Chapter 4

Cloud Networking

Episode 4.01

Network Components Demo

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

Quick Review

- IP version 4 (IPv4) is the most widely used version of the IP protocol
- IPv6 uses a 128-bit address space as opposed to the IPv4 32-bit address space
- A default gateway is a router that connects your IP network to other networks

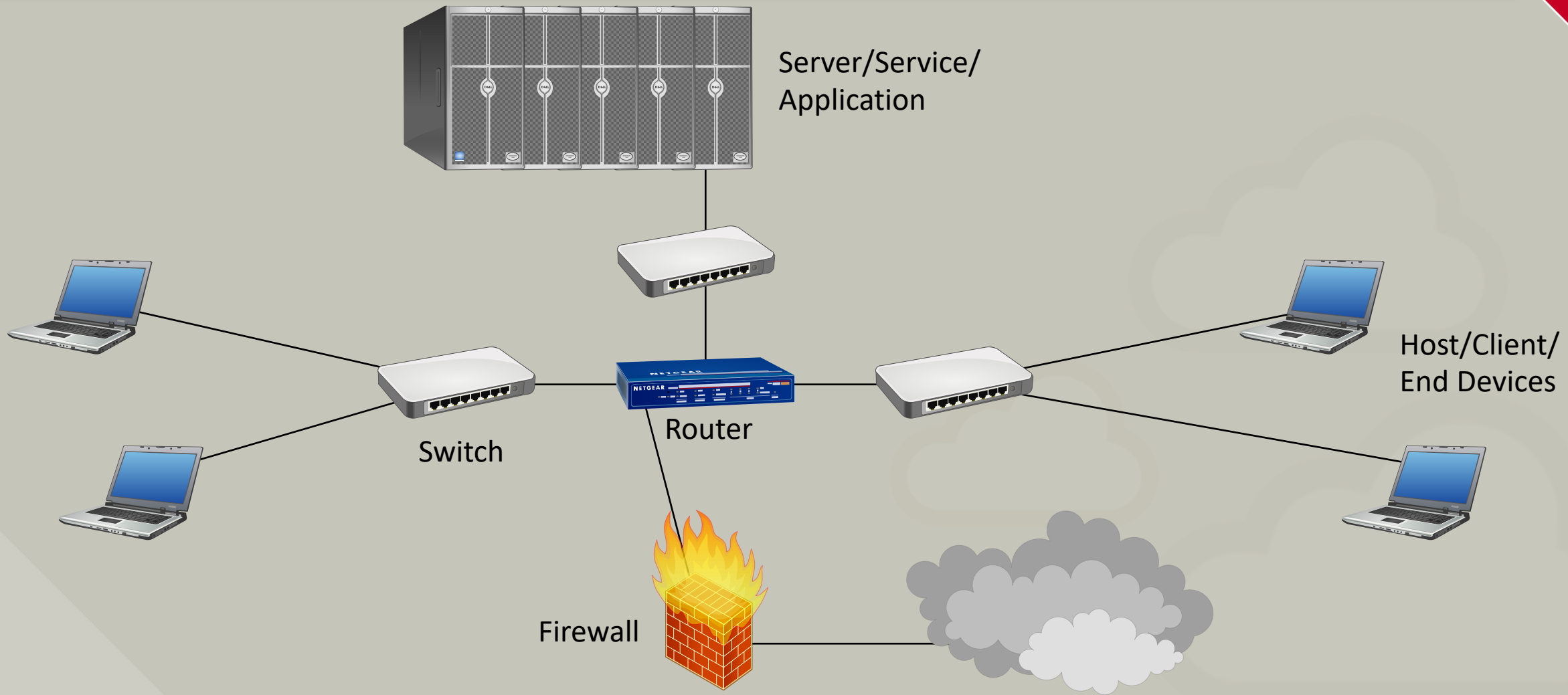
Episode 4.02

Networking Fundamentals

Network Devices

- Host/Client/End Device
- Server/Service/Application
- Switch
- Router
- Firewall

