CSF 432: Intro to Network and System Security

Week 08 - Review

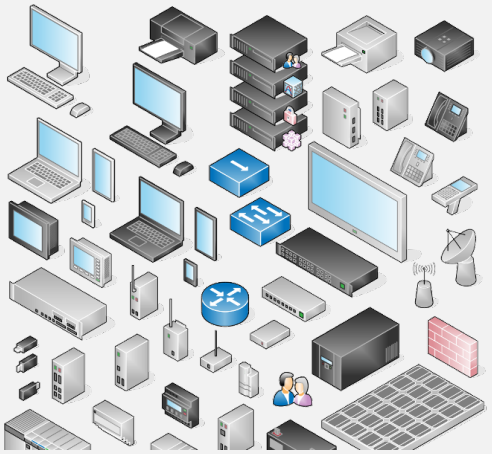
Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes

Networking Devices



Networking Devices

Hub

- "Multi-port repeater"
  - Traffic going in one port is repeated to every other port
  - OSI Layer 1
- Everything is half-duplex
- Becomes less efficient as network speeds increase
- 10 megabit / 100 megabit
- Difficult to find today

Networking Devices

Bridge

- Imagine a switch with two to four ports
  - Makes forwarding decisions in software
- Connects different physical networks
  - Can connect different topologies
  - Gets around physical network size limitations / collisions
- OSI Layer 2 device
  - Distributes traffic based on MAC address
- Most bridges these days are wireless access points
  - Bridges wired Ethernet to wireless

Networking Devices

Switch

- Bridging done in hardware
  - Application-specific integrated circuit (ASIC)
- An OSI layer 2 device
  - Forwards traffic based on data link address
- Many ports and features
  - The core of an enterprise network
  - May provide Power over Ethernet (PoE)
- Multilayer switch
  - Includes Layer 3 (routing) functionality

Networking Devices

Router

- Routes traffic between IP subnets
  - OSI layer 3 device
  - Routers inside of switches sometimes called “layer 3 switches”
  - Layer 2 = Switch
  - Layer 3 = Router
- Often connects diverse network types
  - LAN, WAN, copper, fiber

Networking Devices

Firewall

- Filters traffic by port number
  - OSI layer 4 (TCP/UDP)
  - Some firewalls can filter through OSI layer 7
- Can encrypt traffic into/out of the network
  - Protect your traffic between sites
- Can proxy traffic
  - A common security technique
- Most firewalls can be layer 3 devices (routers)
  - Usually sits on the ingress/egress of the network

Networking Devices

Wireless access point (WAP)

- Not a wireless router
  - A wireless router is a router and a WAP in a single device
- WAP is a bridge
  - Extends the wired network onto the wireless network
  - WAP is an OSI layer 2 device

Networking Devices

Modem

- Modulator / Demodulator
  - Converts analog sounds to digital signals
  - Needs a modem on both sides of the connection
- Uses standard phone lines
  - Limited frequencies, limited bandwidths
- POTS modems now used for backup and utility functions
- ADSL modems used for Internet Access
- Cable modem is a bridge

Networking Devices

Media Converter

- OSI Layer 1
  - Physical layer signal conversion
- Extend a copper wire over a long distance
  - Convert it to fiber, and back again
- You have fiber
  - The switch only has copper ports
- Almost always powered
  - Especially fiber to copper

Networking Devices

Wireless range extender

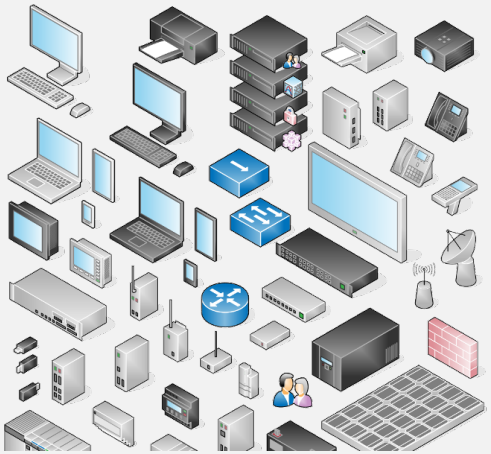
- Wireless never seems to stretch far enough
  - We can’t always choose where to install an access point
- Extend the reach of a wireless network
  - A wireless repeater

