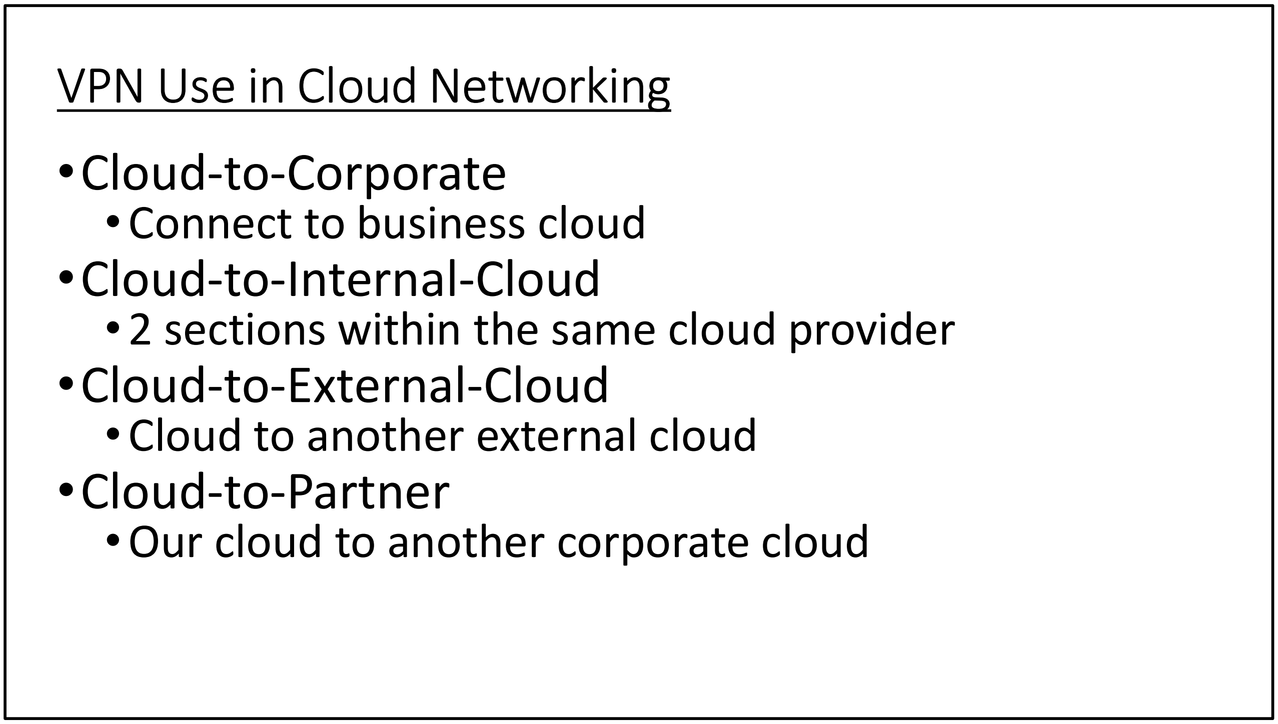
Encapsulation

Data Payload
This is the user data to be transferred across the unsecured network.

IP Header
This is the IP header before encapsulation.

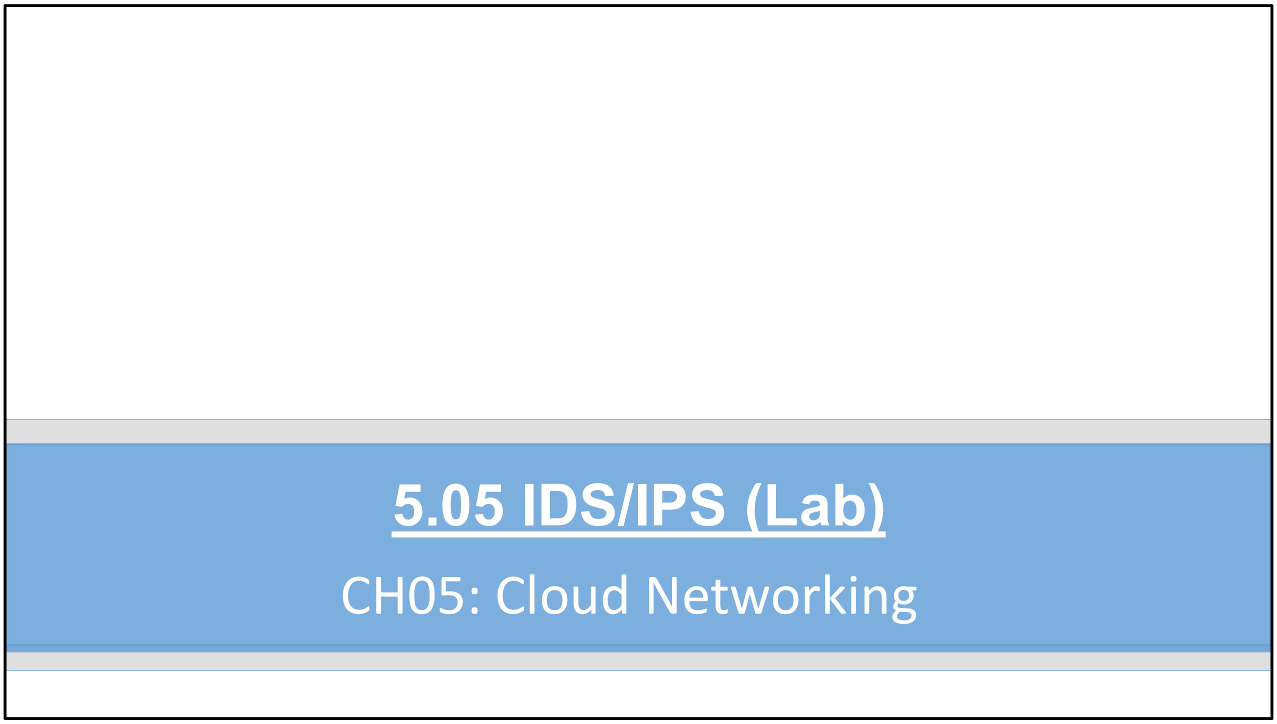
L2TP/IPSec Headers
These are the new headers for the L2TP and IPSec protocols which define parameters of the VPN link.

IP Header
This is the outer IP header used for actual transfer across the unsecured network.