Network Devices Visualized



TCP/IP Suite/Stack

- Application
- TCP/UDP
- IP
- Ethernet/Wi-Fi/Other
- Wired/Wireless

IPv4 Addresses

- Internet Protocol version 4 (IPv4)
  - Communication protocol for devices connected to the internet
  - Assigns unique numeric addresses to devices
- IPv4 Address Structure
  - 32-bit numeric address
  - Written in dotted-decimal notation
  - Format: A.B.C.D (e.g., 192.168.1.1)
  - Each octet (A, B, C, or D) ranges from 0-255

IPv4 Address Categories

- Public
  - Unique, globally routable
  - Assigned in groups by the Internet Assigned Numbers Authority (IANA)
- Private
  - Reserved for local networks
  - Not routable on the Internet

10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

IPv6 Addresses

- 128-bit addresses instead of 32-bit
- Eight 16-bit groups separated by colons
  - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Leading zeros can be omitted
  - 2001:db8::1=2001:0db8:0000:0000:0000:0000:0000:0001
- Can be statically assigned or dynamically assigned through DHCPv6

TCP/UDP Communications

- Based on ports linked to destination/source services and applications
  - HTTP = TCP(80)
  - SMTP = TCP(25)
  - DNS = UDP(53)
  - NTP = UDP(123)

Episode 4.03

Network Protocols

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

Quick Review

- A protocol is a defined way of performing an action
- Network protocols define network communications for various actions
- DNS is used to resolve host names to IP addresses and IP addresses to host names

Episode 4.04

Network Ports Lab

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

Quick Review

- TCP and UDP ports are used to determine target and source applications within a network node
- Ports are referenced in notation as IP address:port, for example, 192.168.17.89:80
- TCP port 22 is used by SSH and TCP port 443 is used by HTTPS

Episode 4.05

Virtual Private Networks VPNs

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)