Networking Devices

VoIP endpoint

- Some people still communicate using voice
  - We now send this using VoIP
- The device can now be anything
  - Traditional phone handset, desktop application, mobile device app

Advanced Networking Devices



Advanced Networking Devices

Multilayer switches

- A switch (Layer 2) and router (Layer 3) in the same physical device
  - Layer 2 router?
- Switching still operates at OSI Layer 2, routing still operates at OSI Layer 3
  - There's nothing new or special happening here

Advanced Networking Devices

Wireless networks everywhere

- Wireless networking is pervasive
  - And you probably don't just have a single access point
- Your access points may not even be in the same building
  - One (or more) at every remote site
- Configurations may change at any moment
  - Access policy, security policies, AP configs
- The network should be invisible to your users
  - Seamless network access, regardless of role

Advanced Networking Devices

Balancing the load

- Distribute the load
  - Multiple servers
  - Invisible to the end-user
- Large-scale implementations
  - Web server farms, database farms
- Fault tolerance
  - Server outages have no effect
  - Very fast convergence

Advanced Networking Devices

Load balancer

- Configurable load
  - Manage across servers
- TCP offload
  - Protocol overhead
- SSL offload
  - Encryption/Decryption
- Caching
  - Fast response
- Prioritization
  - QoS
- Content switching
  - Application-centric balancing

Advanced Networking Devices

IDS and IPS

- Intrusion Detection System / Intrusion Prevention System
  - Watch network traffic
- Intrusions
  - Exploits against operating systems, applications, etc.
  - Buffer overflows, cross-site scripting, other vulnerabilities
- Detection vs. Prevention
  - Detection – Alarm or alert
  - Prevention – Stop it before it gets into the network

Advanced Networking Devices

Identification technologies

- Signature-based
  - Look for a perfect match
- Anomaly-based
  - Build a baseline of what's "normal"
- Behavior-based
  - Observe and report
- Heuristics
  - Use artificial intelligence to identify

Advanced Networking Devices

Proxies

- Sits between the users and the external network
- Receives the user requests and sends the request on their behalf (the proxy)
- Useful for caching information, access control, URL filtering, content scanning
- Applications may need to know how to use the proxy (explicit)
- Some proxies are invisible (transparent)

Advanced Networking Devices

Application proxies

- Most proxies in use are application proxies
  - The proxy understands the way the application works
- A proxy may only know one application, i.e., HTTP
- Many proxies are multipurpose proxies
  - HTTP, HTTPS, FTP, etc.

Advanced Networking Devices

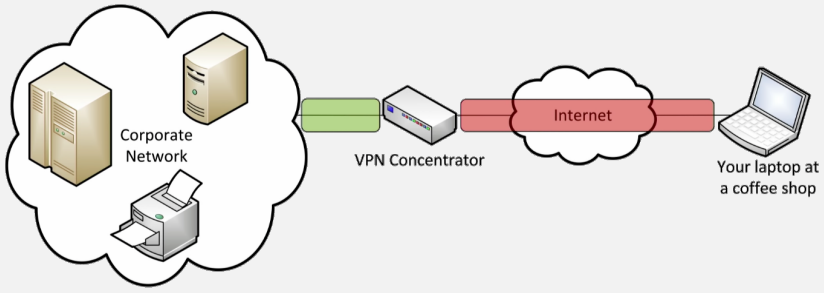
VPN concentrator

- Virtual Private Network
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software
  - Sometimes built into the OS

Advanced Networking Devices

Remote access VPN

- On-demand access from a remote device
  - Software connects to a VPN concentrator
- Some software can be configured as always-on



Advanced Networking Devices

AAA framework

- Identification - This is who you claim to be
  - Usually your username
- Authentication - Prove you are who you say you are
  - Password and other authentication factors
- Authorization
  - Based on your identification and authentication, what access do you have?
- Accounting
  - Resources used: Login time, data sent and received, logout time

Advanced Networking Devices

RADIUS (Remote Authentication Dial-in User Service)

- One of the more common AAA protocols
  - Supported on a wide variety of platforms and devices
- Centralize authentication for users
  - Routers, switches, firewalls
  - Server authentication
  - Remote VPN access
  - 802.1X network access
- RADIUS services available on almost any server operating system

Advanced Networking Devices

UTM / All-in-one security appliance

- Unified Threat Management (UTM) / Web security gateway
- URL filter / Content inspection
- Malware inspection
- Spam filter
- CSU/DSU
- Router, Switch
- Firewall
- IDS/IPS
- Bandwidth shaper
- VPN endpoint