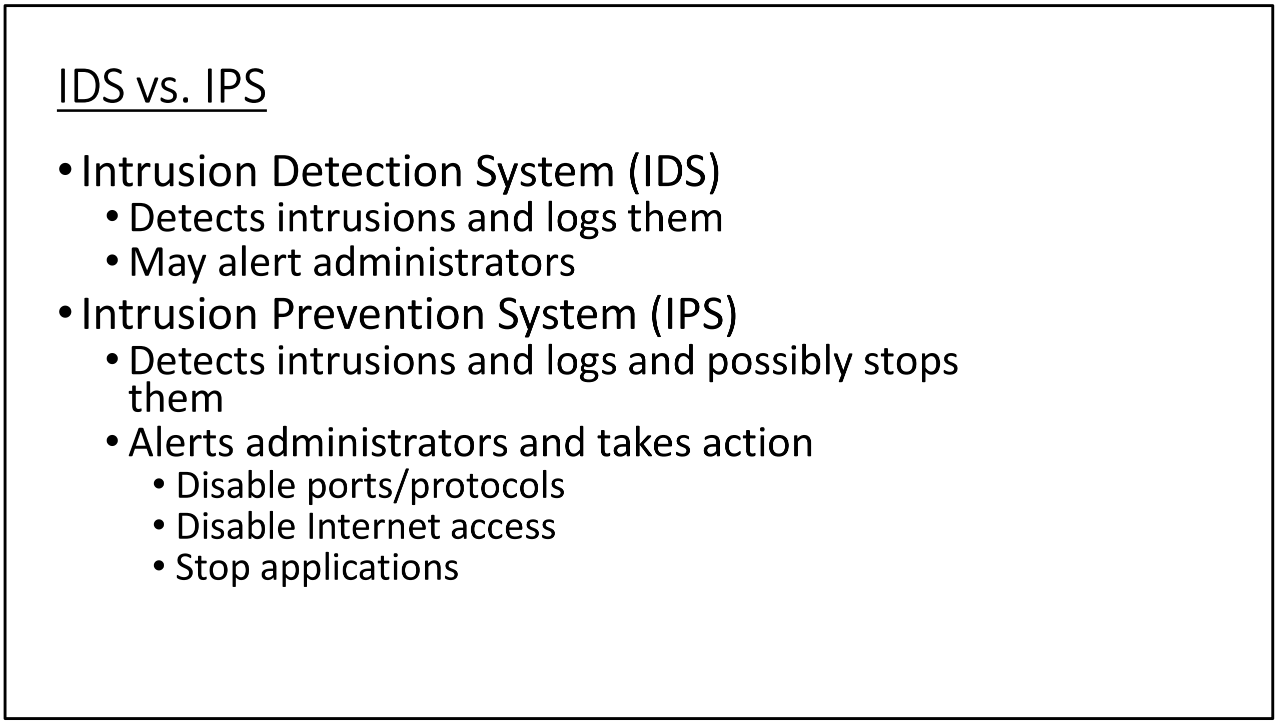
VPN Use in Cloud Networking

- Cloud-to-Corporate
  - Connect to business cloud
- Cloud-to-Internal-Cloud
  - 2 sections within the same cloud provider
- Cloud-to-External-Cloud
  - Cloud to another external cloud
- Cloud-to-Partner
  - Our cloud to another corporate cloud



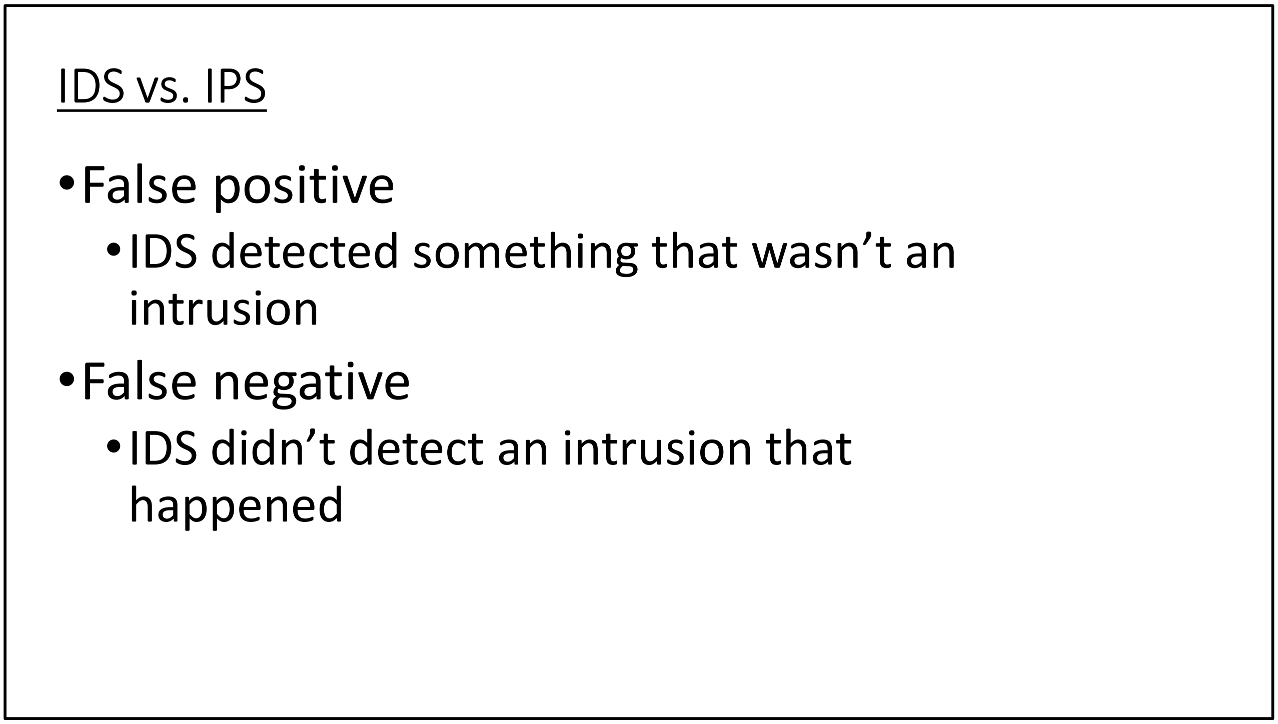
5.05 IDS/IPS (Lab)

CH05: Cloud Networking



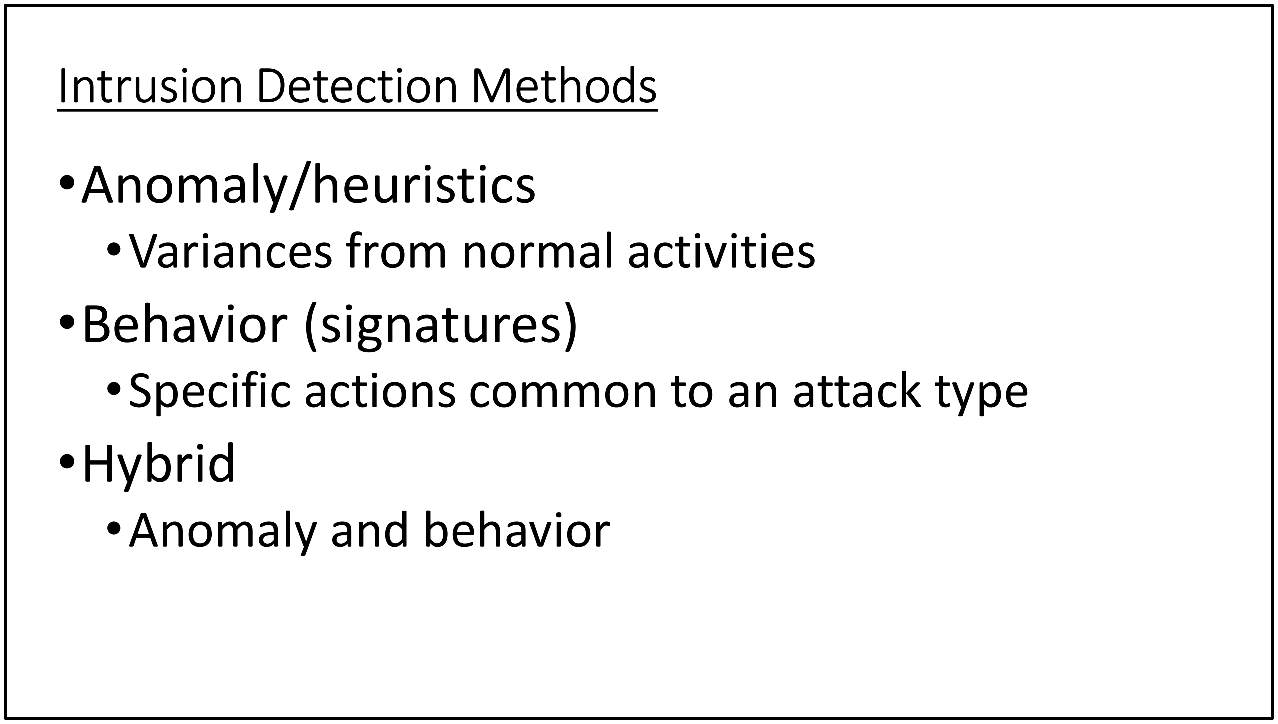
IDS vs. IPS

- Intrusion Detection System (IDS)
  - Detects intrusions and logs them
  - May alert administrators
- Intrusion Prevention System (IPS)
  - Detects intrusions and logs and possibly stops them
  - Alerts administrators and takes action
    - Disable ports/protocols
    - Disable Internet access
    - Stop applications