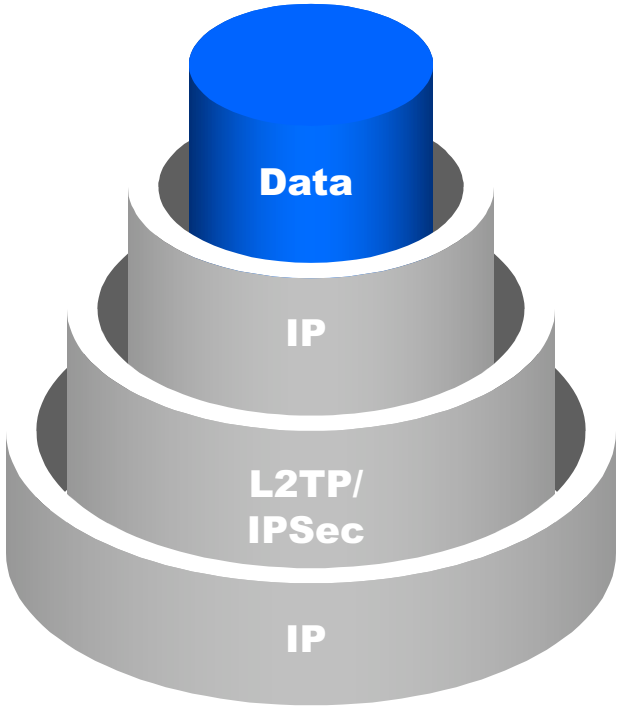
Common VPN Protocols

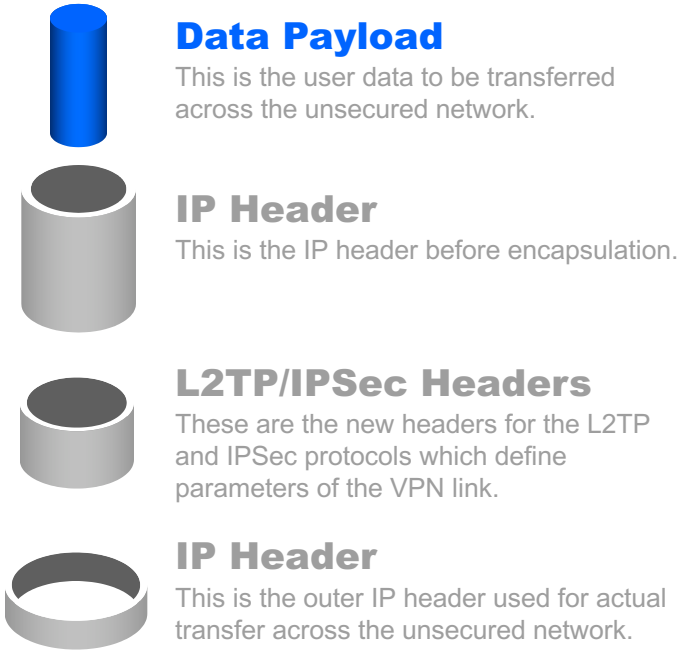
- IPSec (Internet Protocol Security)
  - Layer 3
  - Authenticates and encrypts packets
  - Authenticated Header (AH)
  - Encapsulation Security Payload (ESP)
    - Transport
    - Tunneled Mode

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

Quick Review

- A VPN creates a virtual tunnel that is encrypted between to endpoints
- VPNs encapsulate other network protocols (like TCP and UDP)
- Cloud-to-corporate, cloud-to-internal-cloud, cloud-to-external-cloud, and cloud-to-partner are all common cloud-based VPN implementations

Episode 4.06

IDS vs. IPS

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

Quick Review

- An Intrusion Detection System (IDS) detects potential attacks, logs them, and may notify someone
- An Intrusion Prevention System (IPS) detects potential attacks, logs them, may notify someone, and may take action to stop the attack
- IDS and IPS solutions work based on anomalies (heuristics), behavior (signatures), or both

Episode 4.07

Segmentation

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)

Quick Review

- Network segmentation is implemented with routers or virtual configurations to define network boundaries
- A demilitarized zone (DMZ) is usually implemented between the Internet and the internal network
- VXLANs are virtual extensible LANs that use tunneling to allow Layer 2 network segments to span Layer 3 (IP) routed networks
- Microsegmentation works at the workload or application level rather than Layer 2 or Layer 3 of the network

Episode 4.08

Network SLAs and Change Management

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

Quick Review

- Cloud providers will define their networking SLAs and you can view them to see what you should expect
- All network changes should begin with documentation of the current state and then make changes from there
- All changes should be thoroughly tested to ensure proper functionality

Episode 4.09

Networking in Different Models

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

Quick Review

- Public and community clouds, when offering network configuration, implement virtual network components (networks, segments, routers, switches, etc.)
- Private cloud networks provide full control of the networking as they run in your organization
- Hybrid cloud networks introduce the need to interconnect your private cloud with a public or community cloud

Episode 4.10

Additional Networking Considerations

SDN

- Software-Defined Network/Networking (SDN)
  - Separates the control and data plane
  - Abstracts hardware and behavior
- Three common layers of SDN:
  - Application
  - Control
  - Instrastructure

Virtual routing

- Multiple virtual routers on a single physical router
- May be implemented in VMware or Hyper-V
- Allows for the creation of multiple logical networks
- Within CSPs, each VM or instance can be linked to different virtual routers

MPLS

- Multiprotocol Label Switching (MPLS) uses labels to direct data packets through a network
- May be used to provide connectivity between CSPs and local end users
- May provide network segmentation in the cloud with VPCs (virtual private clouds)
- May be used for cloud interconnection between private and public clouds

SR-IOV

- Single root input/output virtualization (SR-IOV) allows a single NIC to be shared among VMs
- Uses direct access to the NIC for each VM
- Improves performance

Services

- DHCP – Dynamic Host Configuration Protocol
- IPAM – IP Address Management
- NTP – Network Time Protocol
- CDN – Content Delivery/Distribution Network

VPN

- Virtual Private Network (VPN)
  - Create a tunnel
  - Encrypt the tunnel
- Terminology
  - Point-to-Point
  - Point-to-Site
  - Site-to-Site