Advanced Networking Devices

Next-generation Firewalls (NGFW)

- The OSI Application Layer
  - Layer 7 firewall
- Can be called different names
  - Application layer gateway
  - Stateful multilayer inspection
  - Deep packet inspection
- Requires some advanced decodes
  - Every packet must be analyzed, categorized, and a security decision determined

Advanced Networking Devices

VoIP technologies

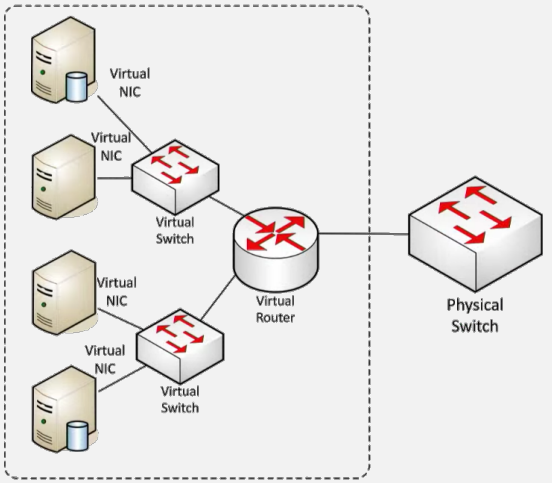
- PBX (Private Branch Exchange)
  - The “phone switch”
  - Connects to phone provider network
  - Analog telephone lines to each desk
- VoIP PBX
  - Integrate VoIP devices with a corporate phone switch
- VoIP Gateway
  - Convert between VoIP protocols and traditional PSTN protocols
  - Often built-in to the VoIP PBX

Advanced Networking Devices

Content filtering

- Control traffic based on data within the content
  - Data in the packets
- Corporate control of outbound and inbound data
  - Sensitive materials
- Control of inappropriate content
  - Not safe for work
  - Parental controls
- Protection against evil
  - Anti-virus, anti-malware

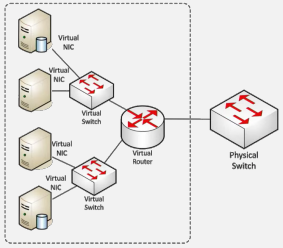
Virtual Networking



Virtual Networking

Network virtualization

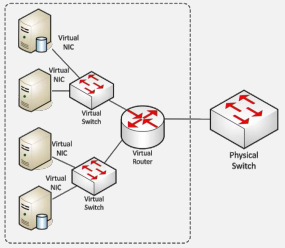
- Server farm with 100 individual computers
  - All servers are connected with enterprise switches and routers, with redundancy
- Migrate 100 physical servers
  - To one physical server with 100 virtual servers inside
- What happens to the network?



Virtual Networking

The hypervisor

- Virtual Machine Manager
  - Manages the virtual platform and guest OS
- May require a CPU that supports virtualization
  - Can improve performance
- Hardware management
  - CPU, networking, security



Virtual Networking

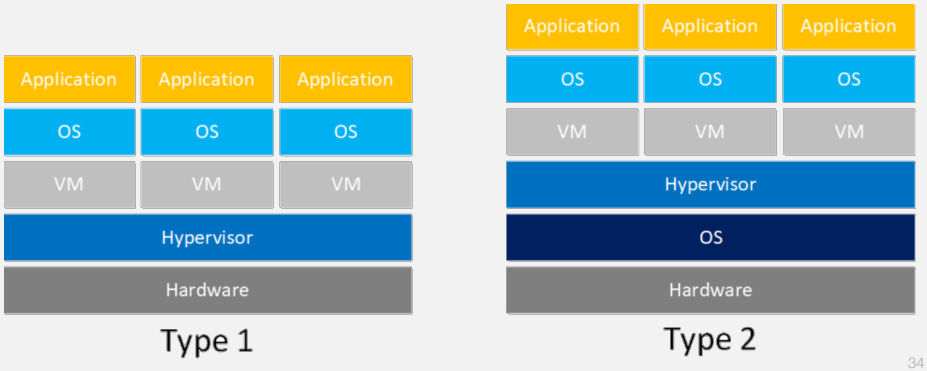
Network requirements

- Most client-side virtual machine managers have their own virtual (internal) networks
- Shared network address
  - The virtual machine shares the same IP address as the physical host
  - Uses a private IP address internally
  - Uses NAT to convert to the physical host IP
- Bridged network address
  - The VM is a device on the physical network
- Private address
  - The VM does not communicate outside of the virtual network