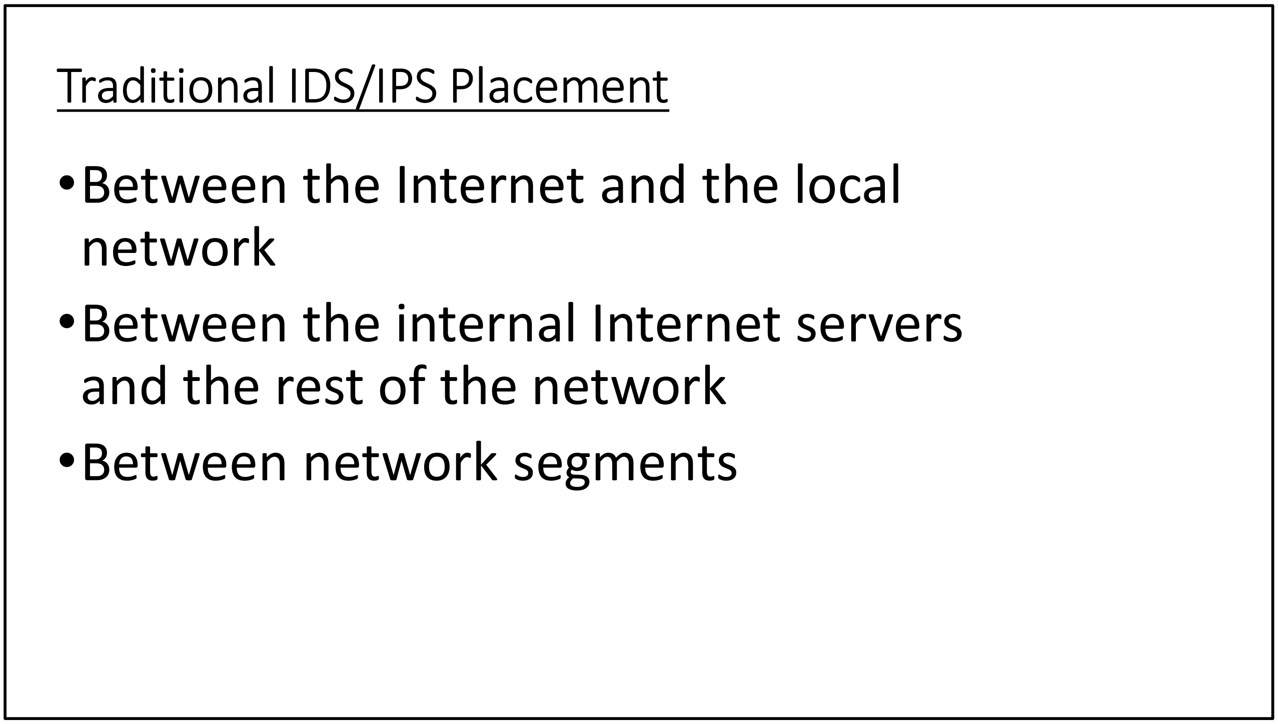
IDS vs. IPS

- False positive
  - IDS detected something that wasn’t an intrusion
- False negative
  - IDS didn’t detect an intrusion that happened



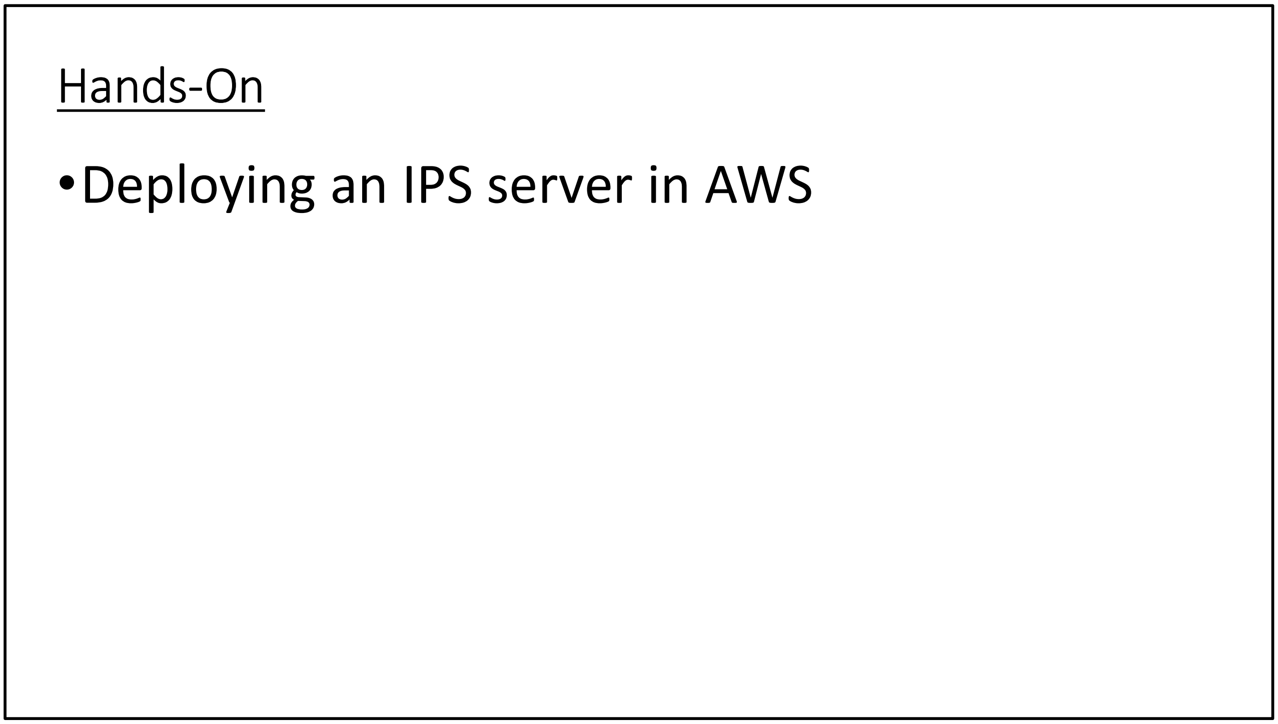
Intrusion Detection Methods

- Anomaly/heuristics
  - Variances from normal activities
- Behavior (signatures)
  - Specific actions common to an attack type
- Hybrid
  - Anomaly and behavior



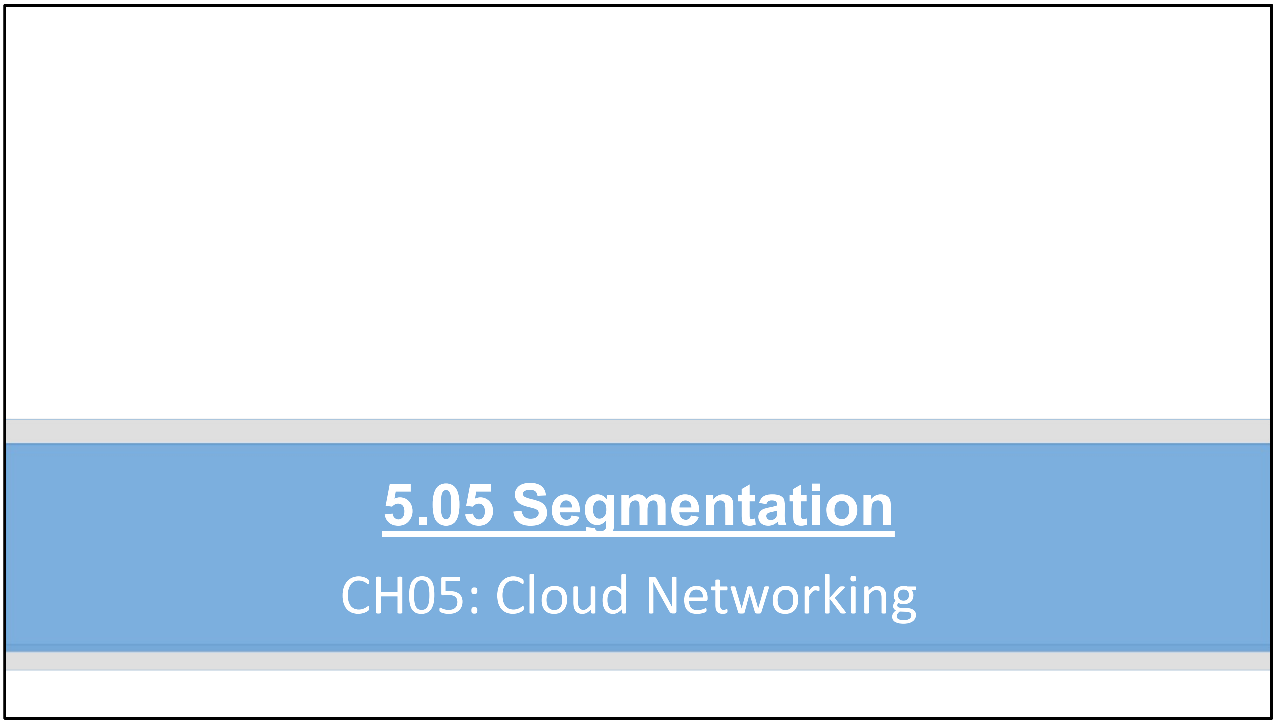
Traditional IDS/IPS Placement

- Between the Internet and the local network
- Between the internal Internet servers and the rest of the network
- Between network segments



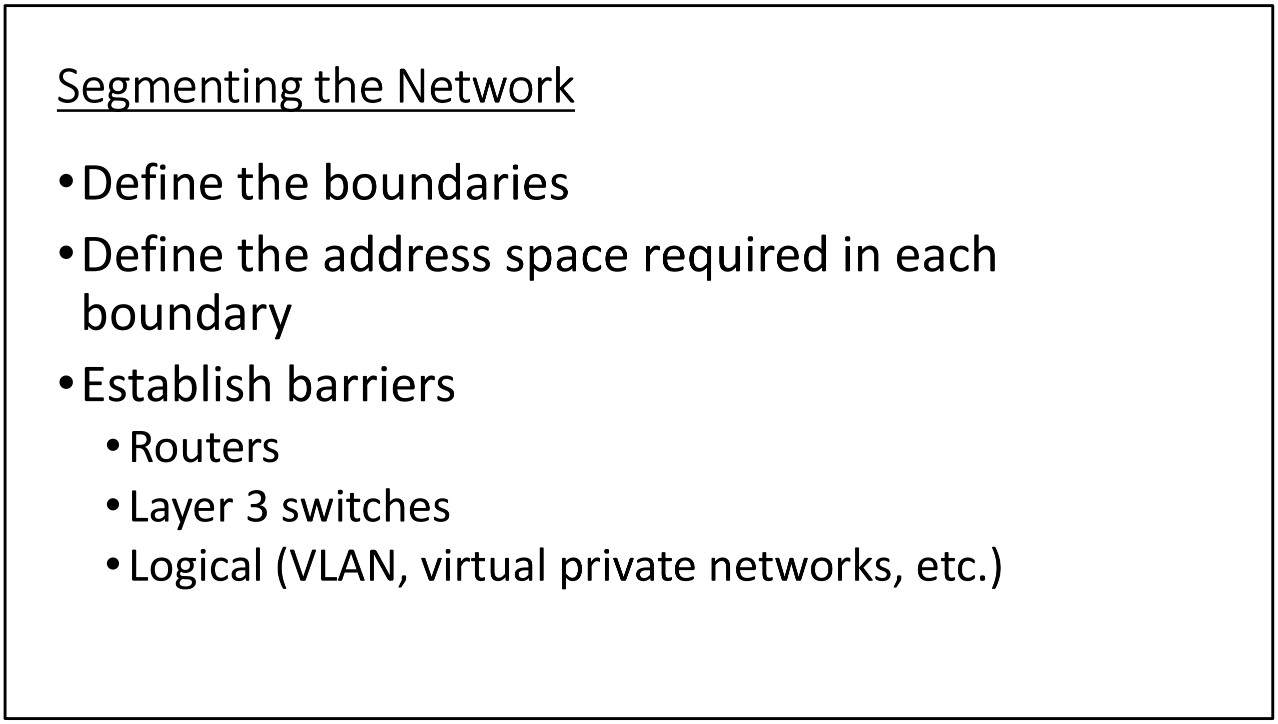
Hands-On

- Deploying an IPS server in AWS



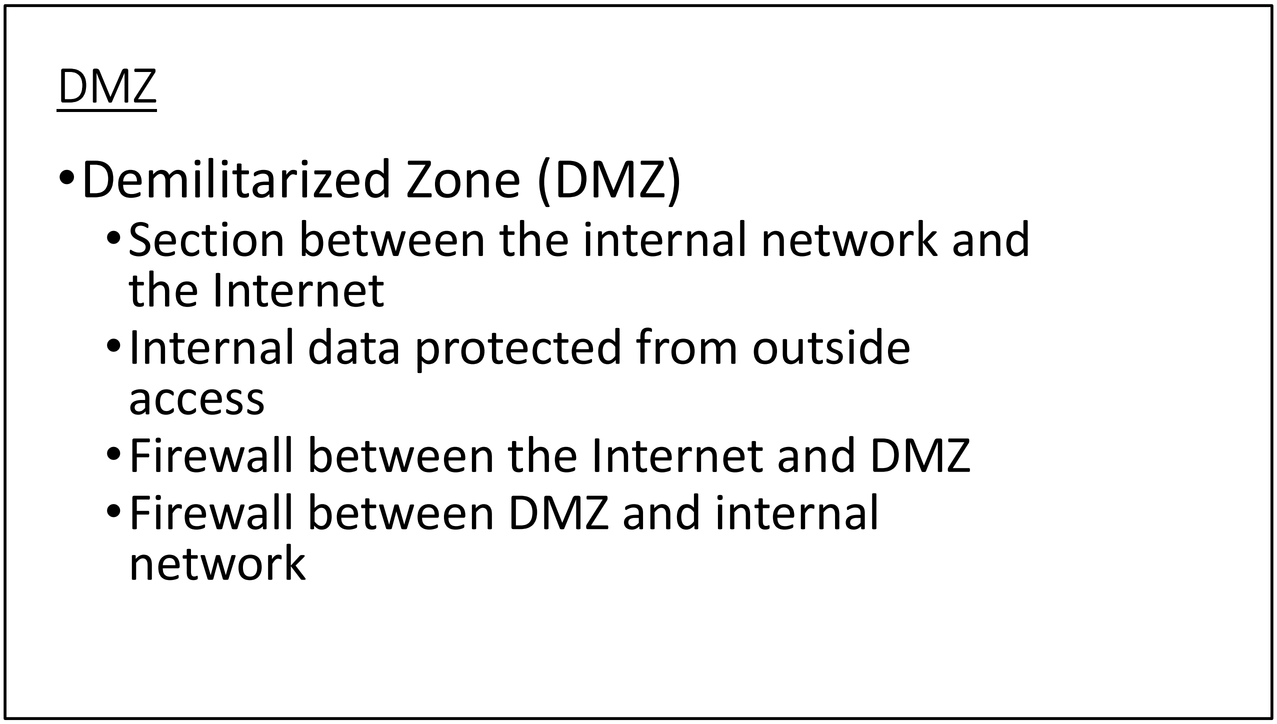
5.05 Segmentation

CH05: Cloud Networking



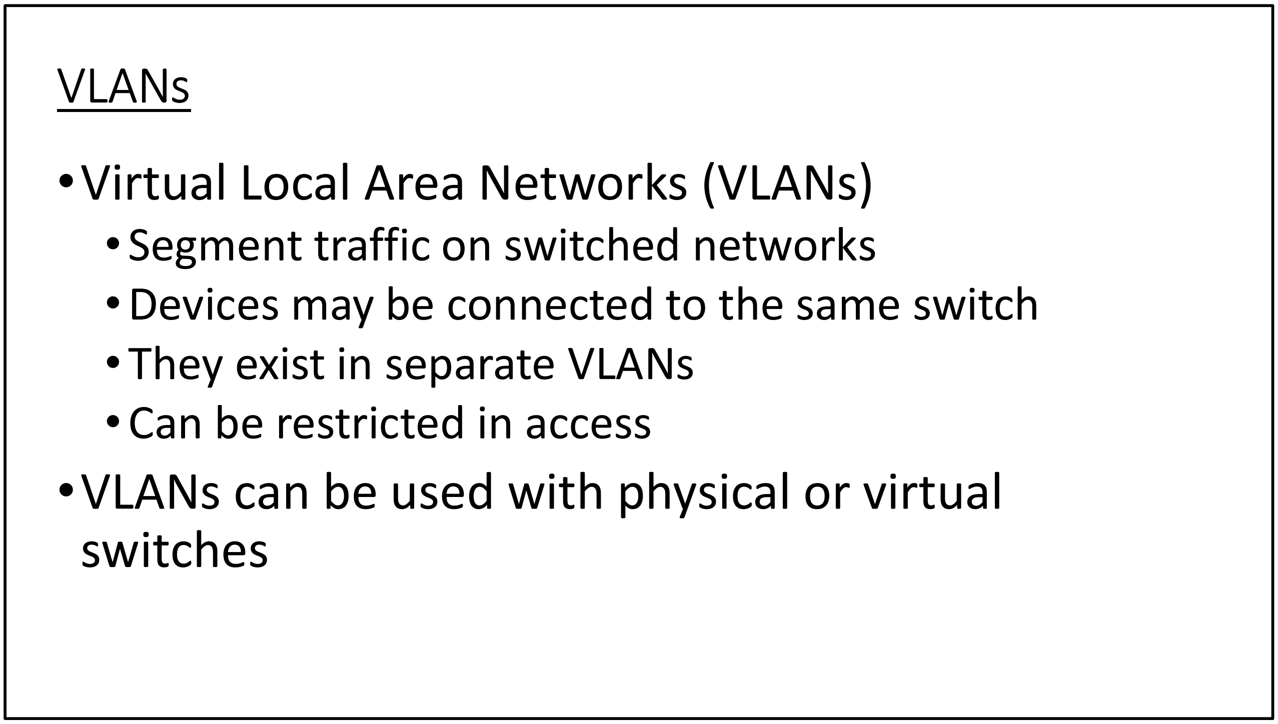
Segmenting the Network

- Define the boundaries
- Define the address space required in each boundary
- Establish barriers
  - Routers
  - Layer 3 switches
  - Logical (VLAN, virtual private networks, etc.)



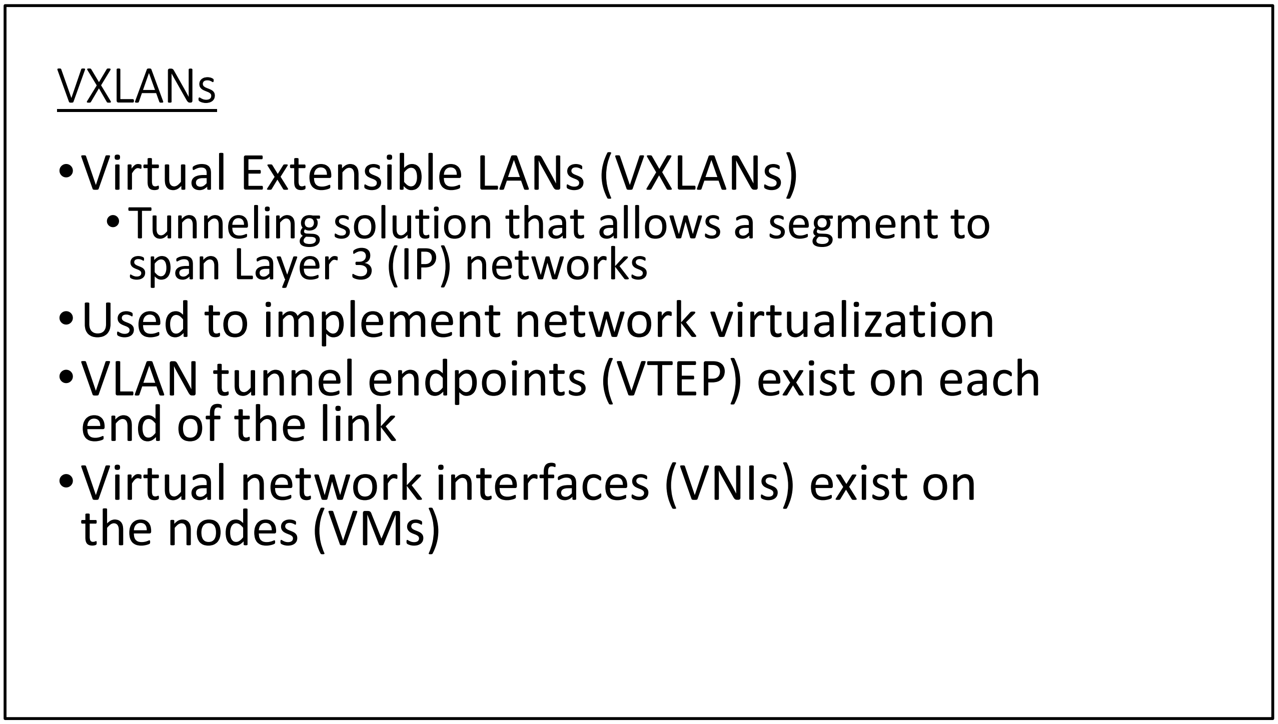
DMZ

- Demilitarized Zone (DMZ)
  - Section between the internal network and the Internet
  - Internal data protected from outside access
  - Firewall between the Internet and DMZ
  - Firewall between DMZ and internal network



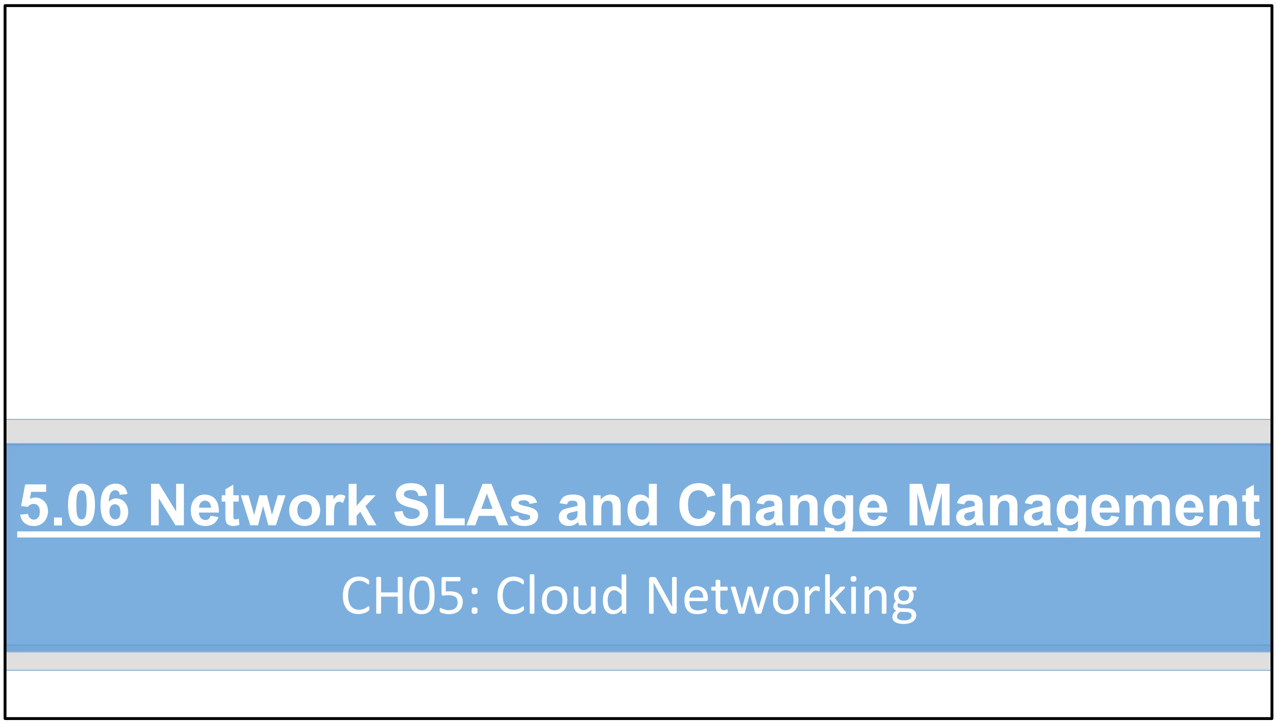
VLANs

- Virtual Local Area Networks (VLANs)
  - Segment traffic on switched networks
  - Devices may be connected to the same switch
  - They exist in separate VLANs
  - Can be restricted in access
- VLANs can be used with physical or virtual switches



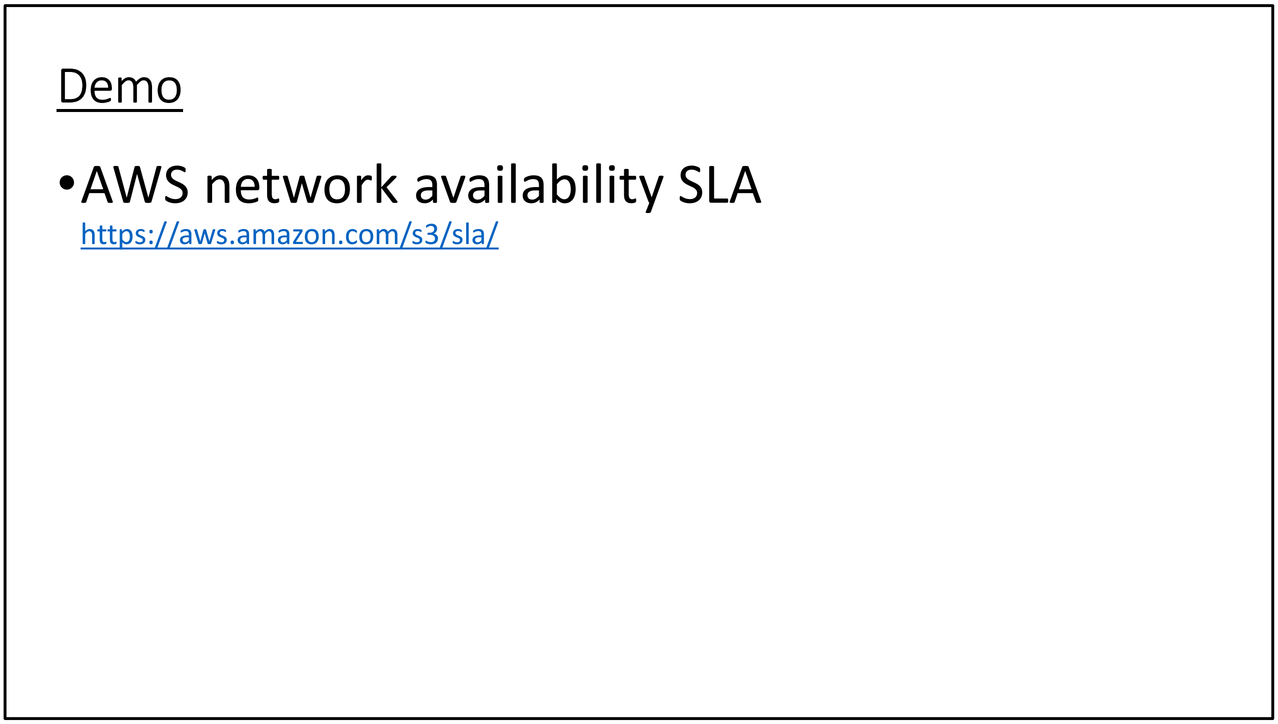
VXLANs

- Virtual Extensible LANs (VXLANs)
  - Tunneling solution that allows a segment to span Layer 3 (IP) networks
- Used to implement network virtualization
- VLAN tunnel endpoints (VTEP) exist on each end of the link
- Virtual network interfaces (VNIs) exist on the nodes (VMs)



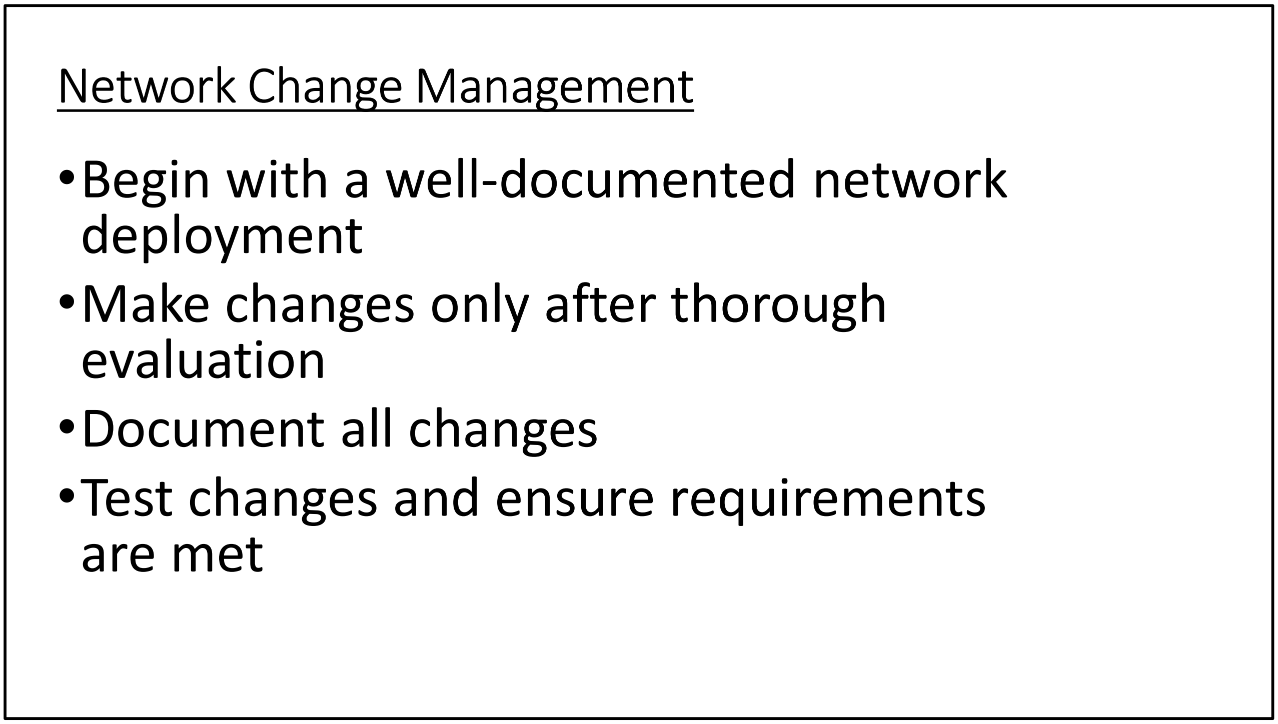
5.06 Network SLAs and Change Management

CH05: Cloud Networking



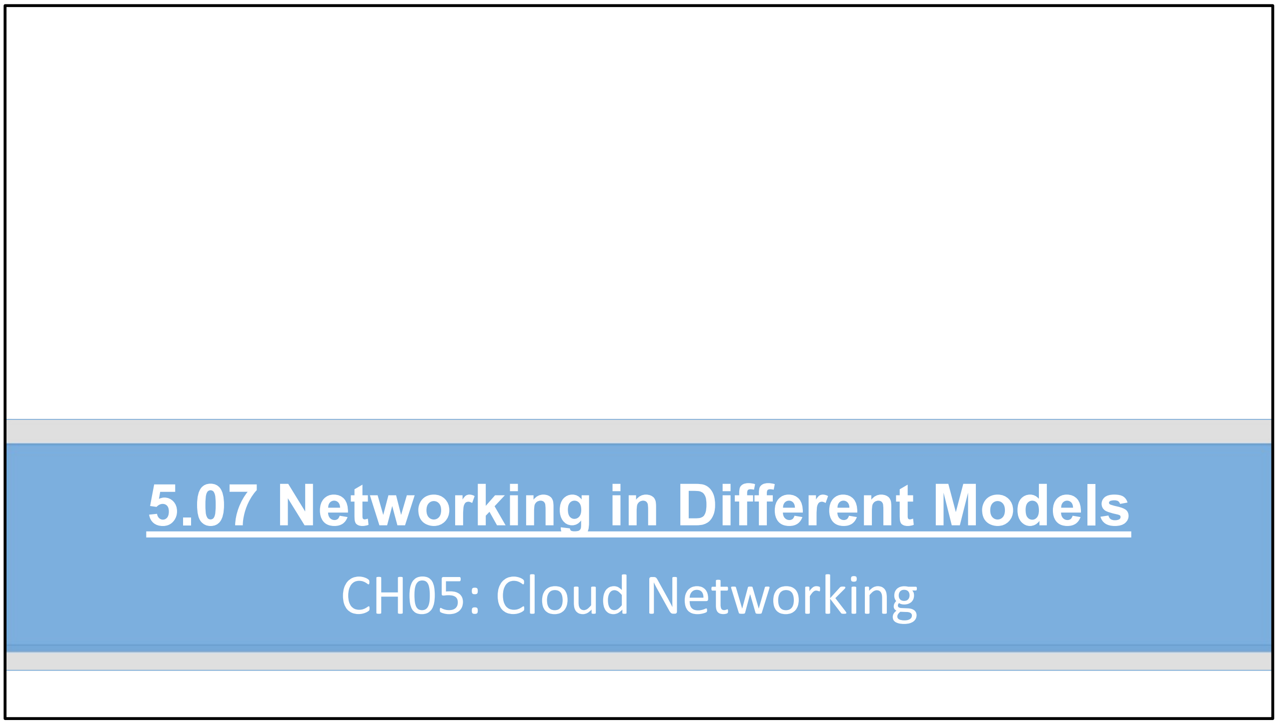
Demo

- AWS network availability SLA
  https://aws.amazon.com/s3/sla/



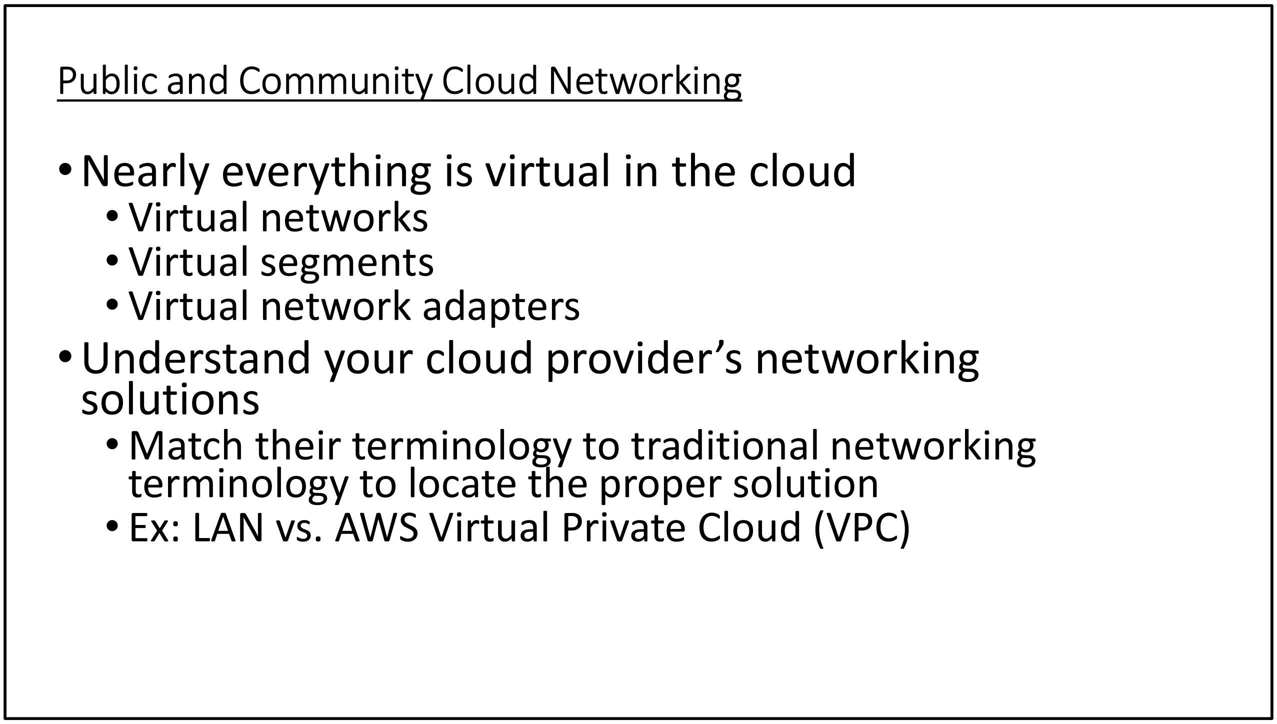
Network Change Management

- Begin with a well-documented network deployment
- Make changes only after thorough evaluation
- Document all changes
- Test changes and ensure requirements are met



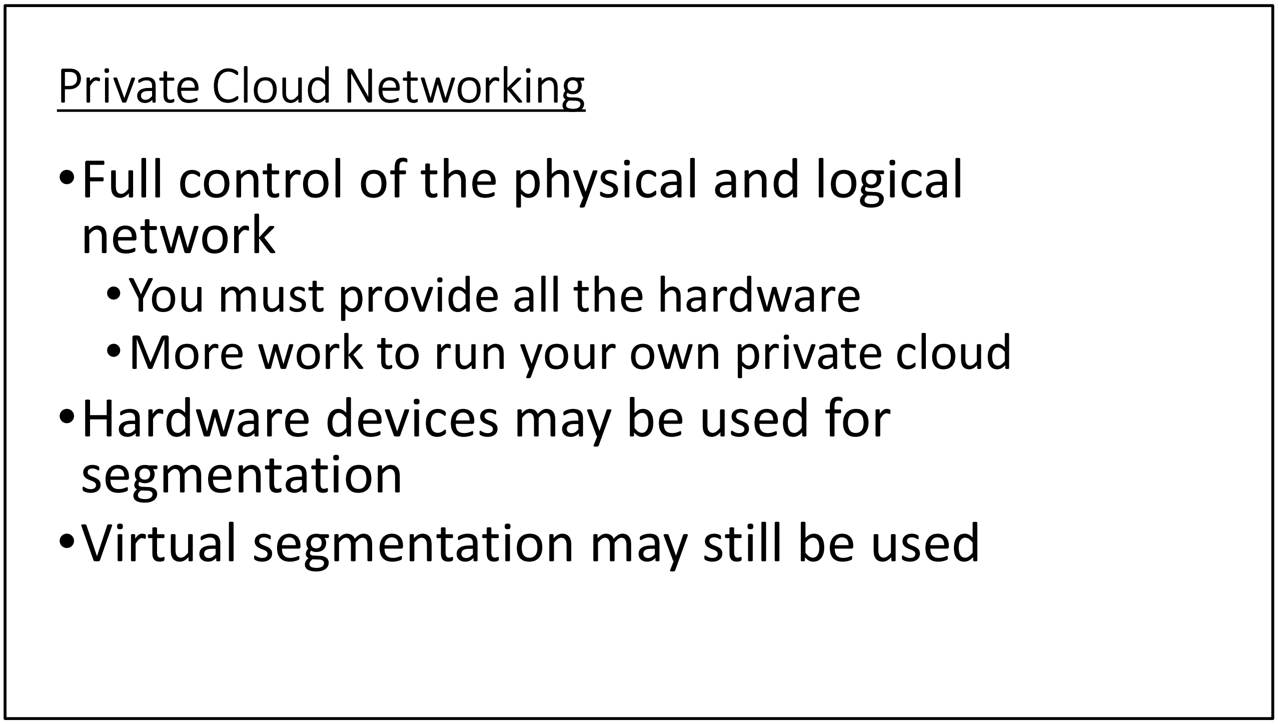
5.07 Networking in Different Models

CH05: Cloud Networking



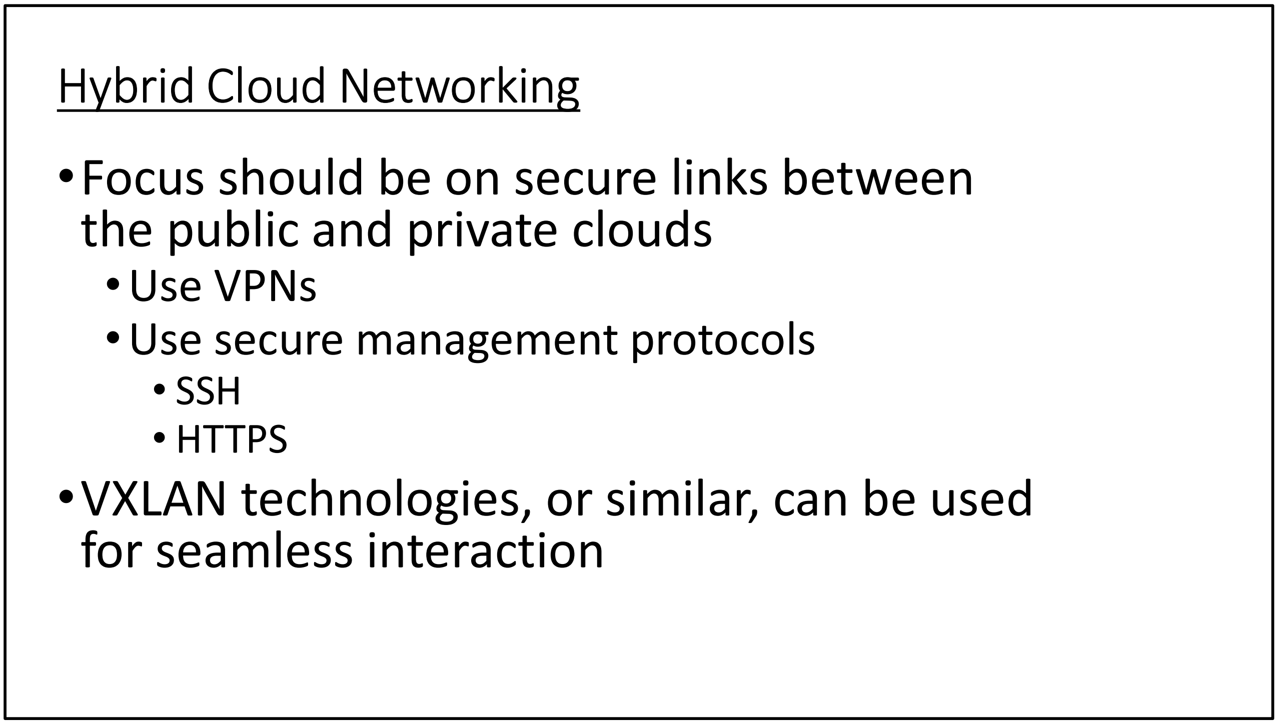
Public and Community Cloud Networking

- Nearly everything is virtual in the cloud
  - Virtual networks
  - Virtual segments
  - Virtual network adapters
- Understand your cloud provider's networking solutions
  - Match their terminology to traditional networking terminology to locate the proper solution
  - Ex: LAN vs. AWS Virtual Private Cloud (VPC)



Private Cloud Networking

- Full control of the physical and logical network
  - You must provide all the hardware
  - More work to run your own private cloud
- Hardware devices may be used for segmentation
- Virtual segmentation may still be used



Hybrid Cloud Networking

- Focus should be on secure links between the public and private clouds
  - Use VPNs
  - Use secure management protocols
    - SSH
    - HTTPS
- VXLAN technologies, or similar, can be used for seamless interaction