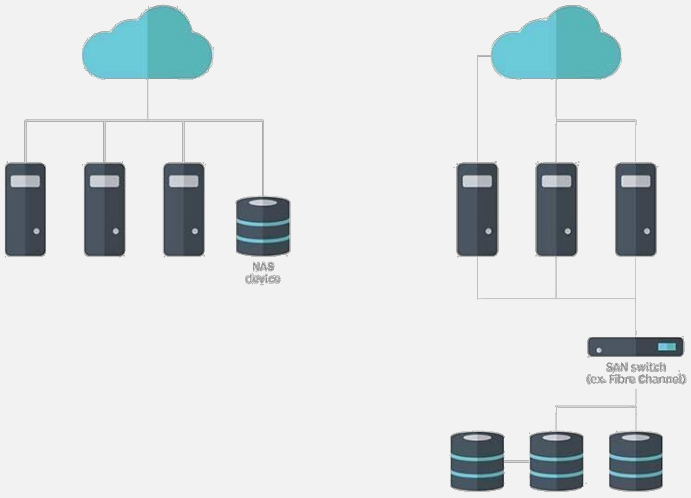
Virtual Networking

Type 1 and Type 2 Hypervisor

- Type 1 hypervisors sit directly on hardware (KVM, VMware ESX/ESXi)
- Type 2 hypervisors sit on a host operation system (VMWare Workstation/ Fusion, VirtualBox)



Network Storage

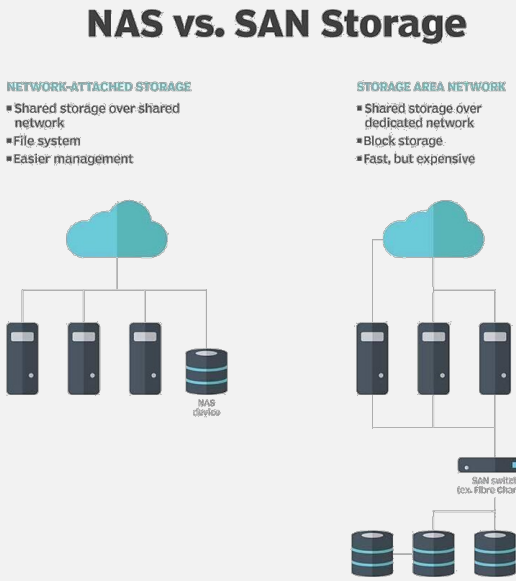


Network Storage

NAS vs. SAN

- Network Attached Storage (NAS)
  - Connect to a shared storage device across the network
  - File-level access
- Storage Area Network (SAN)
  - Looks and feels like a local storage device
  - Block-level access
  - Very efficient reading and writing
- Requires a lot of bandwidth
  - May use an isolated network and high-speed network technologies

Network Storage



Network Storage

Jumbo frames

- ☑ Ethernet frames with more than 1,500 bytes of payload
  - ☑ Up to 9,216 bytes (9,000 is the accepted norm)
- ☑ Increases transfer efficiency
  - ☑ Per-packet size
  - ☑ Fewer packets to switch/route
- ☑ Ethernet devices must support jumbo frames
  - ☑ Switches, interface cards
  - ☑ Not all devices are compatible with others

Network Storage

Common Storage Area Network Types

- ☑ Fibre Channel (FC)
- ☑ FCoE
- ☑ iSCSI
- ☑ InfiniBand

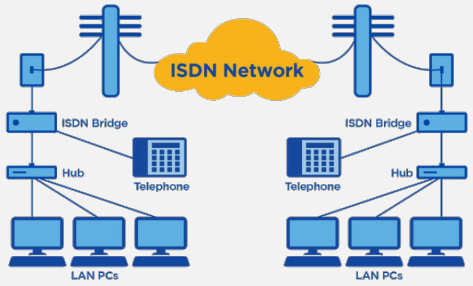
WAN Services

Network	Channels	Line Rate
T1	24 channels at 64 kbit/s each	1.544 Mbit/s
E1	32 channels at 64 kbit/s each	2.048 Mbit/s
T3	28 T1 circuits 672 channels	44.736 Mbit/s
E3	16 E1 circuits 512 channels	34.368 Mbit/s

WAN Services

ISDN - Integrated Services Digital Network

- BRI – Basic Rate Interface (2B+D)
  - Two 64 kbit/s bearer (B) channels
  - One 16 kbit/s signaling (D) channel
- PRI – Primary Rate Interface
  - Delivered over a T1 or E1
  - T1 – 23B + D
  - E1 – 30B + D + alarm channel
  - Commonly used as connectivity from the PSTN to large phone systems (PBX)



Network	Channels	Line Rate
T1	24 channels at 64 kbit/s each	1.544 Mbit/s
E1	32 channels at 64 kbit/s each	2.048 Mbit/s
T3	28 T1 circuits 672 channels	44.736 Mbit/s
E3	16 E1 circuits 512 channels	34.368 Mbit/s

WAN Services

- T1 / E1
- T3 / DS3 / E3

Network	Channels	Line Rate
T1	24 channels at 64 kbit/s each	1.544 Mbit/s
E1	32 channels at 64 kbit/s each	2.048 Mbit/s
T3	28 T1 circuits 672 channels	44.736 Mbit/s
E3	16 E1 circuits 512 channels	34.368 Mbit/s

WAN Services

OC (Optical Carrier)

- SONET (Synchronous Optical Networking)
- Commonly implemented by carriers on SONET rings

SONET	Line Rate
OC-3	155.52 Mbit/sec
OC-12	622.08 Mbit/sec
OC-48	2.49 Gbit/sec
OC-192	9.95 Gbit/sec

WAN Services

DSL

- ADSL (Asymmetric Digital Subscriber Line)
  - Uses telephone lines
- Download speed is faster than the upload speed (asymmetric)
  - ~10,000 foot limitation from the central office (CO)
  - 52 Mbit/s downstream / 16 Mbit/s upstream are common
  - Faster speeds may be possible if closer to the CO

WAN Services

Metro Ethernet

- Metropolitan-area network
  - A contained regional area
- Connect your sites with Ethernet
  - A common standard
  - Not your typical WAN connection
- The Ethernet is usually running over a different topology
  - Pure Ethernet
  - Ethernet over SDH, MPLS, or DWDM

WAN Services

Cable broadband

- Broadband
  - Transmission across multiple frequencies
  - Different traffic types
- Data on the “cable” network
  - DOCSIS (Data Over Cable Service Interface Specification)
- High-speed networking
  - 4 Mbits/s through 250 Mbits/s are common
  - Gigabit speeds are possible
- Multiple services - Data, voice

WAN Services

Dialup

- Network with voice telephone lines
  - Analog lines with limited frequency response
- 56 kbit/s modems - Compression up to 320 kbit/s
- Relatively slow throughput - Difficult to scale
- Legacy systems, network utility
  - May be difficult to find a modem

WAN Transmission Mediums

WAN Transmission Mediums

Satellite networking

- Communication to a satellite
  - Non-terrestrial communication
- High cost relative to terrestrial networking
  - 50 Mbit/s down, 3 Mbit/s up are common
  - Remote sites, difficult-to-network sites
- High latency - 250 ms up, 250 ms down
- High frequencies - 2 GHz
  - Line of sight, rain fade

WAN Transmission Mediums

Copper

- Extensive installations
  - Relatively inexpensive
  - Easy to install and maintain
- Limited bandwidth availability
  - Physics limits electrical signals through copper
- Wide area networks
  - Cable modem, DSL, T1/T3 local loop
- Often combined with fiber
  - Copper on the local loop, fiber in the backbone

WAN Transmission Mediums

Fiber

- High speed data communication - Frequencies of light
- Higher installation cost than copper
  - Equipment is more costly and more difficult to repair
  - Communicate over long distances
- Large installation in the WAN core
  - Supports very high data rates
  - SONET, wavelength division multiplexing
- Fiber is slowly approaching the premise
  - Business and home use

WAN Transmission Mediums

Wireless

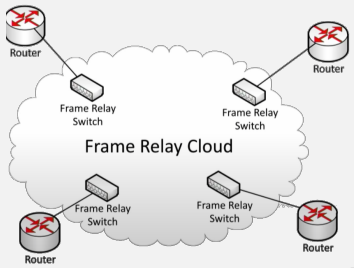
- Use the cellular network - Wireless WAN
  - Use an external hotspot or mobile phone
- Intermittent communication
  - Security system, daily point-of-sale reporting and updates
- Roaming communication
  - Field service, travel
- Limited by coverage and speed
  - Remote areas can be a challenge

WAN Technologies

WAN Technologies

Frame relay

- One of the first cost-effective WAN types
  - Departure from circuit-switched T1s
- LAN traffic is encapsulated into frame relay frames
- Frames are passed into the “cloud”
  - Magically appear out the other side
- Usually 64 Kbits/s through DS3 speeds
- Effectively replaced by MPLS
  - And other WAN technologies



WAN Technologies

ATM

- Asynchronous Transfer Mode
  - A common protocol transported over SONET
- 53-byte “cells” spaced evenly apart
  - 48-byte for data, 5-byte routing header
- High throughput, real-time, low latency
  - Data, voice, and video
- Max speeds of OC-192
  - Limits based on segmentation and reassembly (SAR)

WAN Technologies

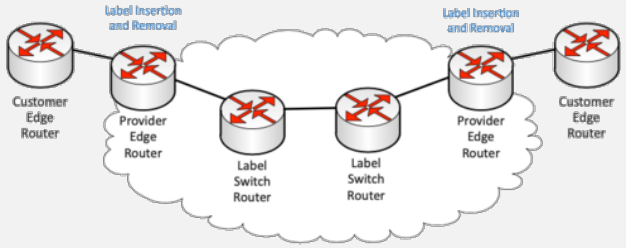
MPLS

- Learning from ATM and Frame Relay
- Packets through the WAN have a label
  - Routing decisions are easy
- Any transport medium, any protocol inside
  - IP packets, ATM cells, Ethernet frames
  - OSI layer 2.5 (!)
- Increasingly common WAN technology
  - Ready-to-network

WAN Technologies

MPLS pushing and popping

- Labels are “pushed” onto packets as they enter the MPLS cloud
- Labels are “popped” off on the way out



WAN Technologies

PPP (Point-to-point protocol)

- Create a network connection between two devices
  - OSI layer 2 / data link protocol
  - Communicate using many different protocols
- Works almost anywhere
  - Dial-up connections, serial links, mobile phone, DSL (PPPoE)
- Provides additional data link functionality
  - Authentication
  - Compression
  - Error detection
  - Multilink

WAN Technologies

PPPoE

- Encapsulate point-to-point protocol over Ethernet
  - The past with the present
- Common on DSL networks
  - Telephone providers know PPP
- Easy to implement
  - Support in most operating systems
  - No routing required
  - Similar to existing dialup architecture
- Allows competition
  - Once connected, data is switched to the appropriate ISP

WAN Technologies

DMVPN

- Dynamic Multipoint VPN
  - Common on Cisco routers
- Your VPN builds itself
  - Remote sites communicate to each other
- Tunnels are built dynamically, on-demand
  - A dynamic mesh

WAN Technologies

SIP trunking

- Session Initiation Protocol
  - Control protocol for VoIP
- Traditional PBX connectivity uses T1/ISDN
  - 23 voice channels, 1 signaling channel
  - When the lines are full, you get a busy signal
- SIP trunking
  - Use SIP/VoIP to communicate to an IP-PBX provider
- More efficient use of bandwidth
  - Less expensive than ISDN lines
  - More phone system options

WAN Termination

WAN Termination

Demarcation point

- The point where you connect with the outside world
  - WAN provider
  - Internet service provider
  - The demarc
- Used everywhere
  - Even at home
- Central location in a building
  - Usually a network interface device
  - Can be as simple as an RJ-45 connection
- You connect your CPE
  - Customer premises equipment or “customer prem”

WAN Termination

Channel Service Unit/Data Service Unit connectivity

- CSU
  - Connects to the network provider
- DSU
  - Connects to the data terminal equipment (usually an internal router)
- Physical device
  - Or built-in to the router

WAN Termination

Smartjack

- Network interface unit (NIU)
  - The device that determines the demarc
  - Network Interface Device, Telephone Network Interface
- Smartjack
  - More than just a simple interface
  - Can be a circuit card in a chassis
- Built-in diagnostics
  - Loopback tests
- Alarm indicators
  - Configuration, status

CSF 432: Intro to Network and System Security

Week 08 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes