2021 CISSP MENTOR PROGRAM

Class 7 – May 5, 2021

Instructor:

- Evan Francen, FRSecure and SecurityStudio CEO

ALMOST HALFWAY THERE!

Let's get on it!

Knowledge isn't power until it is applied -Dale Carnegie

- Check-in.
- How many have read Chapter 1 - 5?
- Questions?

Only 107 slides tonight, but this part of the book is sort of all over the place. We'll finish chapter 5!

GETTING GOING…

Security Models is the BOMB!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the study group
- Exercise or get fresh air in between study sessions

Let's get going!

GETTING GOING…

Security Models is the BOMB!

Study Group:

If you haven't already signed up, we have a study group, you can register at:
https://groups.io/g/FRSecure2021CISSPMentorProgram

Practice Test:

https://www.cccure.education/

Let's get going!

LET'S DO THIS!

Picking up where we left off.

Where we left off…

WHAT ARE WE GOING TO COVER?

Agenda – Domain 4: Communication and Network Security

- Network Architecture and Design
- Secure Network Devices and Protocols
- Secure Communications

Starting on page 253 this evening

Great domain for the techies. A little more challenging for the “normal” people…

NETWORK ARCHITECTURE AND DESIGN

Network Architecture and Design

WAN Technologies and Protocols - T1s, T3s, E1s, E3s

- T Carriers (United States)
- E Carriers (Europe)
- T1:
  - Dedicated 1.544-megabit circuit
  - Twenty-four 64-bit DS0 (Digital Signal 0) channels (such as 24 circuit-switched phone calls)
  - DS1 (Digital Signal 1) and T1 are often used interchangeably
  - DS1 describes the flow of bits (via any medium, such as copper, fiber, wireless, etc.); a T1 is a copper telephone circuit that carries a DS1.
- T3:
  - 28 bundled T1s
  - 44.736-megabit circuit
  - T3 and DS3 (Digital Signal 3) are also used interchangeably

LECTURE

Network Architecture and Design

WAN Technologies and Protocols - T1s, T3s, E1s, E3s

- E1:
  - Dedicated 2.048-megabit circuit
  - 30 channels
- E3:
  - 24 E1s
  - 34.368 megabits.
- T1 and T3 speeds are often rounded off to 1.5 and 45 megabits
- SONET (Synchronous Optical Networking) carries multiple T-carrier circuits via fiber optic cable
- SONET uses a physical fiber ring for redundancy.

LECTURE

Network Architecture and Design

WAN Technologies and Protocols – Frame Relay

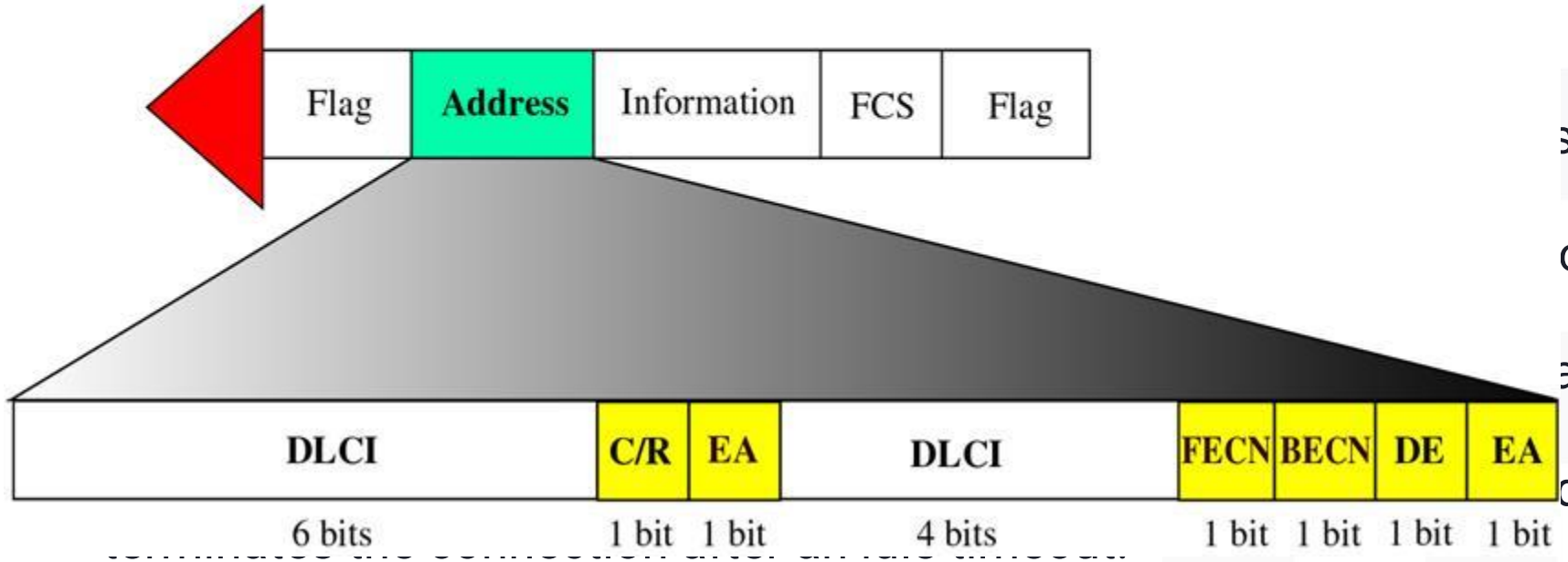
- Packet-switched Layer 2 WAN protocol
- Provides no error recovery
- Focuses on speed
- Higher layer protocols carried by Frame Relay, such as TCP/IP can be used to provide reliability
- Multiplexes multiple logical connections over a single physical connection to create Virtual Circuits
  - PVC (Permanent Virtual Circuit) is always connected, analogous to a real dedicated circuit like a T1.
  - SVC (Switched Virtual Circuit) sets up each “call,” transfers data, and terminates the connection after an idle timeout.
- Frame Relay is addressed locally via Data Link Connection Identifiers (DLCI, pronounced “delsee”).

LECTURE

Network Architecture and Design

WAN

C/R: Command/response
EA: Extended address
FECN: Forward explicit congestion notification
BECN: Backward explicit congestion notification
DE: Discard eligibility
DLCI: Data link connection identifier



- Frame Relay is addressed locally via Data Link Connection Identifiers (DLCI, pronounced “delsee”).

LECTURE

Network Arch

WAN C/R: Comma
EA: Extende
- FECN: Forw
-
-
-
-

- Frame Re
pronounc

n notification

er

sed to

on to

a real

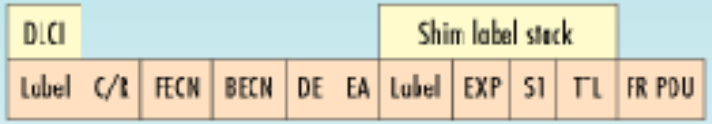
d

it 1 bit 1 bit

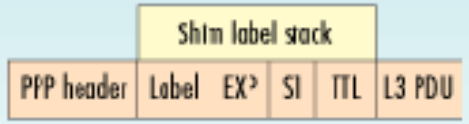
ntifiers (DLCI,

1. ATM-based label header

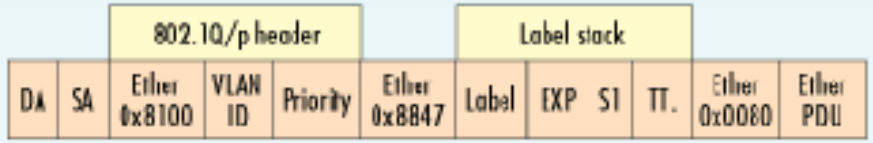
2. Frame relay-based label header



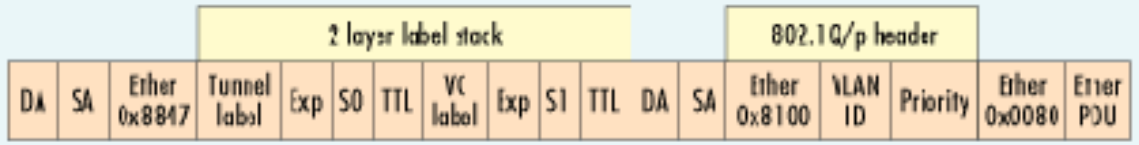
3. PPP with shimming label header



4. MPLS over Ethernet label header



5. Ethernet over MPLS label header



6. Frame relay over MPLS label header

FIGURE 1: Packet-header formats for different MPLS applications.

LECTURE

Network Architecture and Design

WAN Technologies and Protocols – X.25

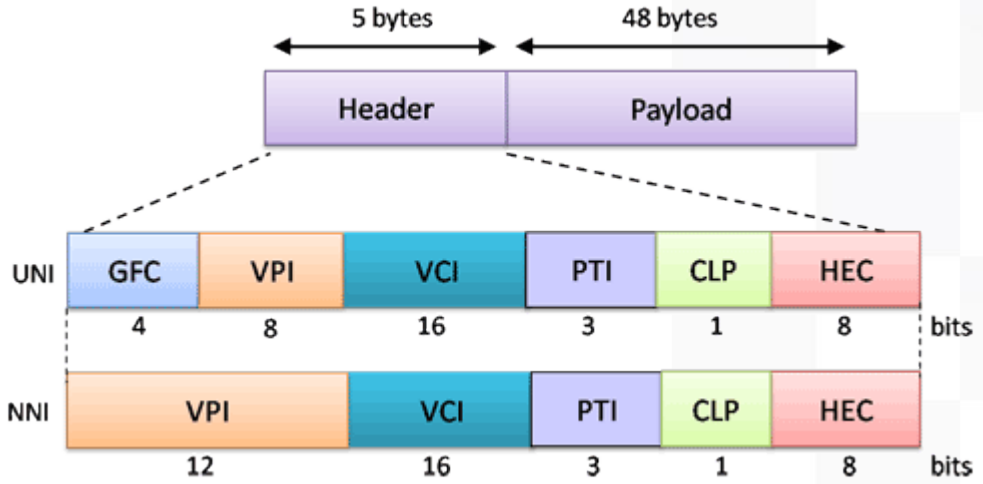
- An older packet-switched WAN protocol
- Provided a cost-effective way to transmit data over long distances in the 1970s though early 1990s
- The global packet switched X.25 network is separate from the global IP-based Internet
- Performs error correction which can add latency on long links
- Can carry other protocols such as TCP/IP

LECTURE

Network Architecture and Design

WAN Technologies and Protocols – ATM

- Asynchronous Transfer Mode (ATM)
- WAN technology that uses fixed length cells
- ATM cells are 53 bytes long, with a 5-byte header and 48-byte data portion
- SMDS (Switched Multimegabit Data Service) is older and similar to ATM, also using 53-byte cells

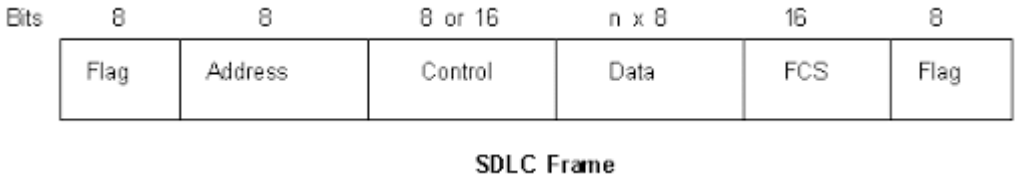


LECTURE

Network Architecture and Design

WAN Technologies and Protocols – SDLC and HDLC

- Synchronous Data Link Control (SDLC)
  - Synchronous Layer 2 WAN protocol
  - Uses polling to transmit data
  - Polling is similar to token passing; the difference is a primary node polls secondary nodes, which can transmit data when polled
  - Combined nodes can act as primary or secondary
  - SDLC supports NRM transmission only (see next slide)



SDLC Frame

LECTURE

Network Architecture and Design

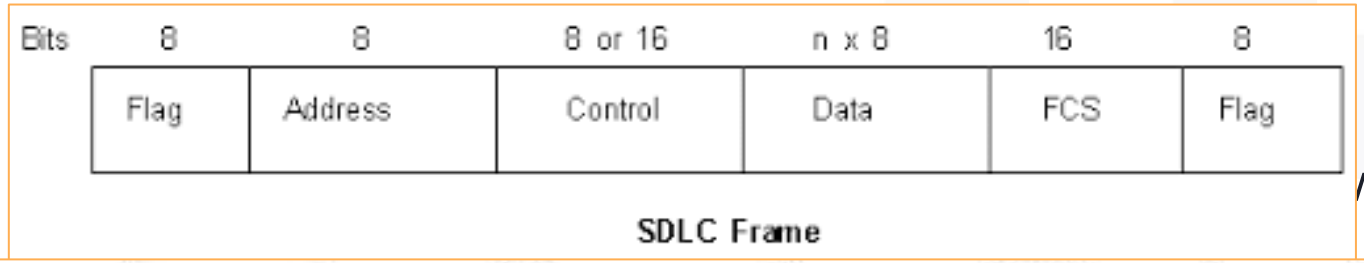
WAN Technologies and Protocols – SDLC and HDLC

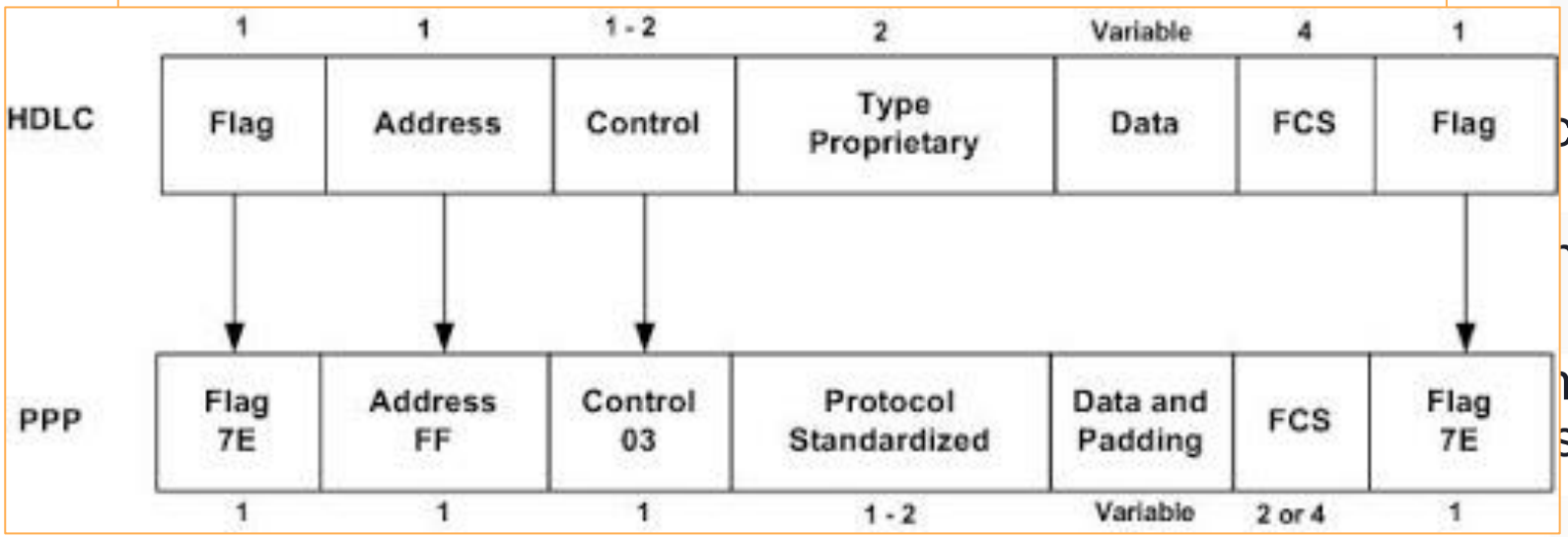
- High-Level Data Link Control (HDLC)
  - Successor to SDLC
  - Adds error correction and flow control, as well as two additional modes (ARM and ABM)
  - The three modes of HDLC are:
    - Normal Response Mode (NRM)—Secondary nodes can transmit when given permission by the primary
    - Asynchronous Response Mode (ARM)—Secondary nodes may initiate communication with the primary
    - Asynchronous Balanced Mode (ABM)—Combined mode where nodes may act as primary or secondary, initiating transmissions without receiving permission

LECTURE

Network Architecture and Design

WAN Technologies and Protocols – SDLC and HDLC





wo additional modes (ARM

can transmit when

nodes may initiate

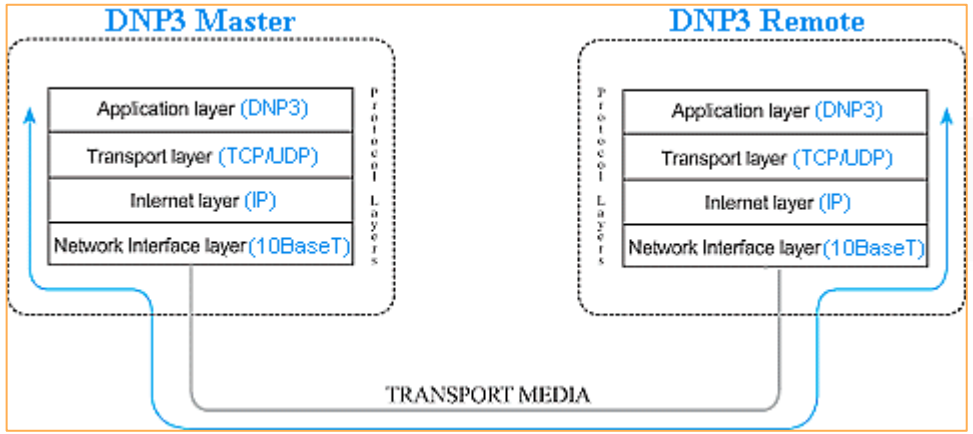
node where nodes may
s without receiving

LECTURE

Network Architecture and Design

Converged Protocols

- Traditional non-IP services all provided on Ethernet and IP.
- Distributed Network Protocol (DNP3) – open standard, mostly used in the energy industry.
  - a multilayer protocol, can be carried via TCP/IP
  - “smart grid technology”
  - became an IEEE standard in 2010, called IEEE 1815-2010 (now deprecated)
  - IEEE 1815-2012 is the current standard; it supports Public Key Infrastructure (PKI)



LECTU

Network A

Converge

- Tradi
- Distri
  indus
  - a
  - "s
  - b
  - IE
    (I

d in the energy

v deprecated)
Infrastructure

InduSoft AN INVENSYS COMPANY

indusoft.com
info@indusoft.com

DNP3 Protocol Main concepts

Master/Slave protocol

ISO/OSI mapping:

ISO/OSI Model	DNP 3
Application	IEC-1815 DNP3 Specific
Presentation	
Session	
Transport	TCP / UDP
Network	IP
Data Link	Data Link
Physical	Multiple (e.g.: Ethernet)

LECTURE

Network Architecture and Design

Storage Protocols

- Fibre Channel over Ethernet (FCoE)
  - FCoE uses Ethernet
  - Fibre Channel over IP (FCIP) encapsulates frames via TCP/IP
  - HBA (Host Bus Adapters)
- Internet Small Computer System Interface (iSCSI)
  - Can access storage across a WAN
  - Uses Logical Unit Numbers (LUNs)

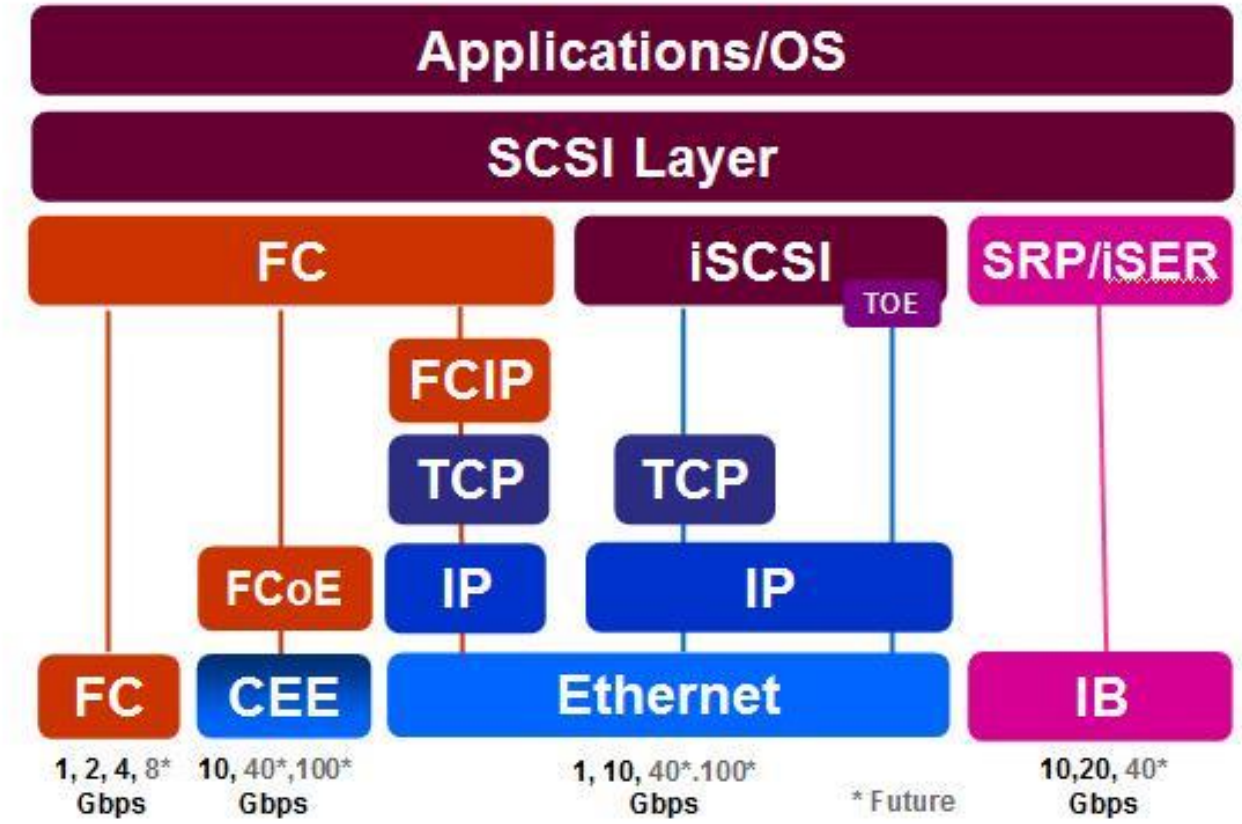
LECTU

Network

Storage F

- Fibre
  - F
  - F
  - H
- Interi
  - C
  - L

FCoE vs. FC vs. iSCSI vs. IB



LECTURE

Network Architecture and Design

Voice over Internet Protocol (VoIP)

- Carries voice via data networks, Lower cost and resiliency
- Replaced analog POTS (Plain Old Telephone Service)
- Real-time Transport Protocol (RTP), designed to carry streaming audio and video
- Session Initiation Protocol (SIP), a signaling protocol
- Secure Real-time Transport Protocol (SRTP), provides secure VoIP using AES and SHA-1
- Without SRTP (RTP only), calls are prone to sniffing. IPSec can also be used.

LECTURE

Network Architecture and Design

Voice

- Ca
- Re
- Re
- Se
- Se
  SH
- W

o and video

ing AES and

e used.

Data	Control and Signaling		Audio/ Video	Registration
T.120	H.225.0 Call Signaling	H.245 Conference Control	RTP/RTCP	H.225.0 RAS
TCP			UDP	
Network Layer				
Data link Layer				
Physical Layer				

LECTURE

Network Architecture and Design

Wireless Local Area Networks

- Transmit information via electromagnetic waves (such as radio) or light
- The most common form of wireless data networking is the 802.11 wireless standard
- The first 802.11 standard with reasonable security is 802.11i

DoS & Availability

- WLANs have no way to assure availability
- An attacker with physical proximity can launch a variety of Denial-of-Service attacks, including polluting the wireless spectrum with noise
- Critical applications that require a reliable network should use wired connections

LECTURE

Network Architecture and Design

Wireless Local Area Networks

Unlicensed Bands

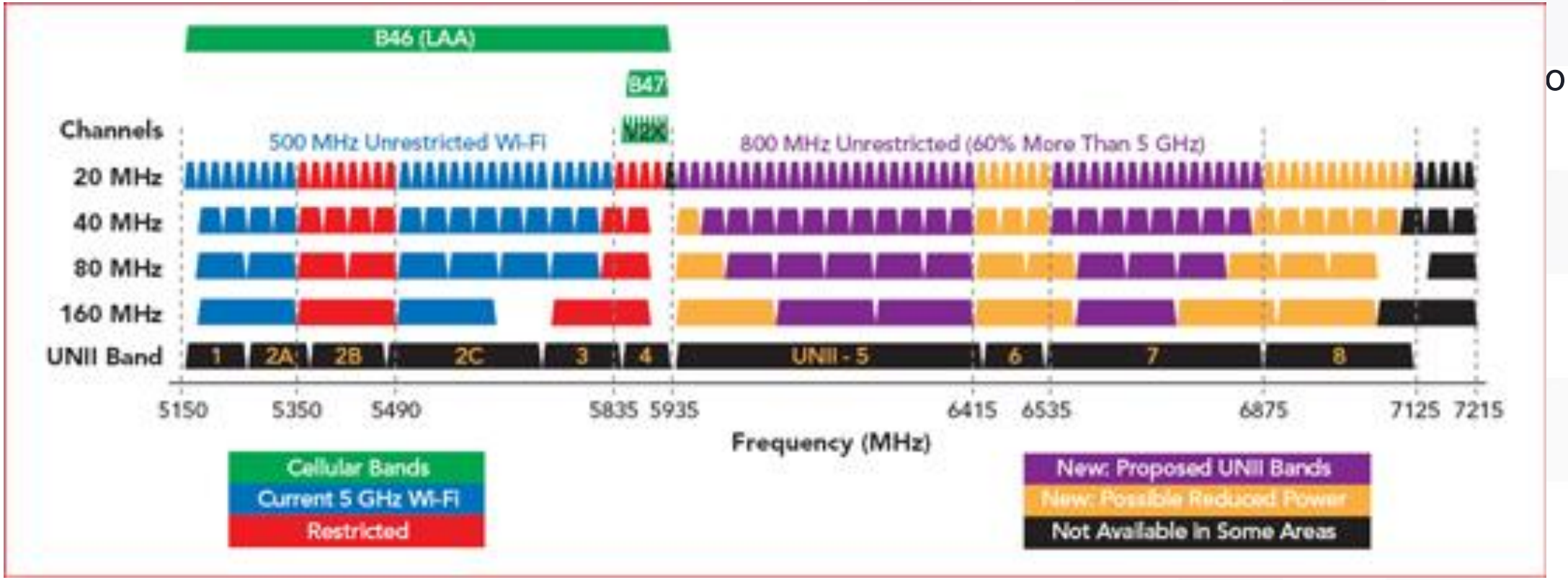
- A “band” is a small amount of contiguous radio spectrum
- Industrial, Scientific, and Medical (ISM) bands are set aside for unlicensed use (no license from an organization such as the Federal Communications Commission (FCC) require to use them)
- Many wireless devices such as cordless phones, 802.11 wireless, and Bluetooth use ISM bands
- Different countries use different ISM bands: two popular ISM bands used internationally are 2.4 and 5 GHz

LECTURE

Network Architecture and Design

Wireless Local Area Networks

Unlicensed Bands



LECTURE

Network Architecture and Design

Wireless Local Area Networks

FHSS, DSSS, and OFDM

- Frequency Hopping Spread Spectrum (FHSS)
  - Method of sending traffic via a radio band
  - Designed to maximize throughput while minimizing the effects of interference
  - Uses a number of small frequency channels throughout the band and “hops” through them in pseudorandom order
- Direct Sequence Spread Spectrum (DSSS)
  - Method of sending traffic via a radio band
  - Designed to maximize throughput while minimizing the effects of interference
  - Uses the entire band at once, “spreading” the signal throughout the band
- Orthogonal Frequency-Division Multiplexing (OFDM)
  - A newer multiplexing method
  - Allows simultaneous transmission using multiple independent wireless frequencies that do not interfere with each other

LECTURE

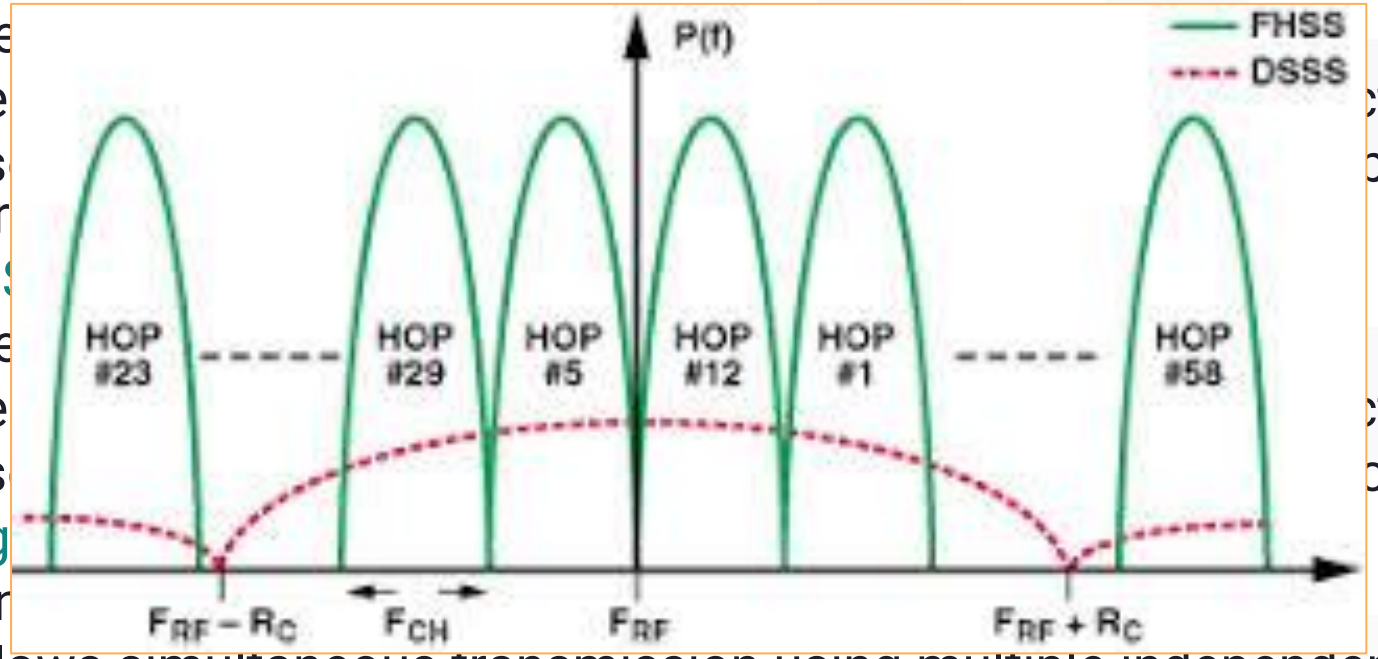
Network Architecture and Design

Wireless Local Area Networks

FHSS, DSSS, and OFDM

- Frequency Hopping Spread Spectrum (FHSS)
  - Me
  - De
  - Us
    thr
- Direct S
  - Me
  - De
  - Us
- Orthog
  - A r
  - Allows simultaneous transmission using multiple independent wireless frequencies that do not interfere with each other

cts of interference
band and “hops”
cts of interference
out the band



LECTURE

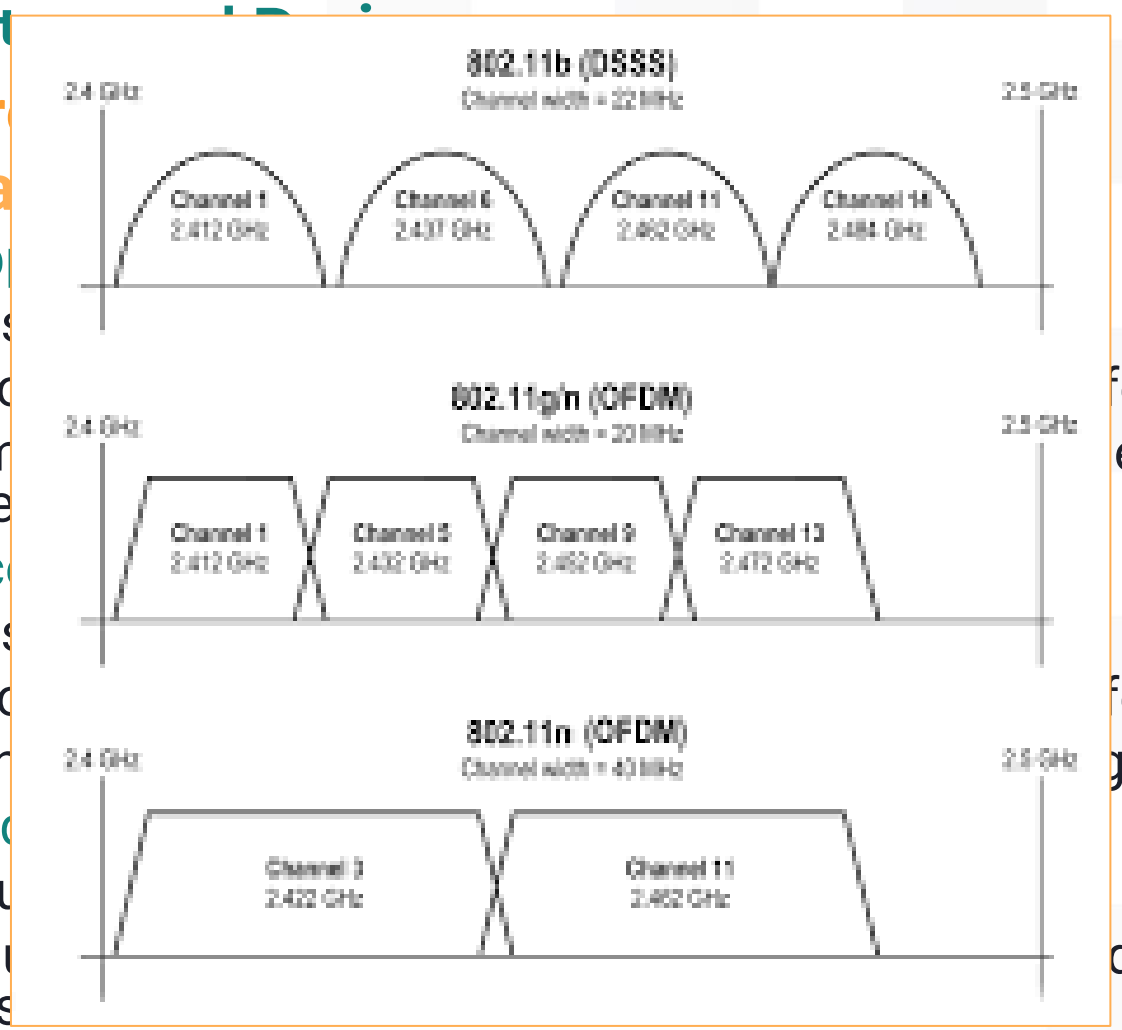
Network Architect

Wireless Local Ar

FHSS, DSSS, a

- Frequency Hop
  - Method of s
  - Designed to
  - Uses a num through the
- Direct Sequenc
  - Method of s
  - Designed to
  - Uses the en
- Orthogonal Freq
  - A newer mu
  - Allows simu frequencies

fects of interference
e band and “hops”
fects of interference
ghout the band
dent wireless



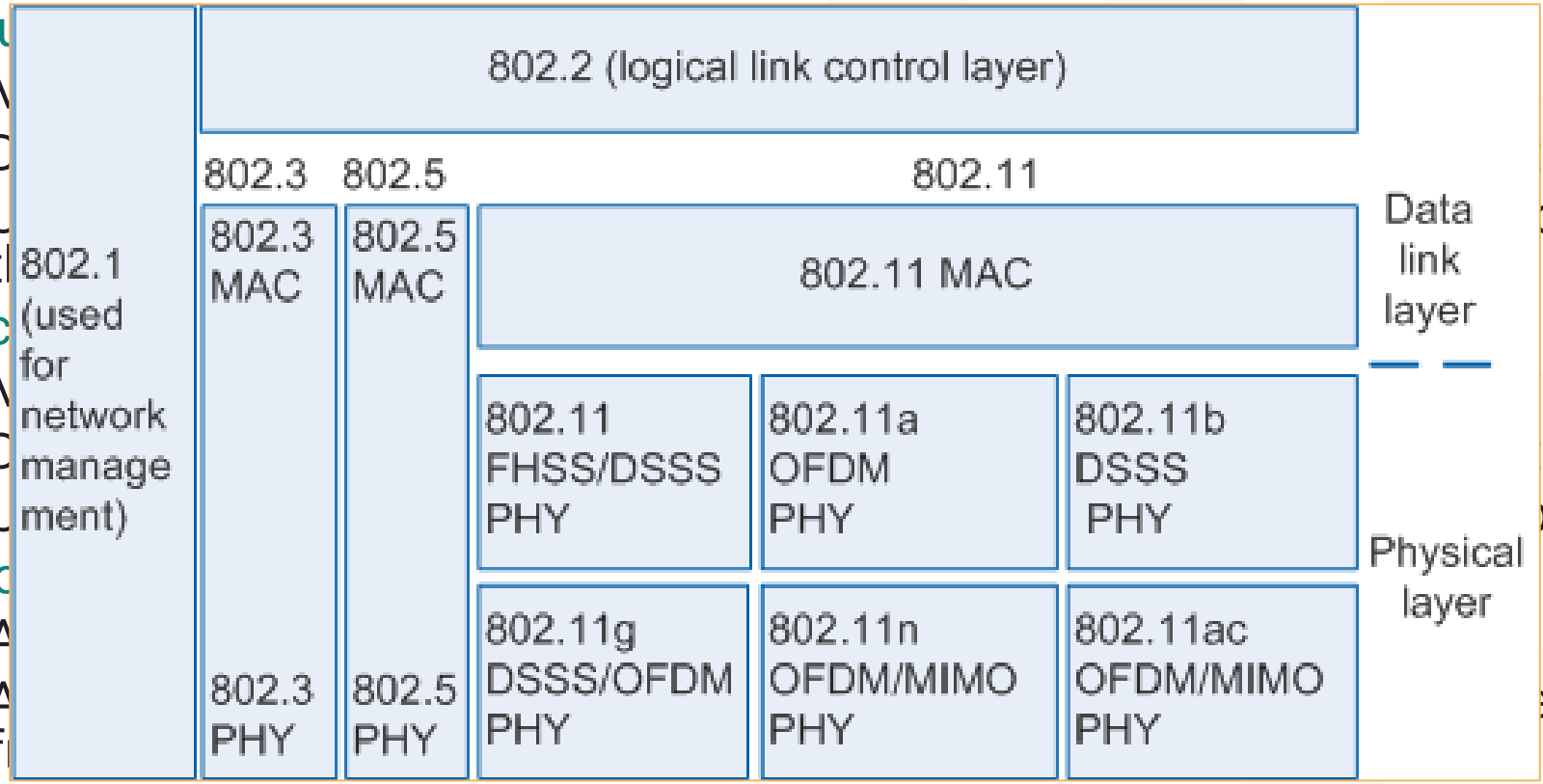
LECTURE

Network Architecture and Design

Wireless Local Area Networks

FHSS, DSSS, and OFDM

- Frequ
  - M
  - D
  - U
    t
- Direc
  - M
  - D
  - U
- Ortho
  - A
  - A
    f



erference
d “hops”
erference
band
ess

LECTURE

Network Architecture and Design

Wireless Local Area Networks

IEEE Network Standards

Wireless Networking Standards		
IEEE Standard	Max. Speed	Max. Range
802.11a	54 Mbps	75 feet
802.11b	11 Mbps	150 feet
802.11g	54 Mbps	150 feet
802.11n	600 Mbps	175 feet
802.11ac	1300 Mpbs	175 feet

IEEE 802 Standards

Standard	Name	Topic
802.1	Internetworking	Routing, bridging, and network-to-network communications
802.2	Logical Link Control	Error and flow control over data frames
802.3	Ethernet LAN	All forms of Ethernet media and interfaces
802.4	Token Bus LAN	All forms of Token Bus media and interfaces
802.5	Token Ring LAN	All forms of Token Ring media and interfaces
802.6	Metropolitan Area Network (MAN)	MAN technologies, addressing, and services
802.7	Broadband Technical Advisory Group	Broadband networking media, interfaces, and other equipment
802.8	Fiber Optic Technical Advisory Group	Fiber optic media used in token-passing networks like FDDI
802.9	Integrated Voice/ Data Networks	Integration of voice and data traffic over a single network medium
802.10	Network Security	Network access controls, encryption, certification, and other security topics
802.11	Wireless Networks	Standards for wireless networking for many different broadcast frequencies and usage techniques also known as Wi-Fi
802.12	High-Speed Networking	A variety of 100 Mbps-plus technologies, including 100BASE-VG
802.14	Cable broadband LANs and MANs	Standards for designing networks over coaxial cable- based broadband connections
802.15	Wireless Personal Area Networks	The coexistence of wireless personal area networks with other wireless devices in unlicensed frequency bands
802.16	Broadband Wireless Access	The atmospheric interface and related functions associated with Wireless Local Loop (WLL)

LECTURE

Network Architecture and Design

Wireless Local Area Networks

802.11 abgn

Parameter	IEEE 802.11 Revisions				
	802.11a	802.11b	802.11g	802.11n	802.11ac
Standard Approved	July 1999	July 1999	June 2003	October 2009	January 2014
Maximum Data Rate (Theoretical)	54 Mbps	11 Mbps	54 Mbps	450 Mbps	6.77 Gbps
Modulation	OFDM	DSSS or CCK	DSSS or OFDM	OFDM	OFDM
RF Band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz or 5 GHz	5 GHz
Number of Spatial Streams	1	1	1	Up to 4	Up to 8
Channel Width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz	20, 40, 80 or 160 MHz

Wireless Standards 802.11a, 802.11b/g/n, and 802.11ac

	✓ PROS	✗ CONS
802.11b	Lowest cost; signal range is good and not easily obstructed	Slowest maximum speed; home appliances may interfere on the unregulated frequency band
802.11a	Fast maximum speed; regulated frequencies prevent signal interference from other devices	Highest cost; shorter range signal that is more easily obstructed
802.11g	Fast maximum speed; signal range is good and not easily obstructed	Costs more than 802.11b; appliances may interfere on the unregulated signal frequency
802.11n	Fastest maximum speed and best signal range; more resistant to signal interference from outside sources	Standard is not yet finalized; costs more than 802.11g; the use of multiple signals may greatly interfere with nearby 802.11b/g based networks

LECTURE

Network Architecture and Design

Wireless Local Area Networks

Managed, Master, Ad-Hoc and Monitor modes

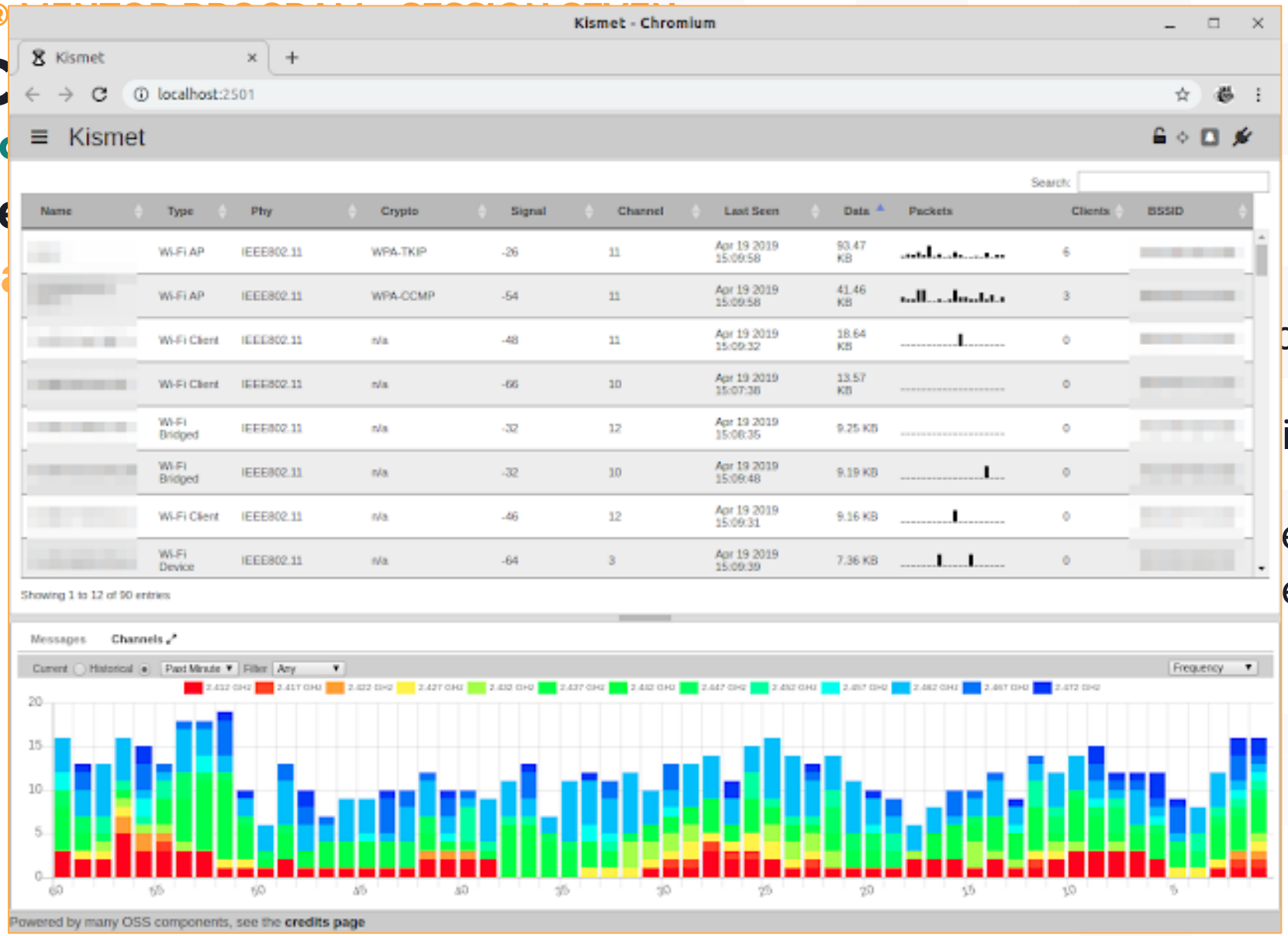
- Managed Mode (aka client mode) – clients cannot connect to anyone other than the access point when connected.
- Master Mode (aka infrastructure mode) – can only connect with clients in managed mode.
- Ad-Hoc Mode – peer-to-peer communication without a central access point.
- Monitor Mode – read-only for sniffing WLAN traffic (Kismet & Wellenreiter)

LEC

Netwo

Wirele

Ma



one other

ients in

ess point.

enreiter)

LECTURE

Network Architecture and Design

Wireless Local Area Networks

SSID and MAC Address Filtering

- 802.11 WLANs use a Service Set Identifier (SSID), which acts as a network name
- Wireless clients must know the SSID before joining the WLAN
- SSIDs are normally broadcasted; some WLANs are configured to disable SSID broadcasts
- Relying on the secrecy of the SSID is a poor security strategy: a wireless sniffer in monitor mode can detect the SSID used by clients as they join WLANs: this is true even if SSID broadcasts are disabled
- MAC addresses are exposed in plaintext on 802.11 WLANs: trusted MACS can be sniffed, and an attacker may reconfigure a nontrusted device with a trusted MAC address in software

LECTURE

Network Architecture and Design

Wireless Local Area Networks

WEP

- Wired Equivalent Privacy protocol
- Has proven to be **critically weak**: new attacks can break any WEP key in minutes
- Provides little integrity or confidentiality protection
- Its use is strongly discouraged. 802.11i and/or other encryption methods such as VPN should be used in place of WEP
- Has 40 and 104-bit key lengths, and uses the RC4 cipher
- Frames have no timestamp and no replay protection

LECTURE

Network Architecture and Design

Wireless Local Area Networks

WEP has been widely criticized for several weaknesses.

- Weakness: Key Management and Key Size.
- Weakness: The Initialization Vector (IV) is Too Small.
- Weakness: The Integrity Check Value (ICV) algorithm is not appropriate.
- Weakness: WEP's use of RC4 is weak.
- Weakness: Authentication Messages can be easily forged.

LECTURE

Network Architecture and Design

Wireless Local Area Networks

802.11i

- The first 802.11 wireless security standard
- Provides reasonable security
- Describes a Robust Security Network (RSN), which allows pluggable authentication modules
- RSN allows changes to cryptographic ciphers as new vulnerabilities are discovered
- RSN is also known as WPA2 (Wi-Fi Protected Access 2), a full implementation of 802.11i
- By default, WPA2 uses AES encryption to provide confidentiality, and CCMP (Counter Mode CBC MAC Protocol) to create a Message Integrity Check (MIC), which provides integrity
- WPA2 may (optionally) use the less secure RC4 (Rivest Cipher 4) and TKIP (Temporal Key Integrity Protocol) ciphers to provide confidentiality and integrity, respectively.

The less secure WPA (without the "2") was designed for access points that lack the power to implement the full 802.11i standard, providing a better security alternative to WEP. WPA uses RC4 for confidentiality and TKIP for integrity. Usage of WPA2 is recommended over WPA.

LECTURE

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

access
i standard,
s RC4 for

tion

ered

of

(Temporal Key Integrity Protocol) ciphers to provide confidentiality and integrity, respectively.

LECTURE

Network Architecture and Design

Wireless Local Area Networks

Bluetooth

- Described by IEEE standard 802.15
- A Personal Area Network (PAN) wireless technology, operating in the same 2.4 GHz frequency as many types of 802.11 wireless
- Can be used by small low-power devices such as cell phones to transmit data over short distances
- Versions 2.1 and older operate at 3 mbps or less; Versions 3 (announced in 2009) and higher offer far faster speeds

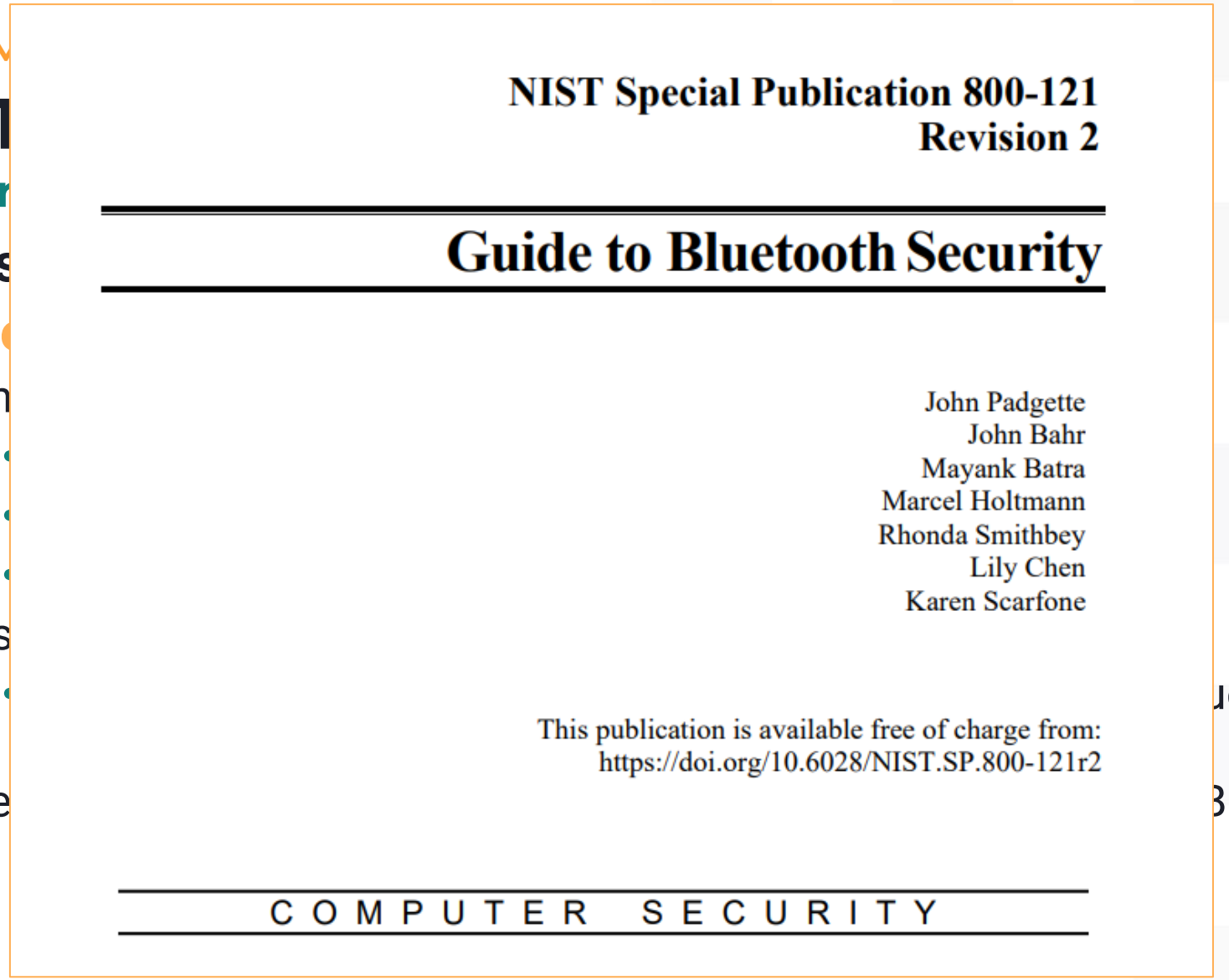
LECTURE

Network Architecture and Design

Wireless Local Area Networks

Bluetooth

- Three classes of devices
  - Class 3: under 10 meters
  - Class 2: 10 meters
  - Class 1: 100 meters
- Uses the 128-bit E0 symmetric stream cipher
  - Cryptanalysis has proven it to be weak; attacks show the true strength to be 38 bits or less
- Sensitive devices should disable automatic discovery by other Bluetooth devices



NIST Special Publication 800-121
Revision 2

Guide to Bluetooth Security

John Padgette
John Bahr
Mayank Batra
Marcel Holtmann
Rhonda Smithbey
Lily Chen
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-121r2

COMPUTER SECURITY

CISSP® M

LECT

Networ

Wireles

Blu

- Th
- Us
- Se

ue strength to be 38

Bluetooth devices

https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final

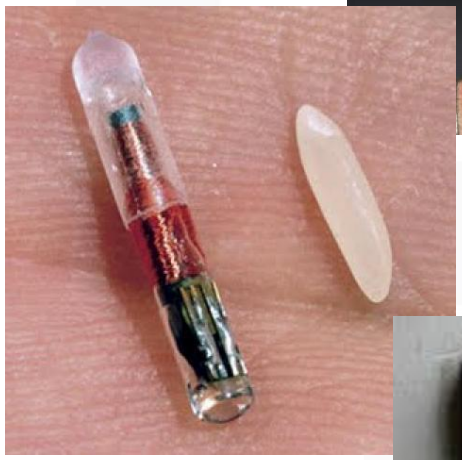
LECTURE

Network Architecture and Design

Wireless Local Area Networks

RFID

- Radio Frequency Identification (RFID)
- A technology used to create wirelessly readable tags for animals or objects
- There are three types of RFID tags…



LECTURE

Network Architecture and Design

Wireless Local Area Networks

RFID

- Radio Frequency Identification (RFID)
- A technology used to create wirelessly readable tags for animals or objects
- There are three types of RFID tags…
  - Active
    - Have a battery
    - An active tag broadcasts a signal
    - Can operate via larger distances
    - Devices like toll transponders
  - Semi-passive
    - Have a battery
    - Semi-passive RFID tags rely on a RFID reader's signal for power
  - Passive
    - Have no battery
    - Rely on the RFID reader's signal for power
    - Tracking inventory in a warehouse

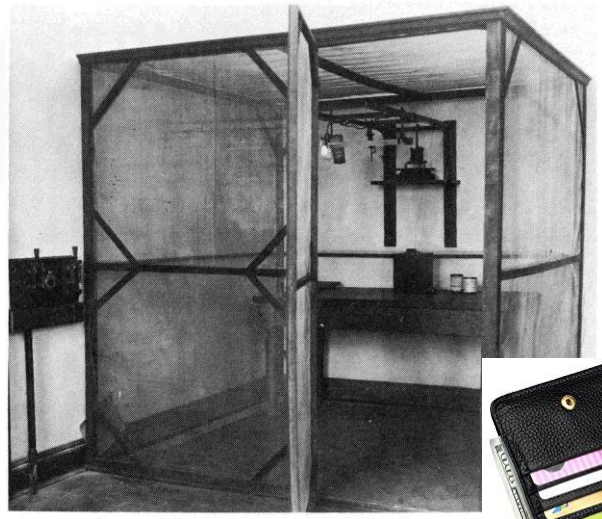
LECTURE

Network Architecture and Design

Wireless Local Area Networks

RFID

- Signals may be blocked with a Faraday Cage
- Cage can be as simple as aluminum foil wrapped around an object
- Instructions for building a Faraday Cage wallet (designed to protect smart cards with RFID chips) from aluminum foil and duct tape are available at: http://howto.wired.com/wiki/Make_a_Faraday_Cage_Wallet



LECTURE

Network Architecture and Design

Network devices and protocols

Repeaters and Hubs

- Layer 1 devices
- Repeater receives bits on one port, and “repeats” them out the other port
- Repeater has no understanding of protocols; it only repeats bits
- Repeaters are often used to extend the length of a network
- A hub is a repeater with more than two ports
- Hubs receive bits on one port and repeat them across all other ports
- No traffic isolation and no security: all nodes see all traffic sent by the hub
- Half-duplex devices: they cannot send and receive simultaneously
- One “**collision domain**”: any node may send colliding traffic with another
- Unsuitable for most modern purposes

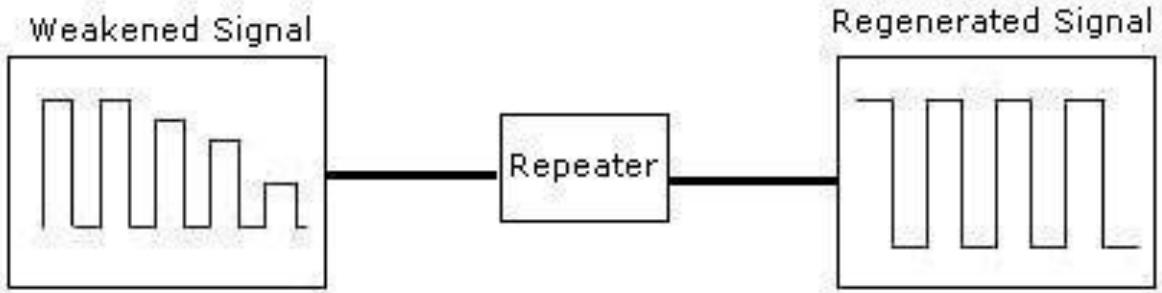
LECTURE

Network Architecture and Design

Network devices and protocols

Repeaters and Hubs

- Layer 1 devices
- Repeater receives bits on one port, and “repeats” them out the other port
- Repeater h its
- Repeaters
- A hub is a
- Hubs rece er ports
- No traffic nt by the hub
- Half-duple ously
- One “collision domain”: any node may send colliding traffic with another
- Unsuitable for most modern purposes



LECTURE

Network Architecture and Design

Network devices and protocols

Bridges

- Layer 2 devices
- Has two ports and connects network segments together
- Provides traffic isolation and makes forwarding decisions by learning the MAC addresses of connected nodes.
- **Two collision domains**

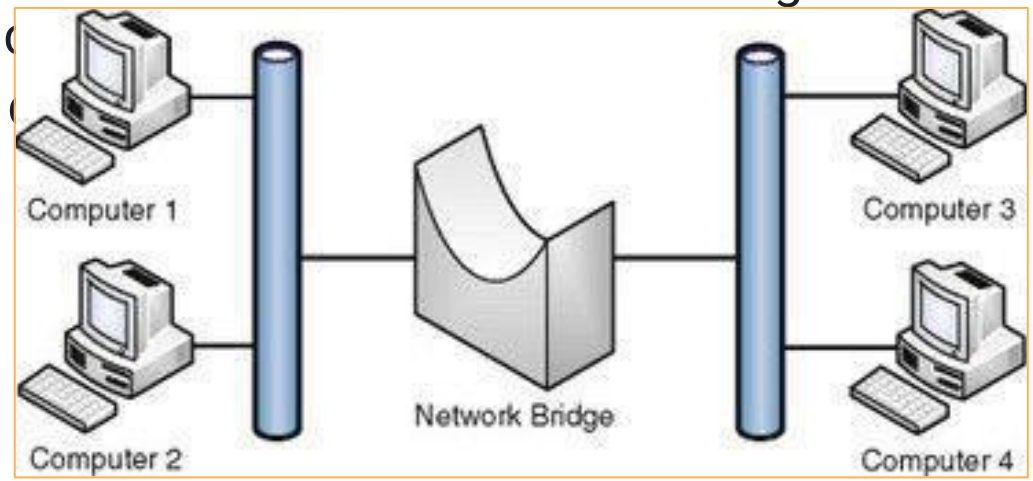
LECTURE

Network Architecture and Design

Network devices and protocols

Bridges

- Layer 2 devices
- Has two ports and connects network segments together
- Provides traffic isolation and makes forwarding decisions by learning the MAC addresses of
- Two collision



LECTURE

Network Architecture and Design

Network devices and protocols

Switches

- A bridge with more than two ports
- Best practice to only connect one device per switch port
- Provides traffic isolation by associating the MAC address of each computer and server with its port
- Shrinks the **collision domain to a single port**
- Trunks are used to connect multiple switches

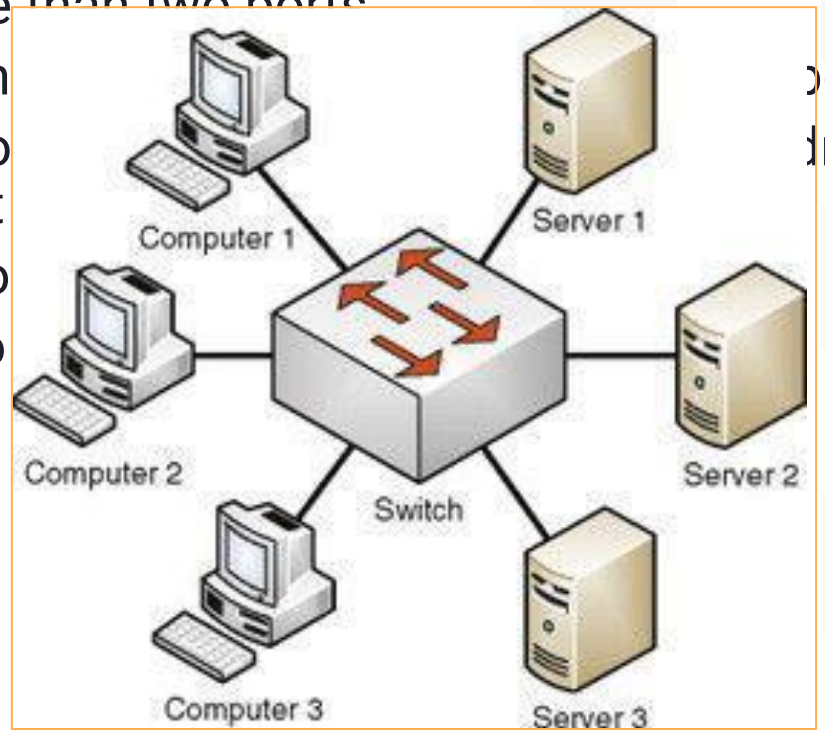
LECTURE

Network Architecture and Design

Network devices and protocols

Switches

- A bridge with more than two ports
- Best practice to on ort
- Provides traffic iso dress of each computer and server with its port
- Shrinks the collisio
- Trunks are used to



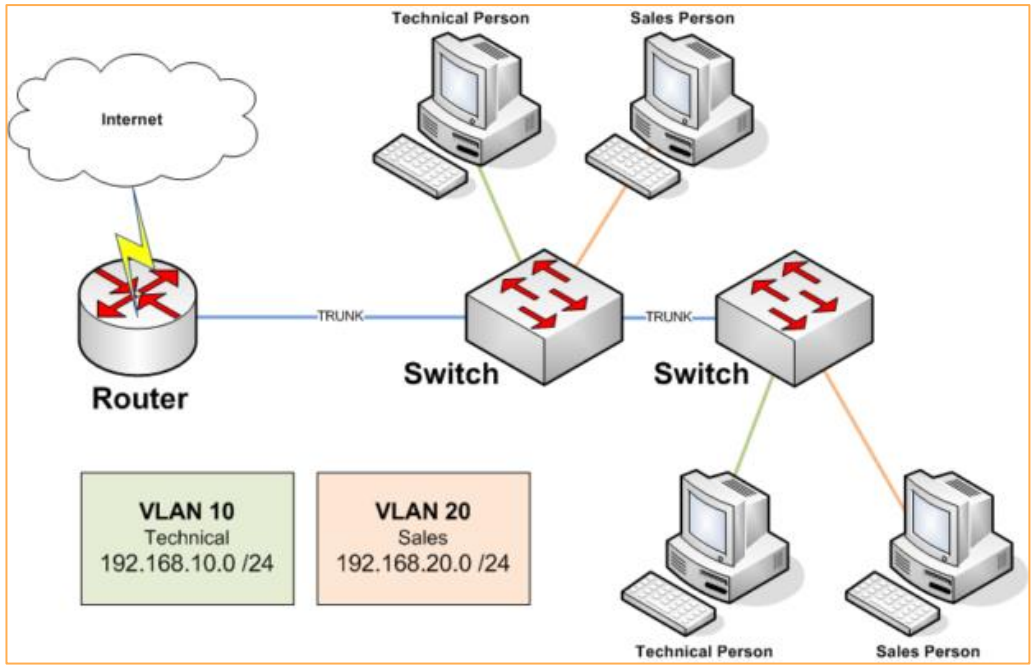
LECTURE

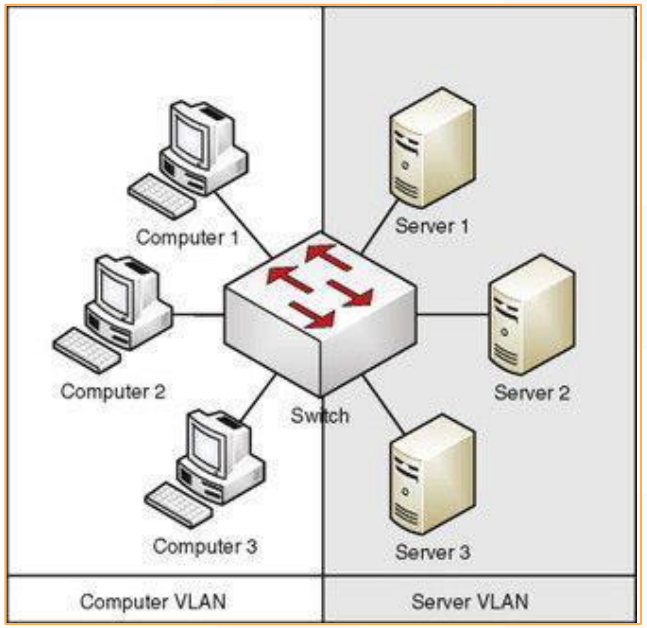
Network Architecture and Design

Network devices and protocols

Switches (VLANs)

- Virtual LAN, which can be thought of as a virtual switch
- Inter-VLAN communication requires layer 3 routing.





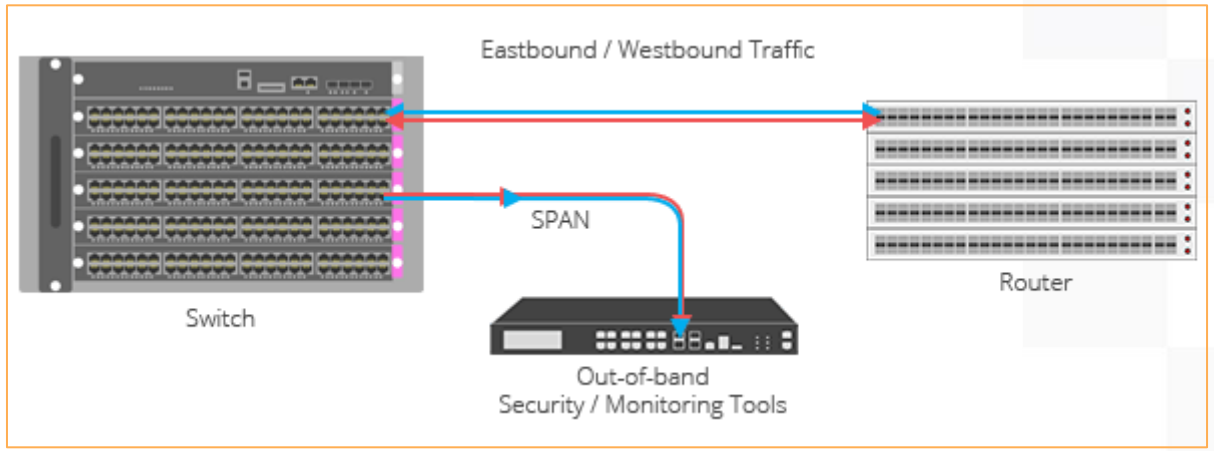
LECTURE

Network Architecture and Design

Network devices and protocols

Switches (SPAN ports)

- Mirroring traffic from multiple switch ports to one “SPAN port”
- SPAN is a Cisco term; HP switches use the term “Mirror port”
- Typically used for Intrusion Detection and/or Prevention
- One drawback to using a switch SPAN port is port bandwidth overload



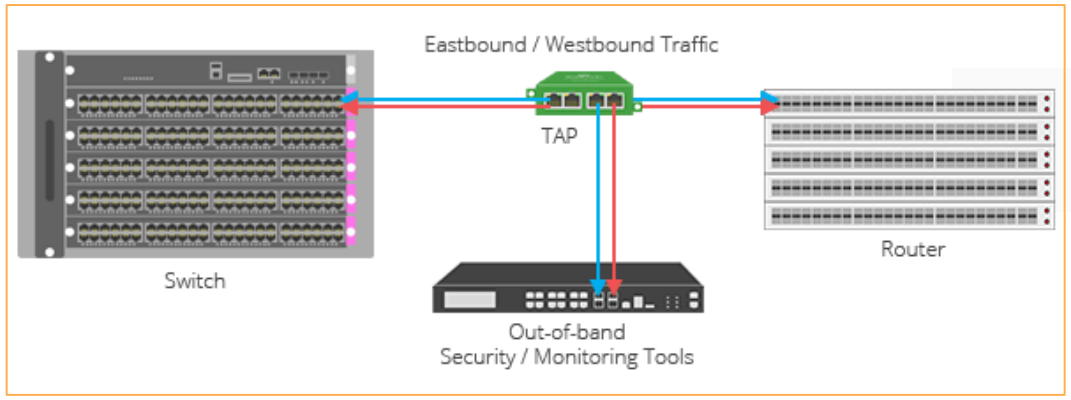
LECTURE

Network Architecture and Design

Network devices and protocols

Switches (TAPs)

- "Test Access Port"
- Provides a way to "tap" into network traffic, and see all unicast streams on a network
- The preferred way to provide promiscuous network access to a sniffer or Networked Intrusion Detection System.
- Can "fail open," so that network traffic will pass in the event of a failure: this is not true for hubs or switch SPAN ports



LECTURE

Network Architecture and Design

Network devices and protocols

Routers

- Layer 3 devices
- Route traffic from one LAN to another
- IP-based routers make routing decisions based on the source and destination IP addresses.

NOTE: In the real world, one chassis, such as a Cisco 6500, can be many devices at once: a router, a switch, a firewall, a NIDS, etc. The exam is likely to give more clear-cut examples: a dedicated firewall, a dedicated switch, etc. If the exam references a multifunction device, that will be made clear. Regardless, it is helpful on the exam to think of these devices as distinct concepts.

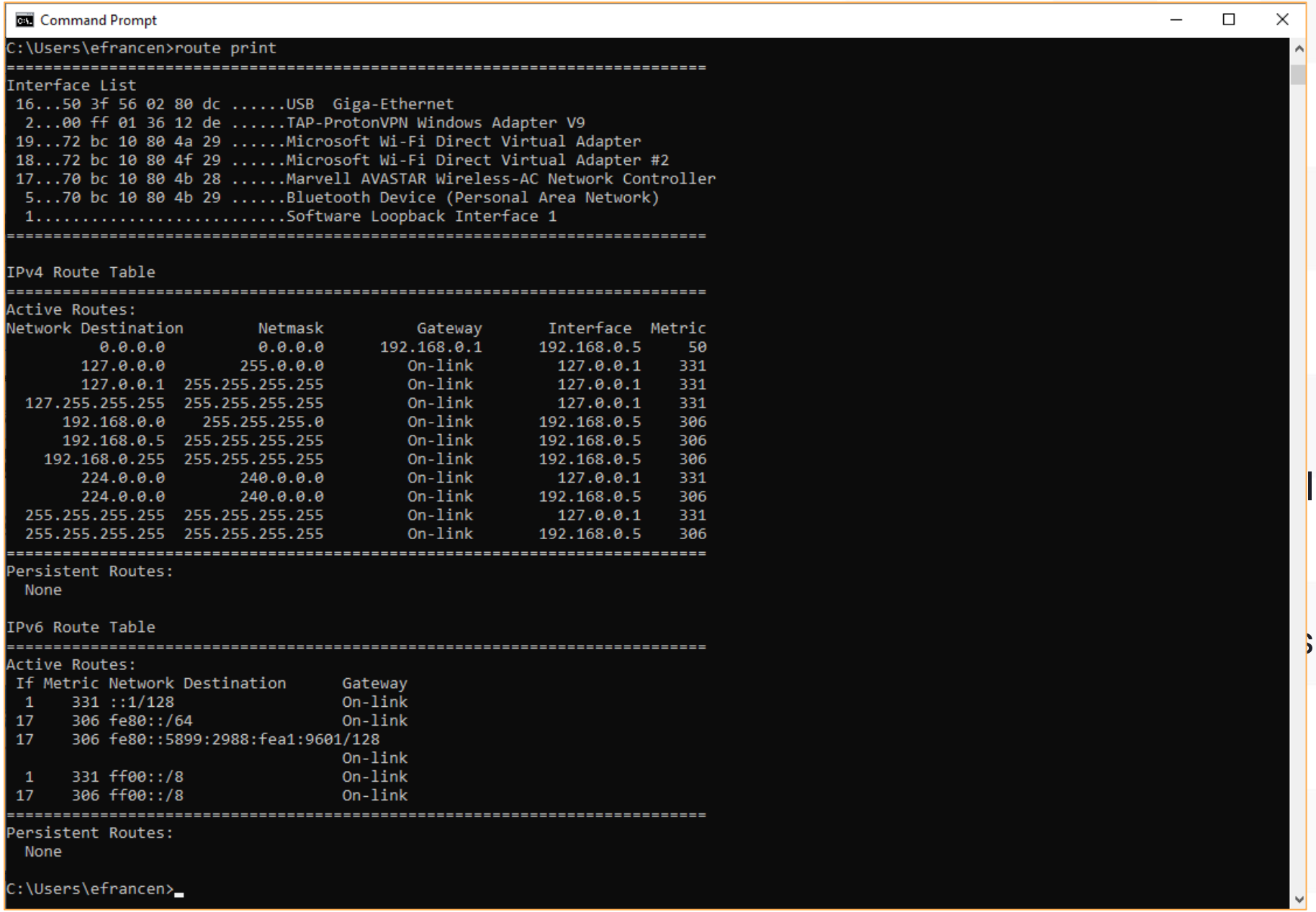
LECTURE

Network Architecture and Design

Network devices and protocols

Routers (Static and Default Routes)

- Static routes
  - Routes to other networks
  - Manually entered into the routing table
  - Good for simple routing needs and fixed networks with little or no redundancy
- Default routes
  - A route to other networks that are not known.
  - If no other routes to a network exist, the default route is used.



le or no redundancy

sed.

Command Prompt

```
C:\Users\efrancen>route print
===========================================================================
Interface List
 16...50 3f 56 02 80 dc ......USB  Giga-Ethernet
  2...00 ff 01 36 12 de ......TAP-ProtonVPN Windows Adapter V9
 19...72 bc 10 80 4a 29 ......Microsoft Wi-Fi Direct Virtual Adapter
 18...72 bc 10 80 4f 29 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 17...70 bc 10 80 4b 28 ......Marvell AVASTAR Wireless-AC Network Controlle
  5...70 bc 10 80 4b 29 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1      192.168.0.5     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link       192.168.0.5    306
      192.168.0.5  255.255.255.255         On-link       192.168.0.5    306
    192.168.0.255  255.255.255.255         On-link       192.168.0.5    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       192.168.0.5    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       192.168.0.5    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 17    306 fe80::/64                On-link
 17    306 fe80::5899:2988:fea1:9601/128
                                    On-link
  1    331 ff00::/8                 On-link
 17    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\Users\efrancen>
```

Administrator: Command Prompt

```
C:\WINDOWS\system32>route add 0.0.0.0 mask 0.0.0.0 192.168.0.2
 OK!

C:\WINDOWS\system32>route print
===========================================================================
Interface List
 16...50 3f 56 02 80 dc ......USB  Giga-Ethernet
  2...00 ff 01 36 12 de ......TAP-ProtonVPN Windows Adapter V9
 19...72 bc 10 80 4a 29 ......Microsoft Wi-Fi Direct Virtual Adapter
 18...72 bc 10 80 4f 29 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 17...70 bc 10 80 4b 28 ......Marvell AVASTAR Wireless-AC Network Controller
  5...70 bc 10 80 4b 29 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1      192.168.0.5     50
          0.0.0.0          0.0.0.0      192.168.0.2      192.168.0.5     51
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link       192.168.0.5    306
      192.168.0.5  255.255.255.255         On-link       192.168.0.5    306
    192.168.0.255  255.255.255.255         On-link       192.168.0.5    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       192.168.0.5    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       192.168.0.5    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 17    306 fe80::/64                On-link
 17    306 fe80::5899:2988:fea1:9601/128
                                    On-link
  1    331 ff00::/8                 On-link
 17    306 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\WINDOWS\system32>
```

LECTURE

Network Architecture and Design

Network devices and protocols

Routing Protocols

- Automatic routing based upon the protocol used.
- **Convergence** – when all the routers are in agreement on the state of routing (routing tables are in sync and/or topology is set).
- **Interior Gateway Protocols (IGP)** – Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP)
- **Exterior Gateway Protocols (EGP)** – Border Gateway Protocol (BGP) is king.

LECTURE

Network Architecture and Design

Network devices and protocols

Routers (Distance Vector Routing Protocols)

- Metrics are used to determine the “best” route across a network
- Simplest metric is hop count – number of routers to a destination network
- Does not account for link speed between networks
- Prone to routing loops

LECTURE

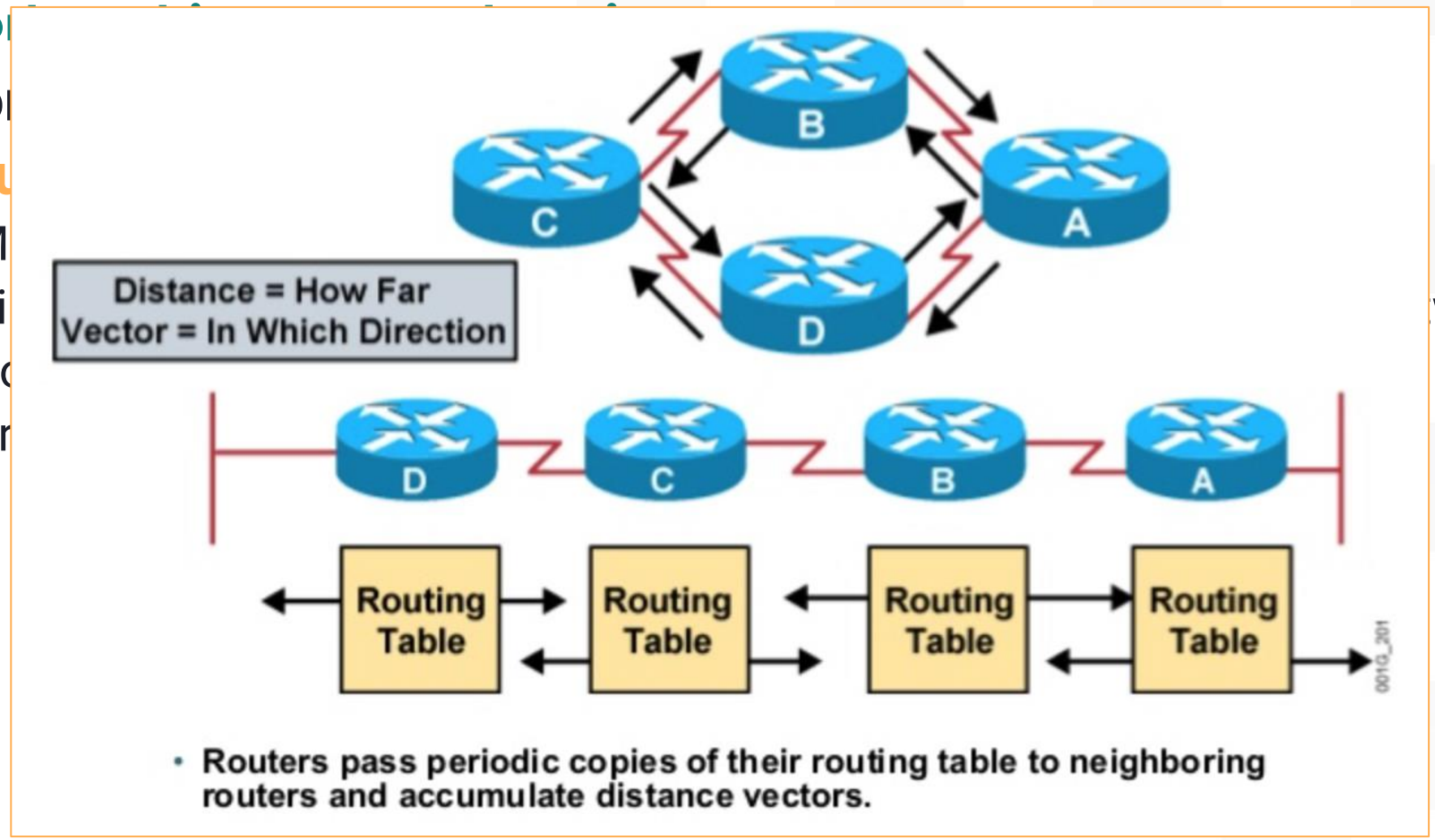
Netwo

Netwo

Rou

- M
- Si
- Dc
- Pr

work



LECTURE

Network Architecture and Design

Network devices and protocols

Routing Information Protocol (RIP)

- A distance vector routing protocol
- Uses hop count as its metric
- Does not have a full view of a network: it can only “see” directly connected routers
- Convergence is slow
- Sends routing updates every 30 seconds, regardless of routing changes
- Maximum hop count is 15; 16 is considered “infinite.”
- RIPv1 can route classful networks only
- RIPv2 added support for CIDR
- Uses split horizon to help avoid routing loops - means that a router will not “argue back”
- Uses a hold-down timer to avoid “flapping” (repeatedly changing a route’s status from up to down)

LECTURE

Netwo

Netwo

Ro

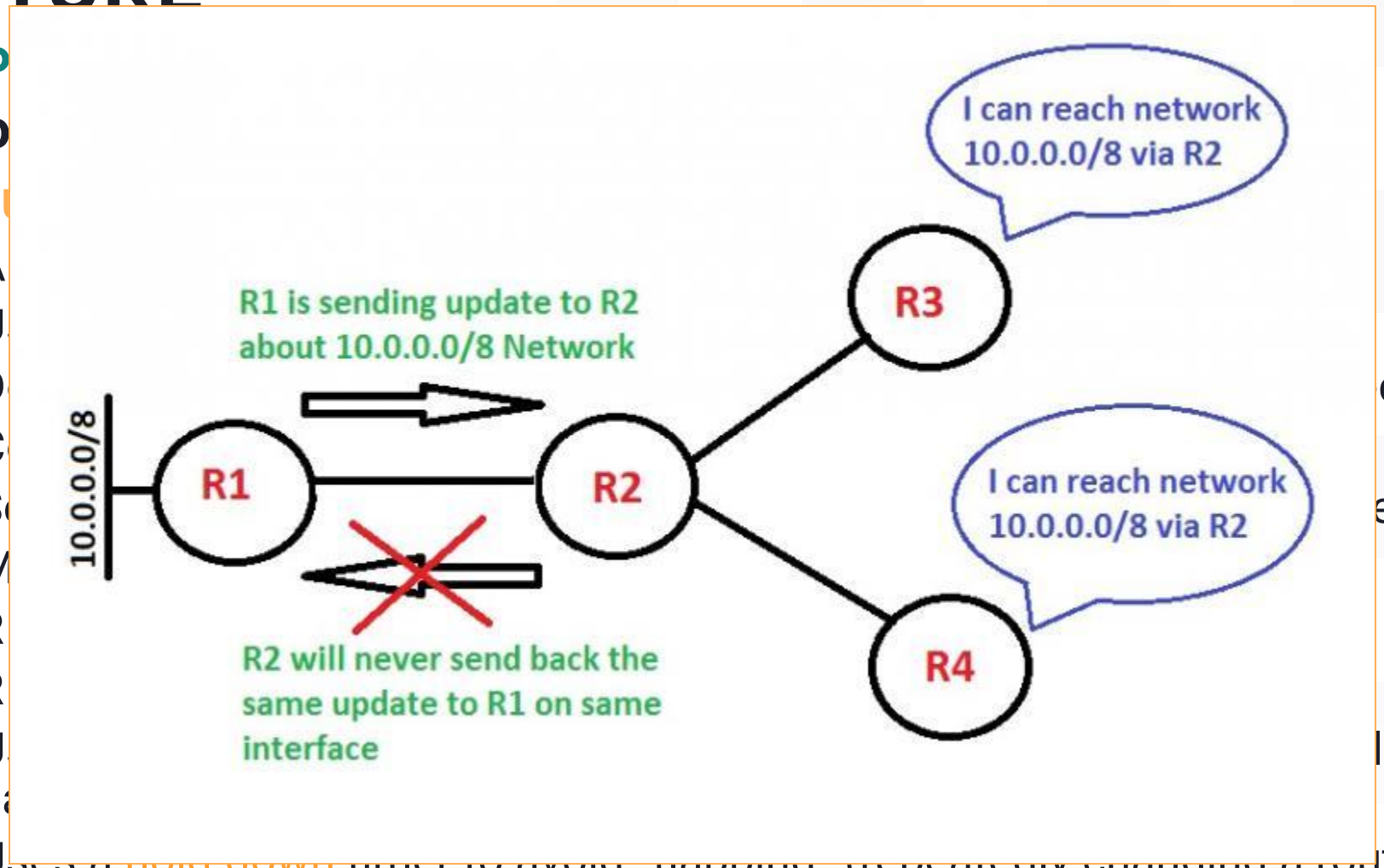
- A
- U
- D
- C
- S
- M
- R
- R
- U
- U

cted routers

es

ll not “argue

te’s status



from up to down)

LECTURE

Network Architecture and Design

Network devices and protocols

Routing Protocols

- Automatic routing based upon the protocol used.
- Link State Routing Protocols – additional metrics for determining best route.
  - OSPF is an example.
  - Can use bandwidth, congestion, and other metrics for routing decisions.

Distance vector	Link state
sends the entire routing table	sends only link state information
slow convergence	fast convergence
susceptible to routing loops	less susceptible to routing loops
updates are sometimes sent using broadcast	always uses multicast for the routing updates
doesn't know the network topology	knows the entire network topology
simpler to configure	can be harder to configure
examples: RIP, IGRP	examples: OSPF, IS-IS

LECTURE

Network Architecture and Design

Network devices and protocols

Routers (OSPF)

- OSPF
  - Open Shortest Path First (OSPF)
  - An open link state routing protocol
- Routers learn the entire network topology for their “area” (the portion of the network they maintain routes for, usually the entire network for small networks)
- Routers send event-driven updates
- Far faster convergence than distance vector protocols such as RIP

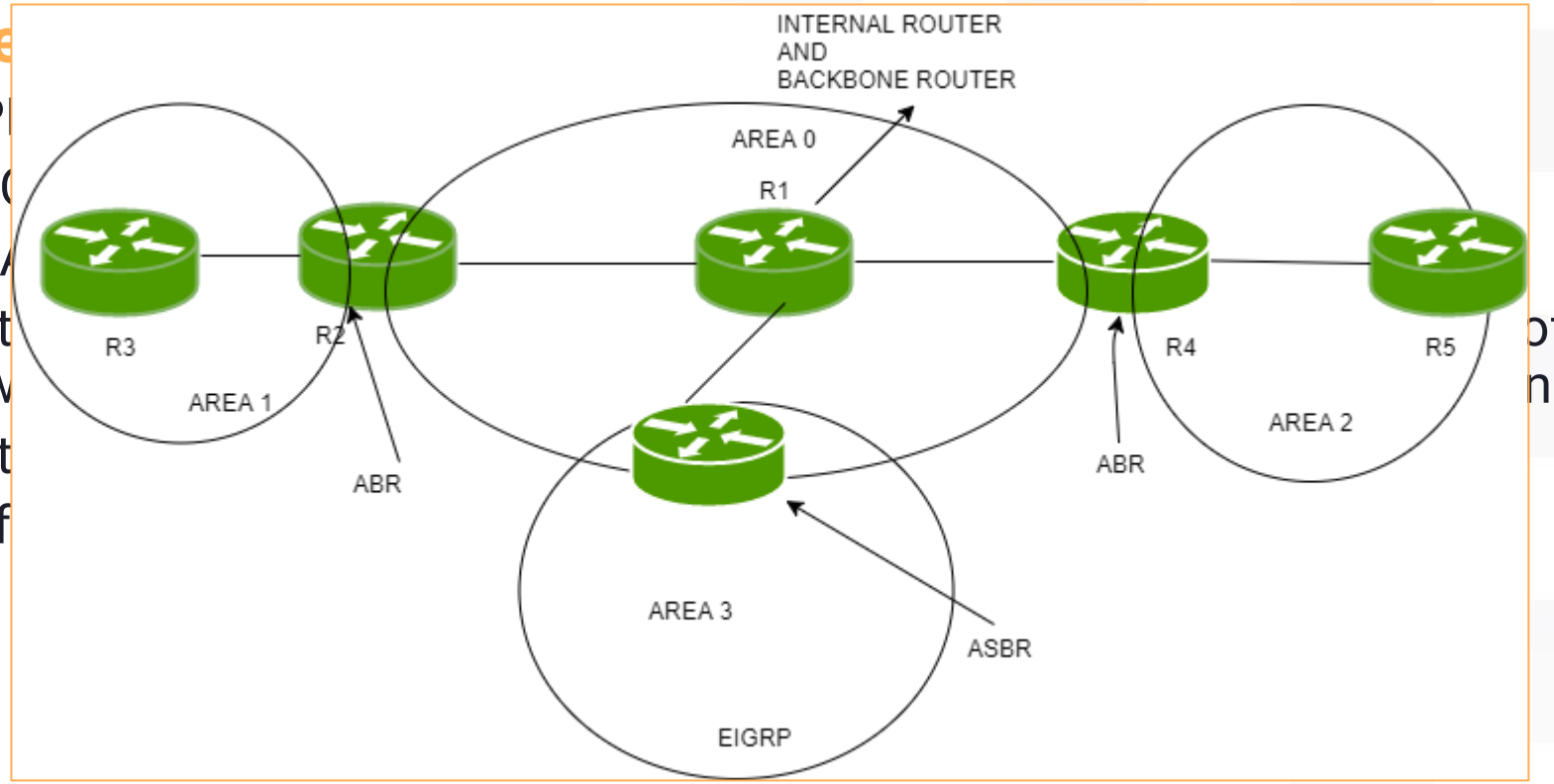
LECTURE

Network Architecture and Design

Network devices and protocols

Route

- OSPF
  - (
  - A
- Rout
  netw
- Rout
- Far f



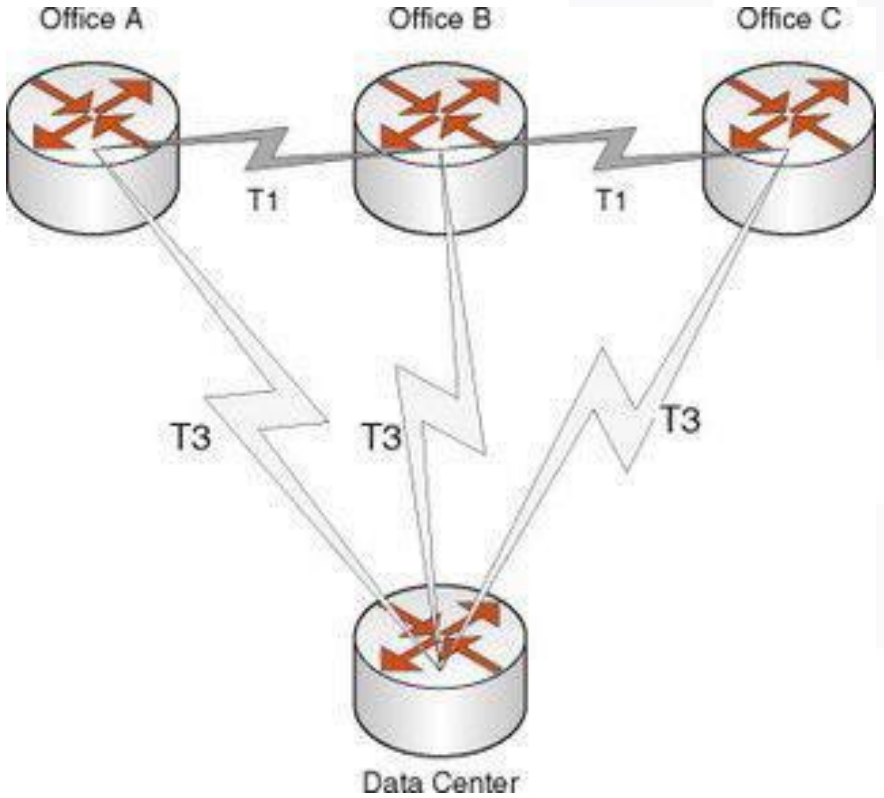
of the
networks)

LECTURE

Network Architecture and Design

Network devices and protocols

Routers (Static and Default Routes)



LECTURE

Network Architecture and Design

Note - The exam strongly prefers open over proprietary standards, which is why proprietary routing protocols like Cisco's EIGRP are not covered.

Network devices and protocols

Routers (BGP)

- Border Gateway Protocol; there's IBGP and EBGP.
- The routing protocol used on the Internet
- Routes between autonomous systems, which are networks with multiple Internet connections
- Has some distance vector properties, but is formally considered a path vector routing protocol
- As described in RFC4271 and ratified in 2006, the current version of BGP-4 supports both IPv6 and Classless Inter-Domain Routing (CIDR).
- Uses TCP port 179 for communications with other routers.

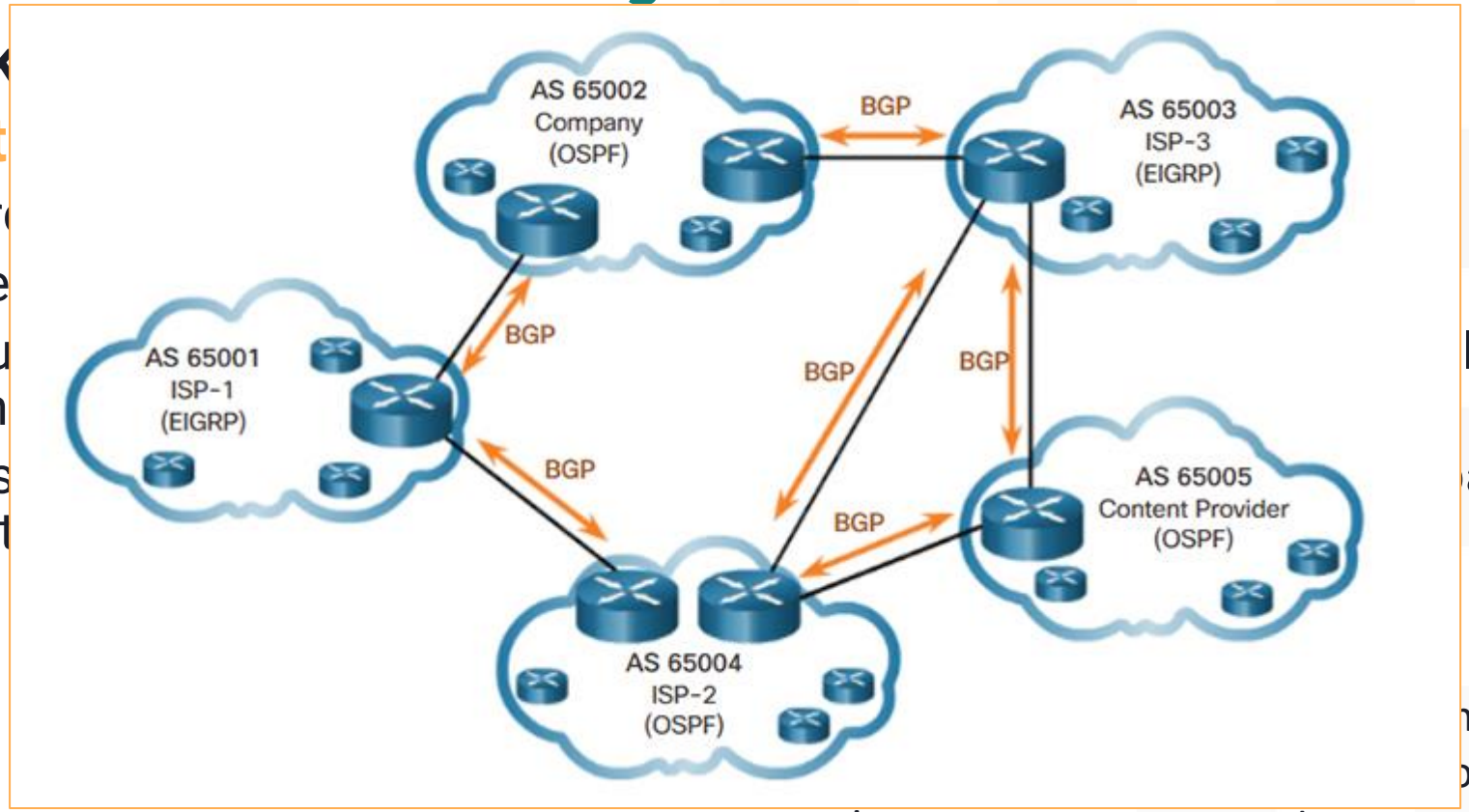
LECTURE

Network Architecture and Design

Network

Rout

- Bor
- The
- Rou
  con
- Has
  rout



ltiple Internet

ath vector

n over proprietary
outing protocols like Cisco's EIGRP are not covered.

LECTURE

Network Architecture and Design

Network devices and protocols

Firewalls

- Filter traffic between networks
- TCP/IP packet filter and stateful firewalls make decisions based on layers 3 and 4 (IP addresses and ports)
- Proxy firewalls can also make decisions based on layers 5-7
- Firewalls are multi-homed: they have multiple NICs connected to multiple different networks

LECTURE

Network Architecture and Design

Network devices and protocols

Firewalls

- Filter traffic bet
- TCP/IP packet f based on layers 3 and 4 (IP addresses a
- Proxy firewalls 5-7
- Firewalls are mu cted to multiple different networks

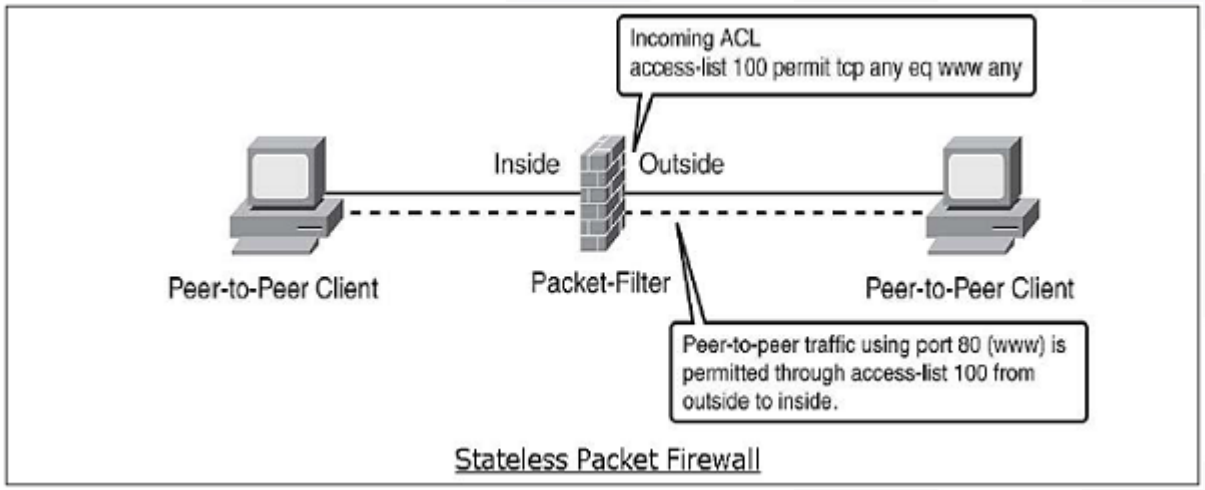
LECTURE

Network Architecture and Design

Network devices and protocols

Firewalls (Packet Filter)

- A simple and fast firewall
- No concept of “state”: each filtering decision must be made on the basis of a single packet
- No way to refer to past packets to make current decisions
- Lack of state makes packet filter firewalls less secure, especially for session less protocols like UDP and ICMP



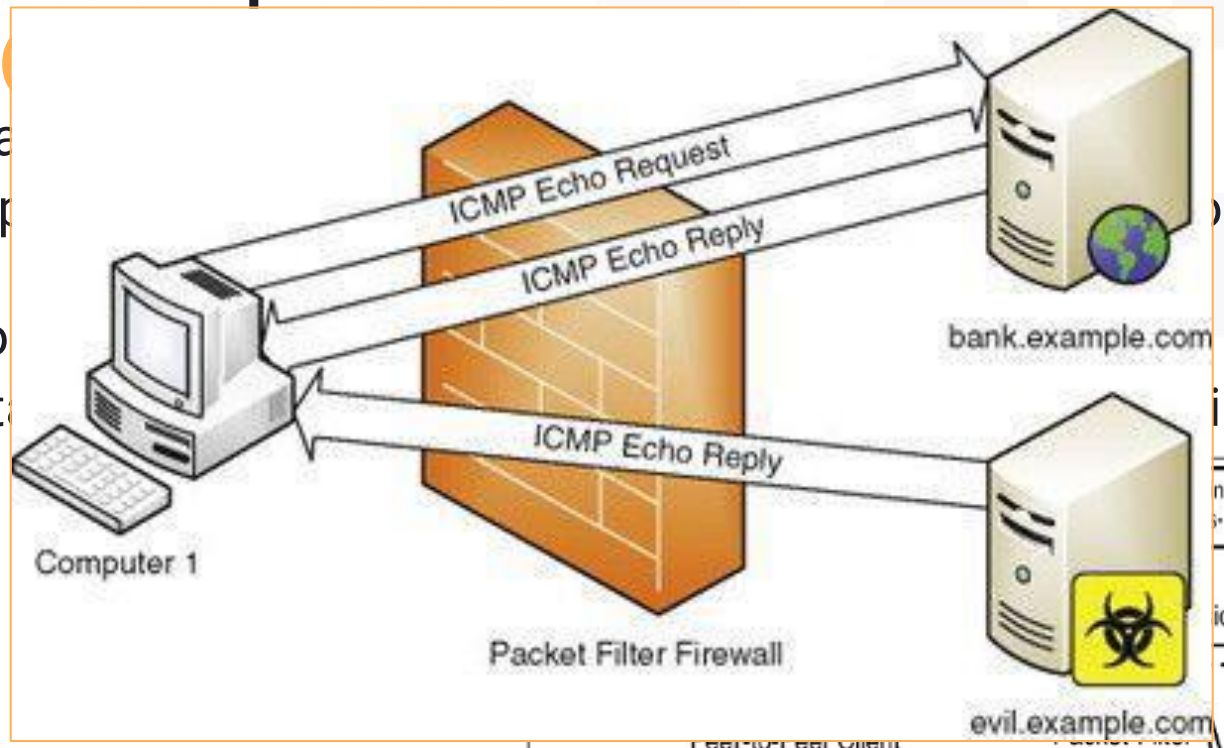
LECTURE

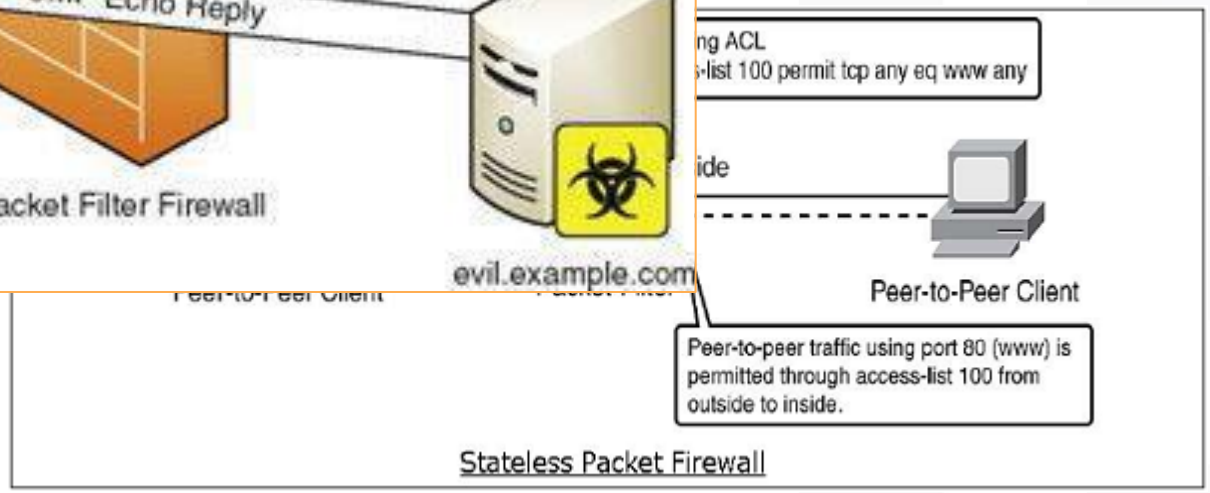
Network Architecture and Design

Network devices and protocols

Firewalls (

- A simple a
- No concep on the basis of a single packet
- No way to
- Lack of st ially for session less protocols





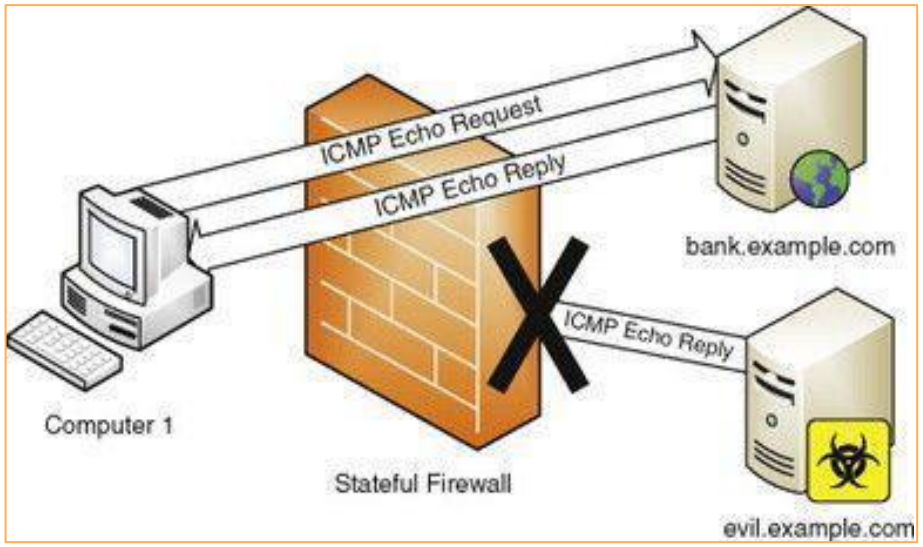
LECTURE

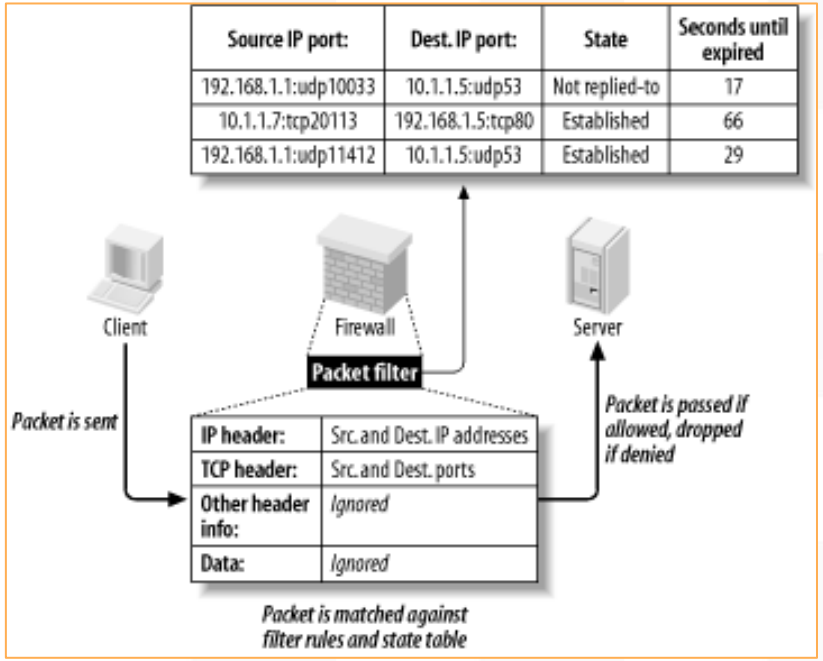
Network Architecture and Design

Network devices and protocols

Firewalls (Stateful)

- A state table that allows the firewall to compare current packets to previous ones
- Slower than packet filters, but are far more secure





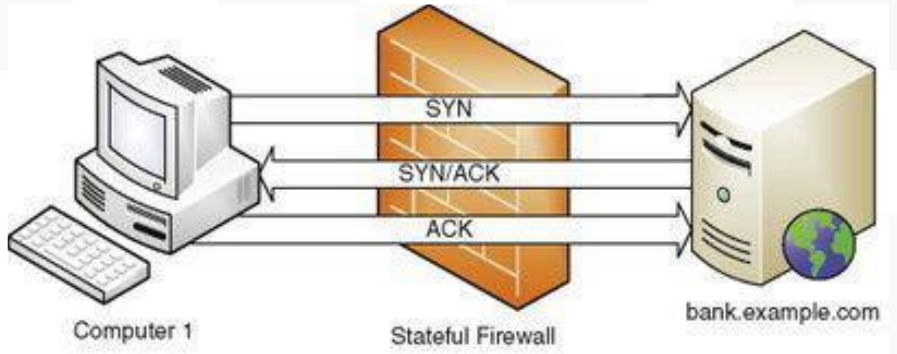
LECTURE

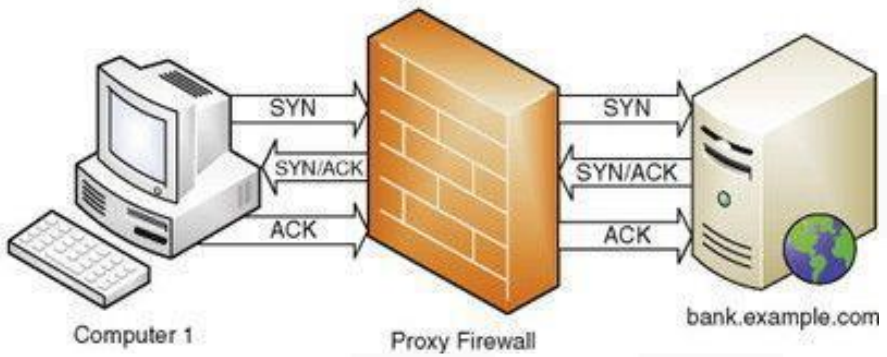
Network Architecture and Design

Network devices and protocols

Proxy Firewalls

- Firewalls that act as intermediary servers
- Proxies terminate connections





LECTURE

Network Architecture and Design

Network devices and protocols

Proxy Firewalls

Application-Layer Proxy Firewalls

- Operate up to Layer 7
- Can make filtering decisions based on application-layer data, such as HTTP traffic, in addition to layers 3 and 4
- Must understand the protocol that is proxied, so dedicated proxies are often required for each protocol: an FTP proxy for FTP traffic, an HTTP proxy for Web traffic, etc.
- Allows tighter control of filtering decisions

LECTURE

Network Architecture and Design

Network devices and protocols

Proxy Firewalls

Circuit-Level Proxies Including SOCKS

- Operate at Layer 5 (session layer) - allows circuit-level proxies to filter more protocols: there is no need to understand each protocol; the application-layer data is simply passed along
- Most popular example of a circuit-level proxy is SOCKS
  - SOCKS uses TCP port 1080
  - Some applications must be “socksified” to pass via a SOCKS proxy
  - SOCKS5 is current version of the protocol
- Cannot make filtering decisions based on application layer data, such as explicit Web content

LECTUR

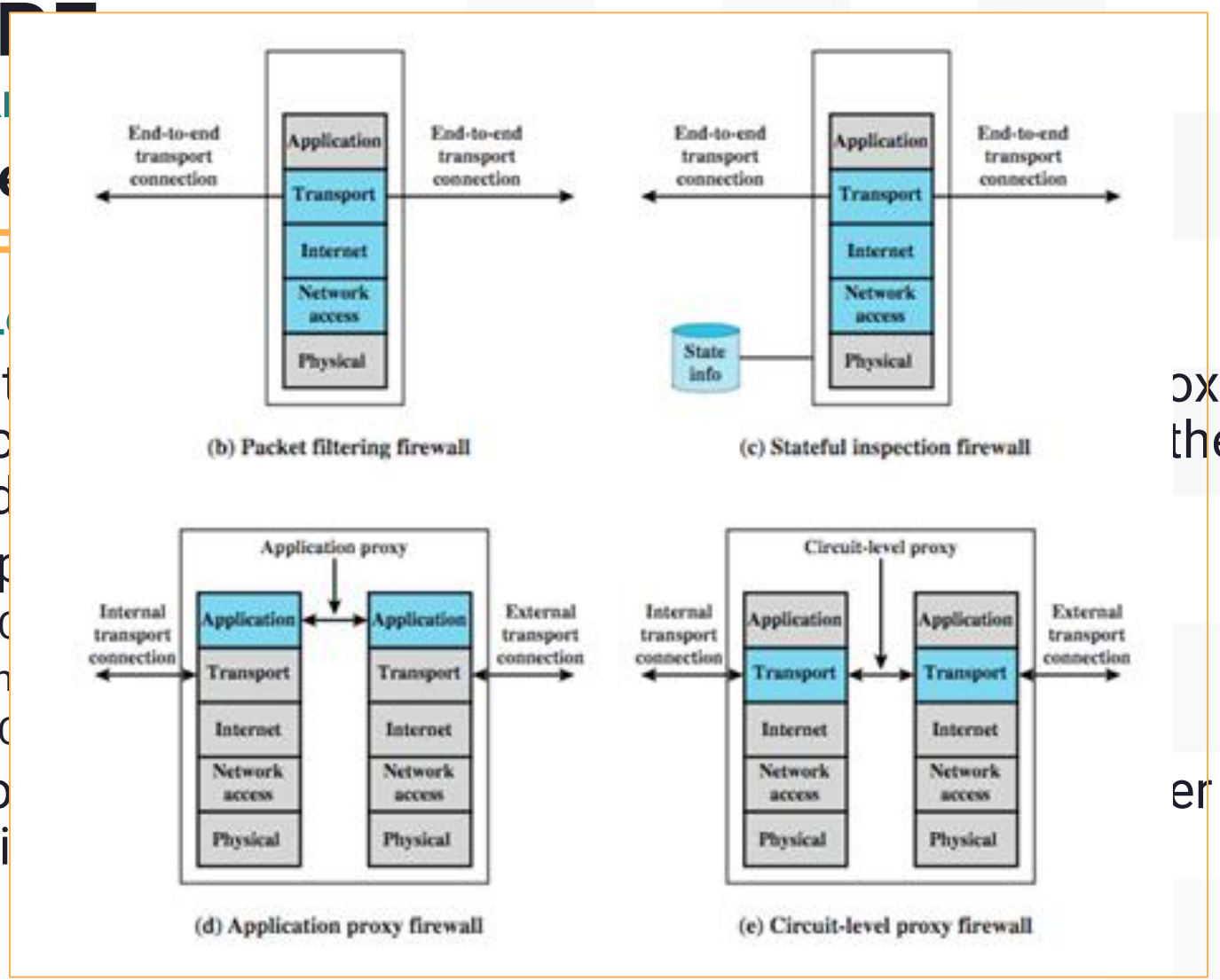
Network A

Network de

Proxy F

Circuit-L

- Operat oxies to filter more protoc the application-layer d
- Most p
  - soc
  - Son
  - soc
- Canno er data, such as explici



LECTURE

Network Architecture and Design

Network devices and protocols

Fundamental Firewall Designs –

Dual-Homed Host

- Two network interfaces: one connected to a trusted network, and the other connected to an untrusted network, such as the Internet
- Host does not route: a user wishing to access the trusted network from the Internet, would log into the dual-homed host first, and then access the trusted network from there
- Common design before modern firewalls in the 1990s

LECTURE

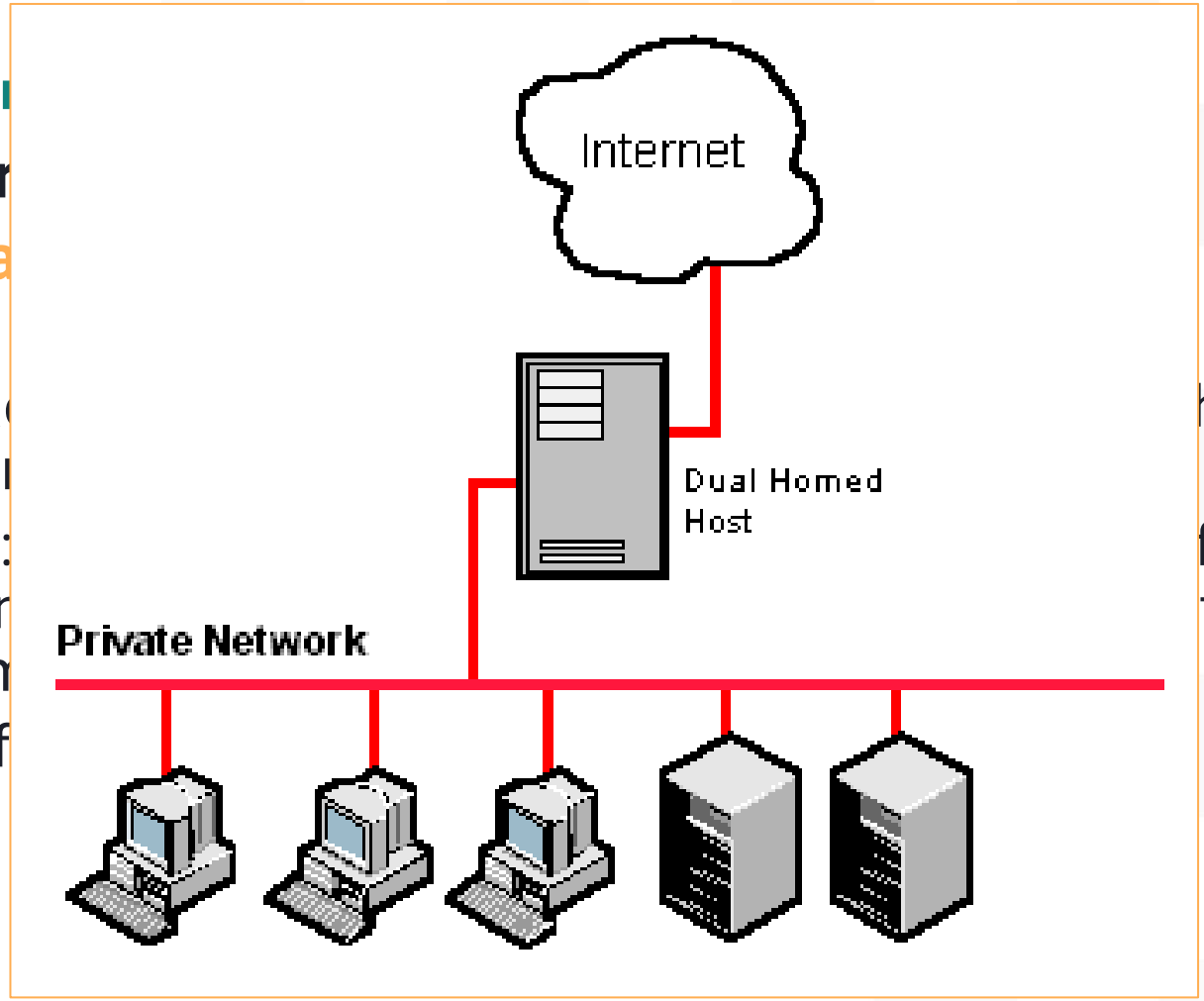
Network Architecture a

Network devices and pr

Fundamental Firewa

Dual-Homed Host

- Two network interfa he other connected to an untr
- Host does not route: from the Internet, would log ir the trusted network from
- Common design bef



LECTURE

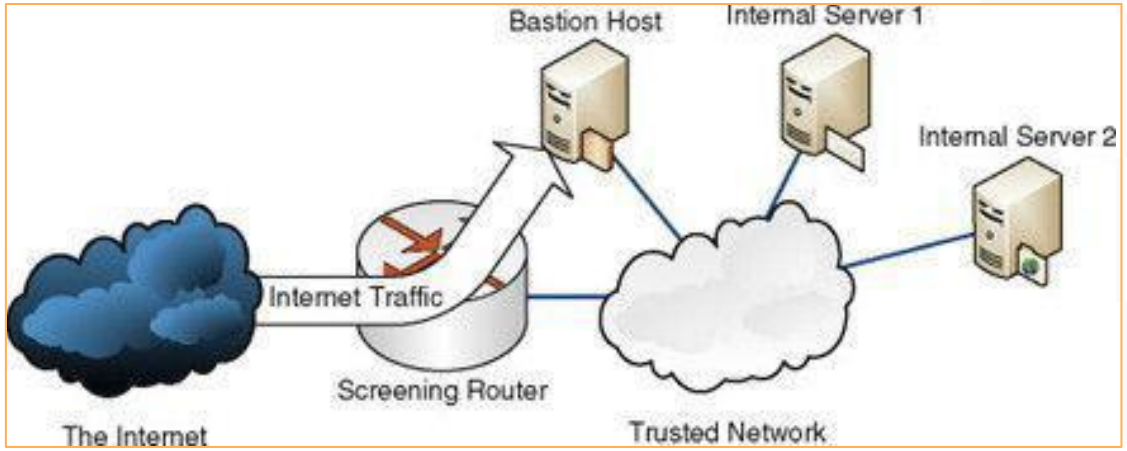
Network Architecture and Design

Network devices and protocols

Fundamental Firewall Designs –

Screened Host Architecture

- An older flat network design using one router to filter external traffic to and from a bastion host via an access control list (ACL)
- The bastion host can reach other internal resources, but the router ACL forbids direct internal/external connectivity



LECTURE

Network Architecture and Design

Network devices and protocols

Fundamental Firewall Designs –

DMZ Networks and Screened Subnet Architecture

- An older flat network design using one router to filter external traffic to and from a bastion host via an access control list (ACL)
- The bastion host can reach other internal resources, but the router ACL forbids direct internal/external connectivity

LECTURE

Network Architecture and Design

Network devices and protocols

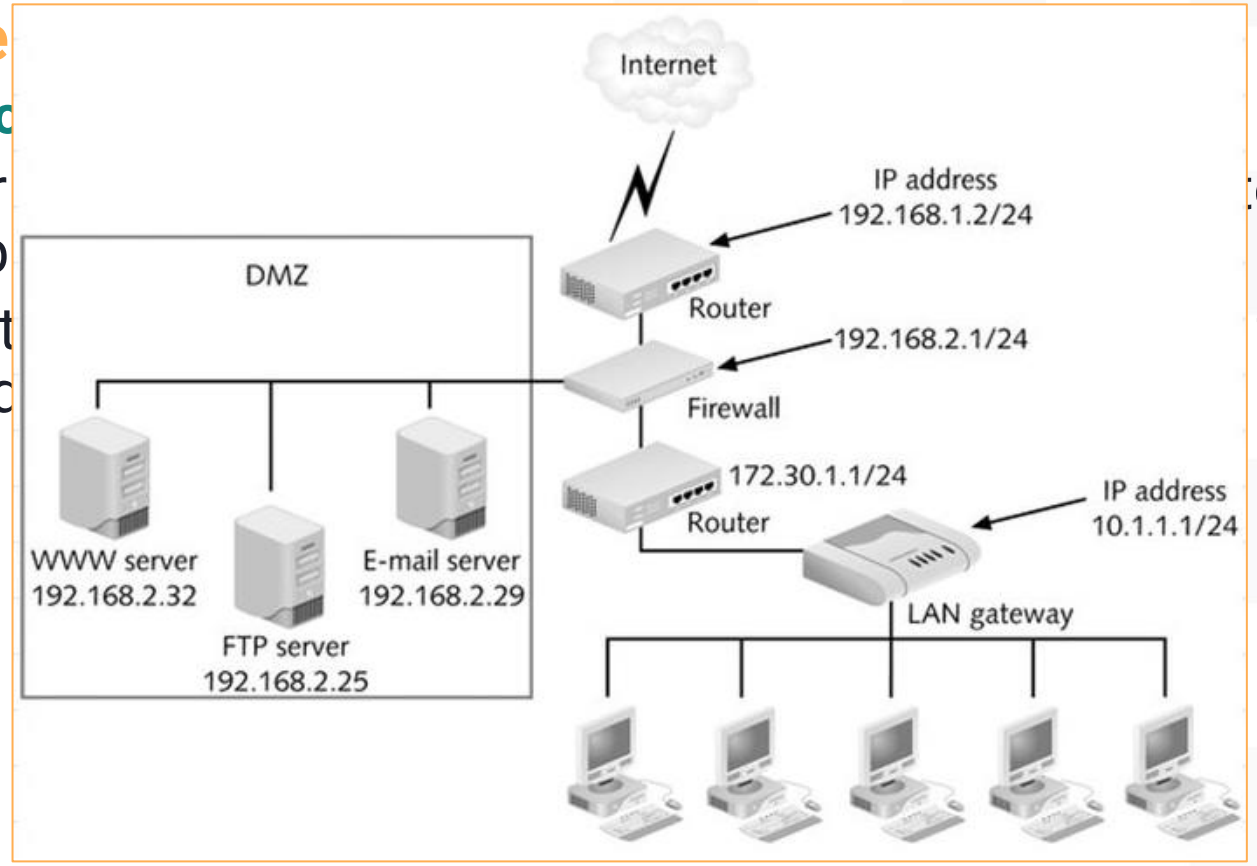
Fundame

DMZ Netwo

- An older
- The bast

ternal traffic to and from a b

the router ACL forbids c



LECTURE

Network Architecture and Design

Network devices and protocols

Fundamental Firewall Designs –

DMZ Networks and Screened Subnet Architecture

- DMZ is “Demilitarized Zone” network
- Hosts that receive traffic from untrusted networks such as the Internet should be placed on DMZ networks
- Designed with the assumption that any DMZ host may be compromised: the DMZ is designed to contain the compromise, and prevent it from extending into internal trusted networks
- Hosts on a DMZ should be hardened

LECTURE

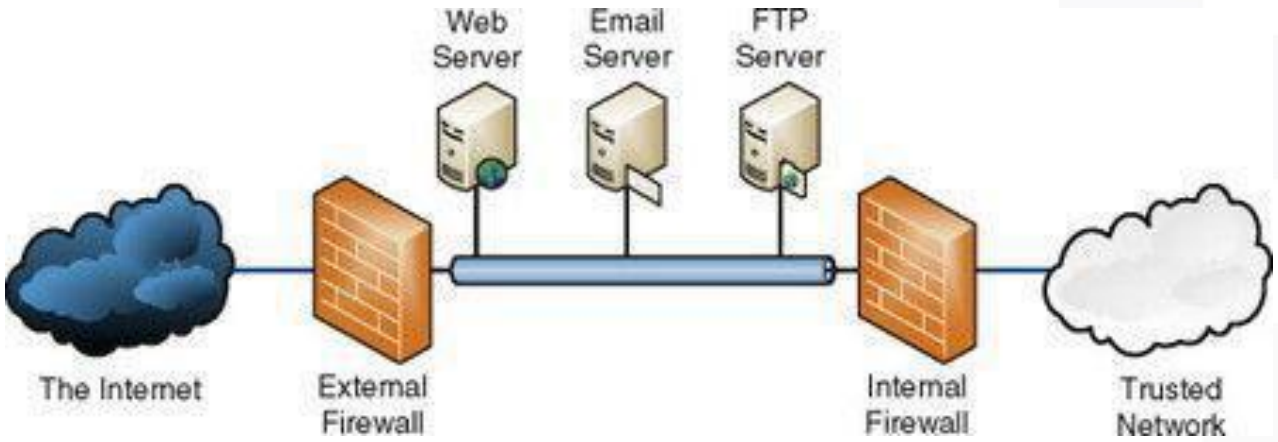
Network Architecture and Design

Network devices and protocols

Fundamental Firewall Designs –

DMZ Networks and Screened Subnet Architecture

A “classic” DMZ uses two firewalls (shown below) - called a screened subnet dual firewall design: two firewalls screen the DMZ subnet.



LECTURE

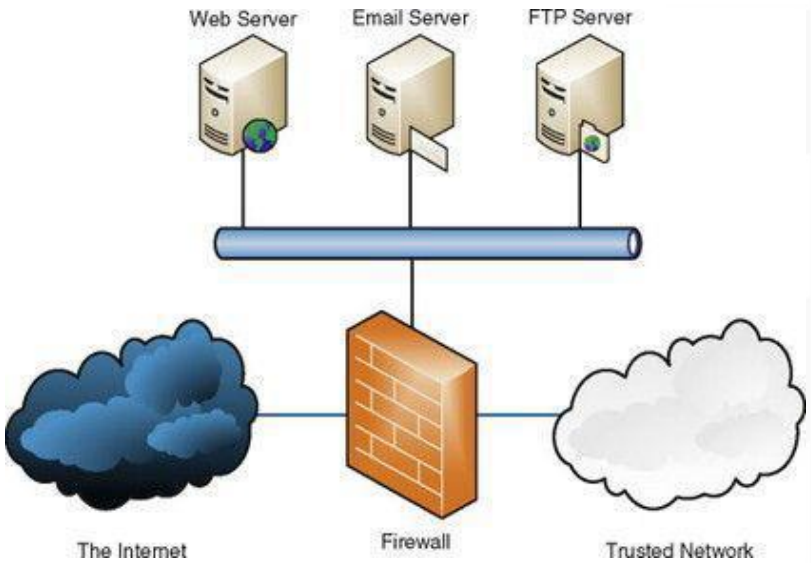
Network Architecture and Design

Network devices and protocols

Fundamental Firewall Designs –

DMZ Networks and Screened Subnet Architecture

A single-firewall DMZ uses one firewall (shown at side) - sometimes called a “three-legged” DMZ.



LECTURE

Network Architecture and Design

Network devices and protocols

Fundamental Firewall Designs –

DMZ Networks and Screened Subnet Architecture

- Single firewall design requires a firewall that can filter traffic on all interfaces: untrusted, trusted, and DMZ
- Dual-firewall designs are more complex, but considered more secure
- The term “DMZ” alone implies a dual-firewall DMZ.

LECTURE

Network Architecture and Design

Network devices and protocols

Modem

- Modulator/Demodulator
- Binary data is modulated it into analog sound that can be carried on phone networks designed to carry the human voice
- Receiving modem then demodulates the analog sound back into binary data
- Asynchronous devices: they do not operate with a clock signal

LECTURE

Network Architecture and Design

Network devices and protocols

Modem

- Modulator/Demodulator
- Binary data is modulated it into analog sound that can be carried on phone networks designed to carry the human voice
- Receiving modem then demodulates the analog sound back into binary data
- Asynchronous devices: they do not operate with a clock signal

LECTURE

Network Architecture and Design

Network devices and protocols

Modem

- Modulator/De
- Binary data is
- Receiving mo
- Asynchronou

networks des
data

at can be carried on phone

sound back into binary

a clock signal

LECTURE

Network Architecture and Design

Network devices and protocols

DTE/DCE and CSU/DSU

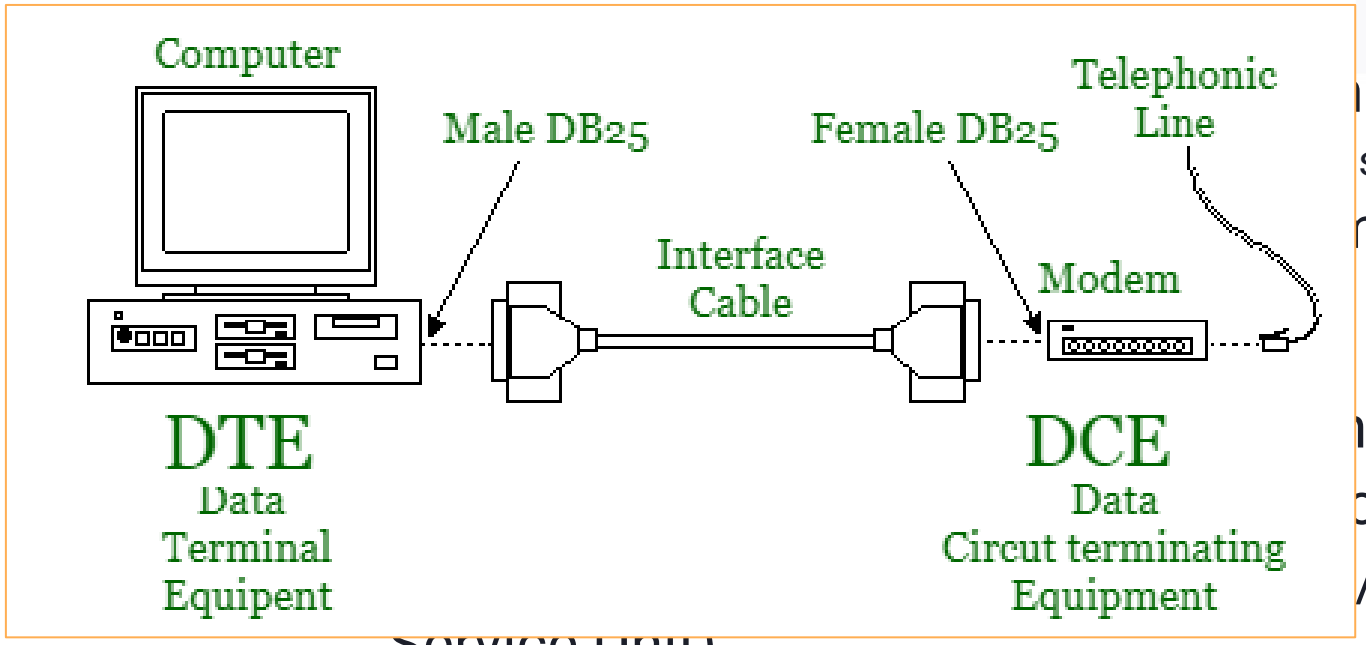
- DTE (Data Terminal Equipment) is a network “terminal”
  - Any type of network-connected user machine, such as a desktop, server, or actual terminal
- DCE (Data Circuit-Terminating Equipment, or sometimes called Data Communications Equipment)
  - A device that networks DTEs, such as a router
- The circuit carried via DCE/DTE is synchronous (it uses a clock signal)
- Both sides must synchronize to a clock signal, provided by the DCE
- The DCE device is a modem or a CSU/DSU (Channel Service Unit/Data Service Unit)

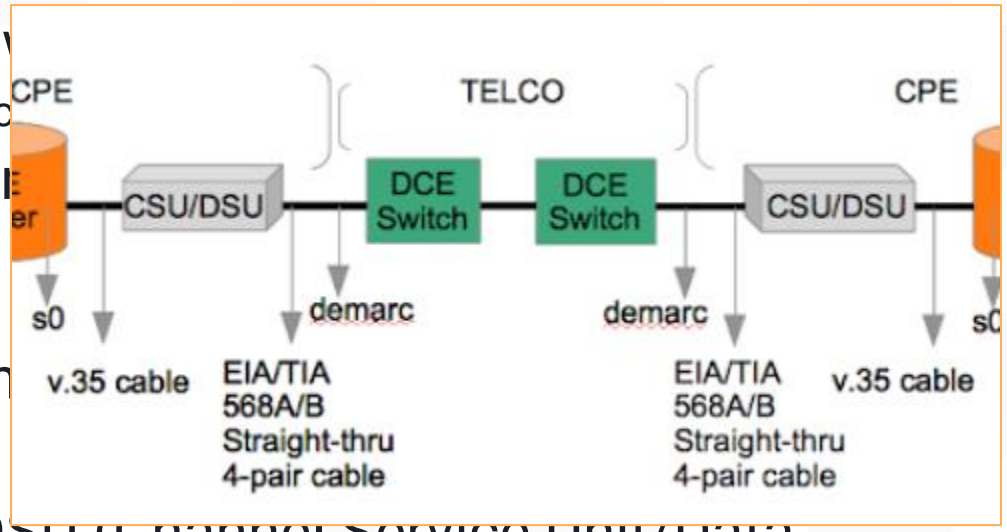
LECTURE

Network Architecture and Design

Network devices and protocols

DTE/DCE and CSU/DSU





Service Unit)

LECTURE

Network Architecture and Design

Network devices and protocols

DTE/DCE and CSU/DSU

- The most common use of these terms is DTE/DCE, and the meaning of each is more specific:
  - DCE marks the end of an ISP's network, connecting to:
  - Data Terminal Equipment (DTE), which is the responsibility of the customer
  - The point where the DCE meets the DTE is called the demarc: the demarcation point, where the ISP's responsibility ends, and the customer's begins

LECTURE

Network Architecture and Design

Secure Communications

Authentication Protocols and Frameworks

- Authenticates an identity claim over the network
- Good security design assumes that a network eavesdropper may sniff all packets sent between the client and authentication server: the protocol should remain secure

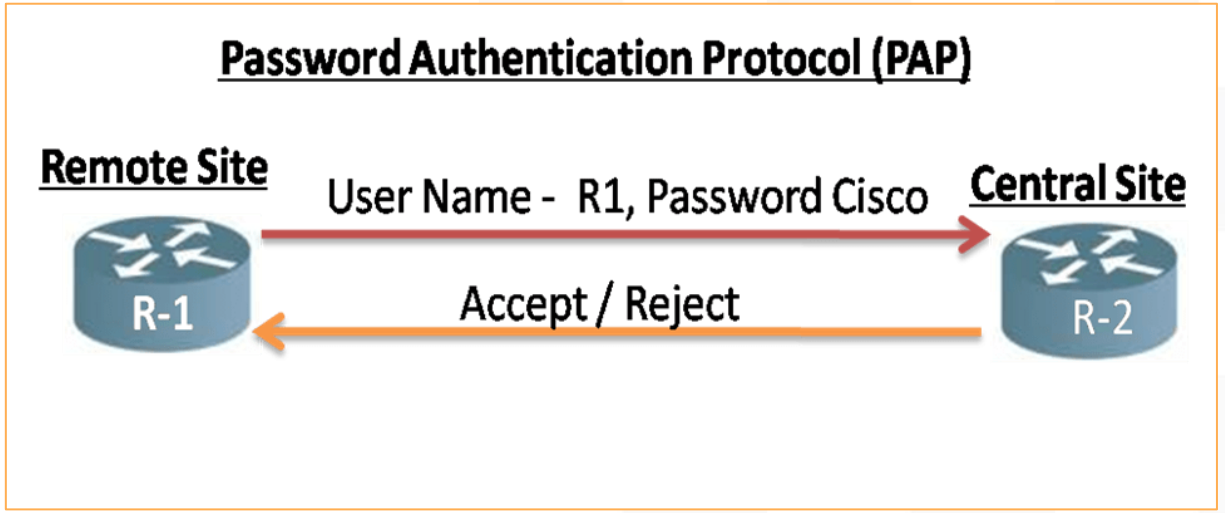
LECTURE

Network Architecture and Design

Secure Communications

PAP & CHAP

- PAP (Password Authentication Protocol)
  - Very weak authentication protocol
  - Sends the username and password in cleartext
  - Insecure and should not be used



LECTURE

Network Architecture and Design

Secure Communications

PAP & CHAP

- CHAP (Challenge-handshake Authentication Protocol)
  - A more secure authentication protocol
  - Does not expose the cleartext password
  - Not susceptible to replay attacks
  - Relies on a shared secret: the password
  - Password is securely created (such as during account enrollment) and stored on the CHAP server
  - Since both the user and the CHAP server share a secret (the plaintext password), they can use that secret to securely communicate
  - The server stores plaintext passwords of each client (weakness)

LECTURE

Network Architecture and Design

Secure Communications

PAP & CHAP

- CHAP (Challenge-handshake Authentication Protocol)
  - To authenticate, the client first creates an initial (unauthenticated) connection via LCP (Link Control Protocol). The server then begins the three-way CHAP authentication process:
  - Server sends a challenge, which is a small random string (also called a nonce).
  - The user takes the challenge string and the password, uses a hash cipher such as MD5 to create a hash value, and sends that value back to the CHAP server as the response.
  - The CHAP server also hashes the password and challenge, creating the expected response. It then compares the expected response with the response received from the user.
  - If the responses are identical, the user must have entered the appropriate password, and is authenticated. If they are different, the user entered the wrong password, and access is denied.

LECTURE

Network Arch

Secure Comm

PAP & CH

- CHAP (Ch
  - To au
    via LC
    authe
  - Serve
  - The u
    as MD
    as the
  - The C
    expec
    receiv
  - If the
    passw
    password, and access is denied.

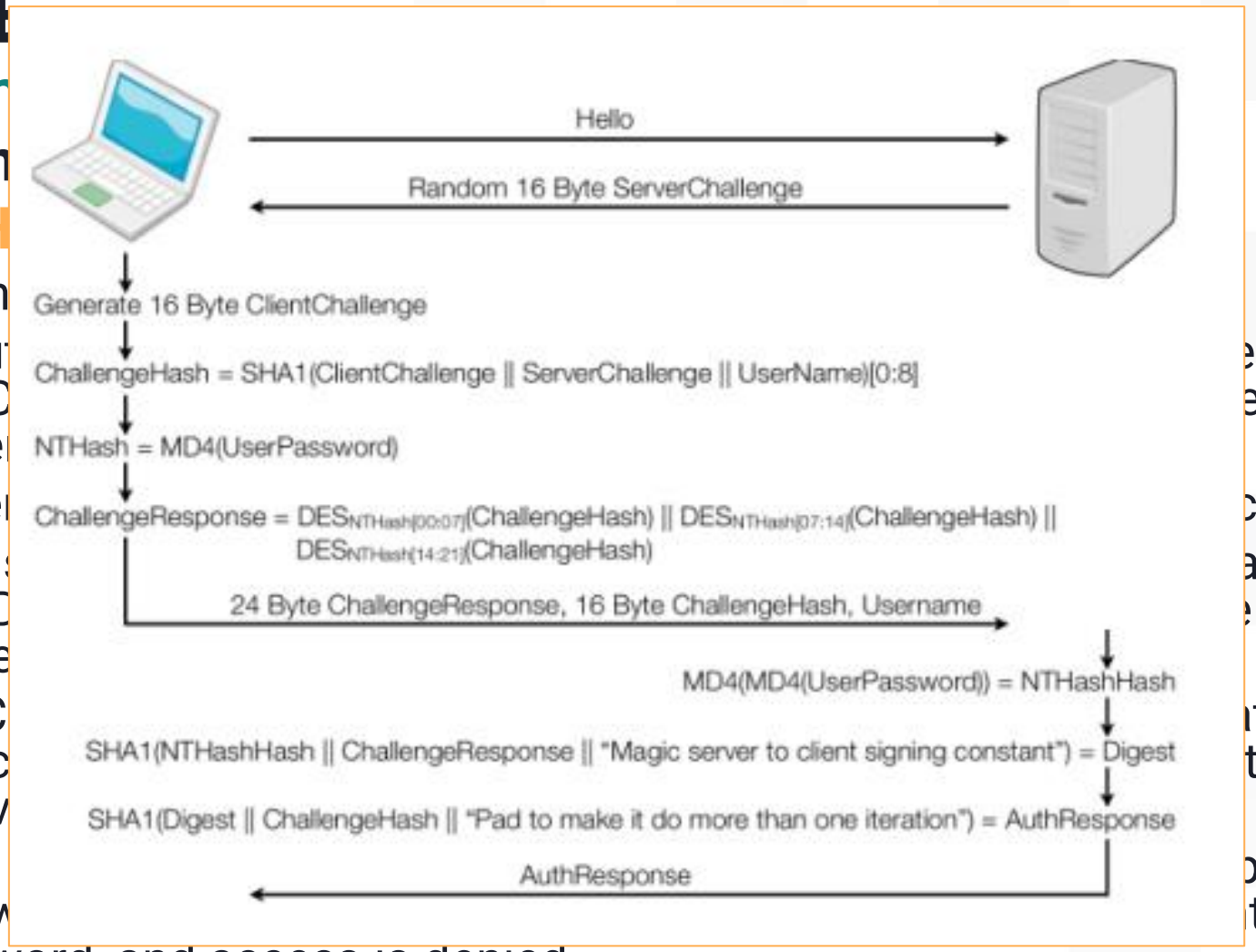
ed) connection
e-way CHAP

called a nonce).

ash cipher such
e CHAP server

ting the
th the response

ppropriate
tered the wrong



LECTURE

Network Architecture and Design

Secure Communications

802.1X and EAP

802.1X is:

- "Port Based Network Access Control"
- Includes EAP (Extensible Authentication Protocol)
  - An authentication framework that describes many specific authentication protocols
  - Designed to provide authentication at Layer 2, before a node receives an IP address
  - Protects against the "roaming infected laptop"
  - Available for both wired and wireless, but is most commonly deployed on WLANs
  - An EAP client is called a **supplicant**, which requests authentication from an **authenticator**

LECTURE

Network Architecture and Design

Secure Communications

802.1X and EAP

EAP Types

- **LEAP (Lightweight Extensible Authentication Protocol)**
  - Cisco-proprietary protocol released before 802.1X was finalized
  - Has significant security flaws, and **should not be used**
- **EAP-TLS (EAP-Transport Layer Security)**
  - Uses **PKI**, requiring both server-side and client-side certificates
  - Establishes a secure TLS tunnel used for authentication
  - Very secure due to the use of PKI, but is **complex and costly** for the same reason

LECTURE

Network Architecture and Design

Secure Communications

802.1X and EAP

EAP Types

- **EAP-TTLS (EAP Tunneled Transport Layer Security)**
  - Developed by Funk Software and Certicom
  - Simplifies EAP-TLS by **dropping the client-side certificate** requirement, allowing other authentication methods (such as password) for client-side authentication
  - Easier to deploy than EAP-TLS, but less secure when omitting the client-side certificate
- **PEAP (Protected EAP)**
  - Jointly developed by Cisco Systems, Microsoft, and RSA Security
  - Similar to (and may be considered a competitor to) EAP-TTLS, including not requiring client-side certificates

LECTURE

Network Architecture and Design

Secure Communications

802.1X and EAP

EA

- |

- |

requirement,
for client-side
ing the client-
ecurity
TLS, including
not requiring client-side certificates

EAP METHODS						
	EAP-MD5	EAP-TLS	EAP-TTLS	EAP-FAST	PEAP	LEAP
Mutual Authentication	NO	YES	YES	YES	YES	YES
Certificates Required	NO	CLIENT + SERVER	SERVER only CLIENT optional	NO	Server only	NO
Dynamic Key Generation	NO	YES	YES	YES	YES	YES
Proprietary	NO	NO	YES Funk Software Certicom	YES Cisco	YES Cisco RSA and Microsoft	YES Cisco
Other	Vulnerable to dictionary attacks; weak	Relatively strong ; must also specify ciphersuite when configuring	User's name is never transmitted in unencrypted plain text	Uses a PAC file (Protected Access Credential)	Due to multiple vendors, this may not be considered "proprietary"	Uses WEP keys; User credentials can still be easily compromised

LECTURE

Network Architecture and Design

Secure Communications

VPN

- Secure data sent via insecure networks such as the Internet
- Goal is to provide the privacy provided by a circuit such as a T1, virtually

SLIP and PPP

- **SLIP (Serial Line Internet Protocol)**
  - A Layer 2 protocol
  - Provides IP connectivity via asynchronous connections such as serial lines and modems
  - First introduced in 1988
  - Allowed routing packets via modem links for the first time (previously, modems were primarily used for nonrouted terminal access)
  - Provides no built-in confidentiality, integrity, or authentication
  - Largely replaced with PPP

LECTURE

Network Architecture and Design

Secure Communications

VPN

- Secure data sent via insecure networks such as the Internet
- Goal is to provide the privacy provided by a circuit such as a T1, virtually

SLIP and PPP

- **PPP (Point-to-Point Protocol)**
  - A Layer 2 protocol that pretty much replaced SLIP.
  - Based on HDLC
  - Adds confidentiality, integrity, and authentication via point-to-point links
  - Supports synchronous links (such as T1s) in addition to asynchronous links such as modems

LECTURE

Network Architecture and Design

Secure Communications

VPN

- **PPTP (Point-to-Point Tunneling Protocol)**
  - Tunnels PPP via IP
  - Developed by a consortium of vendors, including Microsoft, 3COM, and others
  - Uses GRE (Generic Routing Encapsulation) to pass PPP via IP, and uses TCP for a control channel (using TCP port 1723)
- **L2TP (Layer 2 Tunneling Protocol)**
  - Combines PPTP and L2F (Layer 2 Forwarding, designed to tunnel PPP)
  - Focuses on authentication and **does not provide confidentiality**
  - Frequently used with IPSec to provide encryption
  - L2TP can also be used on non-IP networks, such as ATM

LECTURE

Network Architecture and Design

Secure Communications

VPN

- IPv4 has no built-in confidentiality
- IPSec (Internet Protocol Security) was designed to provide confidentiality, integrity, and authentication via encryption for IPv6
- IPSec has been ported to IPv4
- IPSec is a suite of protocols:
  - Major two are **Encapsulating Security Protocol (ESP) and Authentication Header (AH)**
  - Each has an IP protocol number: ESP is protocol 50; AH is protocol 51.

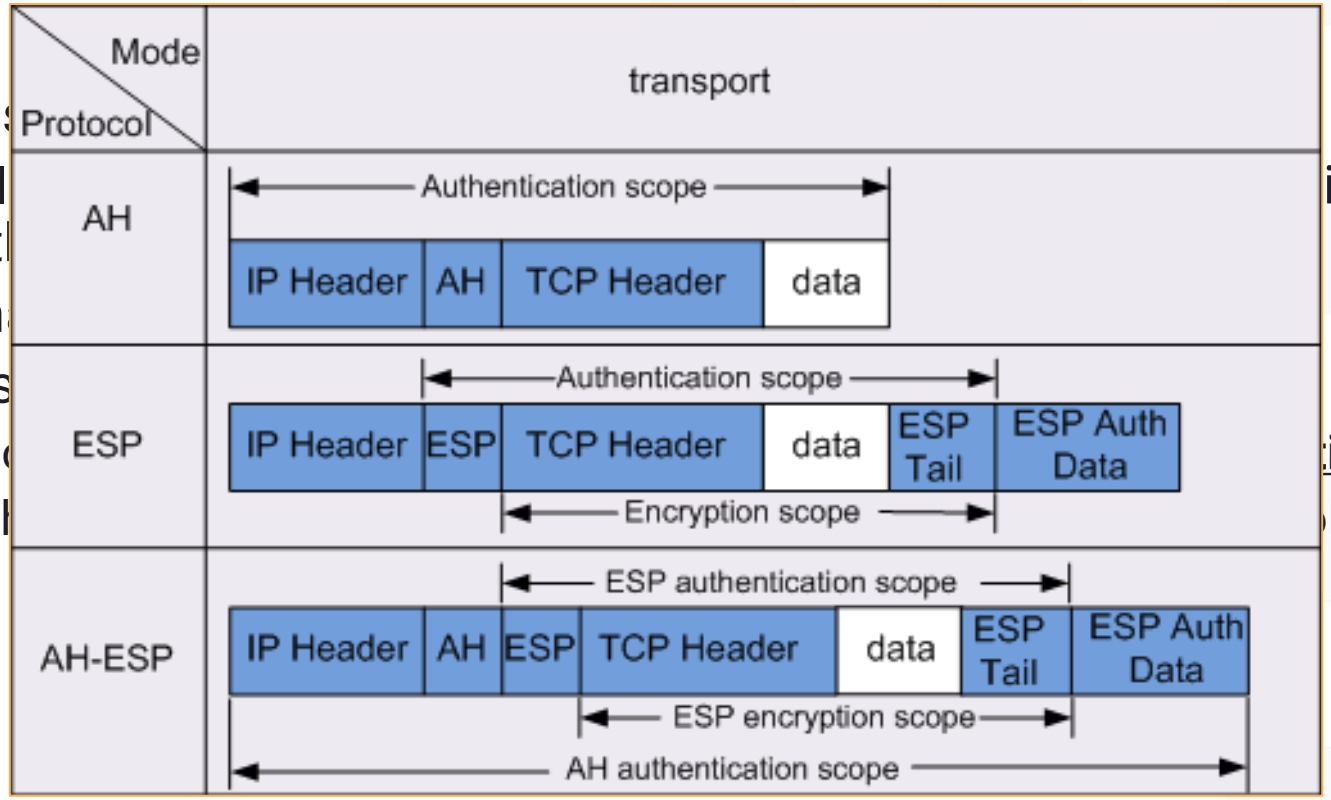
LECTURE

Network Architecture and Design

Secure Communications

VPN

- IPv4 has
- IPSec (I identiality, integrity, and auth
- IPSec h
- IPSec is
  - Majo ication Header (AH)
  - Each l 51.



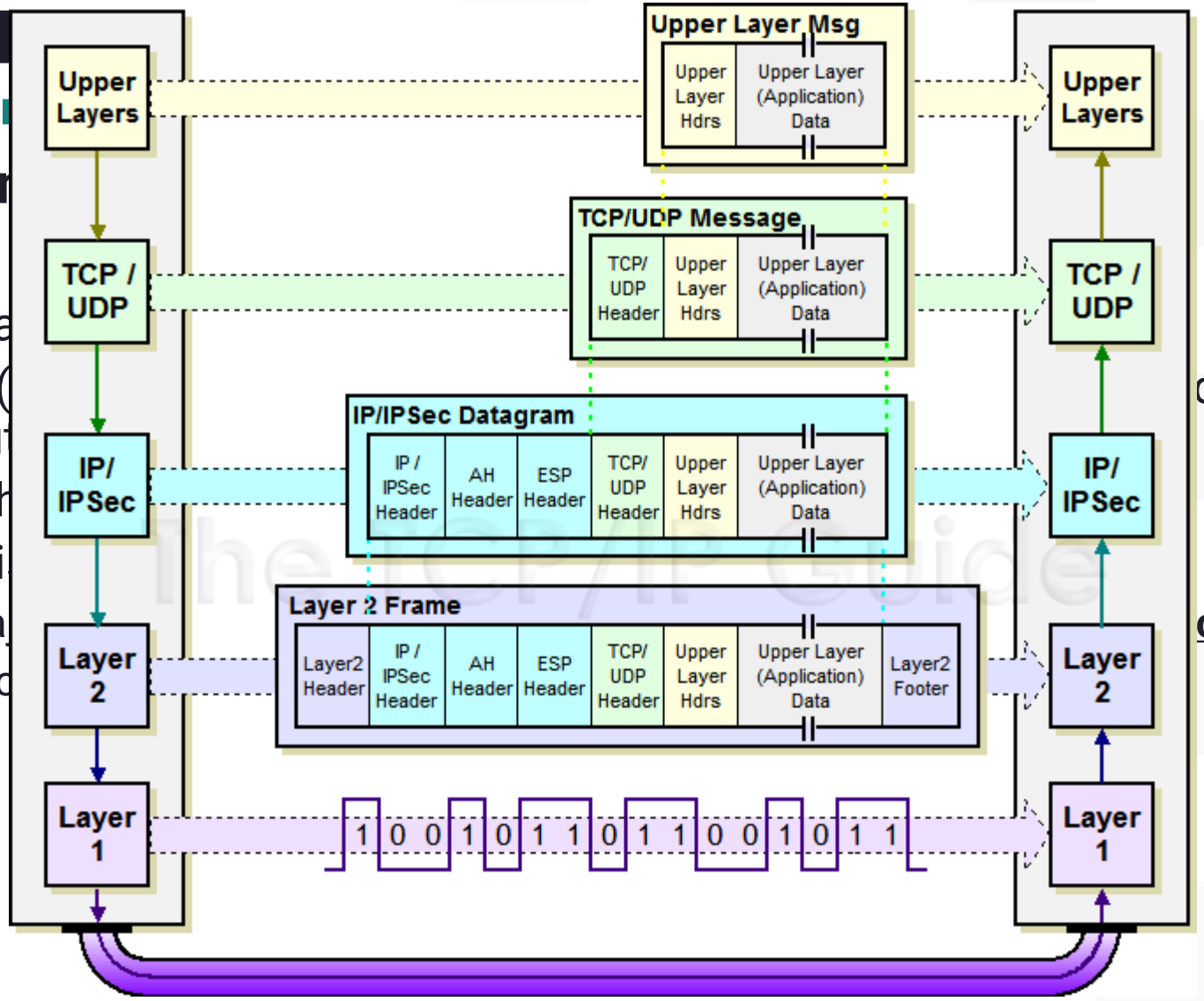
LECTU

Network A

Secure Co

VPN

- IPv4 ha
- IPSec (and au
- IPSec h
- IPSec i
  - Ma
  - Eac



dentiality, integrity,

cation Header (AH)

51.

LECTURE

Network Architecture and Design

Secure Communications

VPN

IPSec Architectures

IPSec has three architectures:

- **Host-to-gateway**
  - Also called client mode
  - Used to connect one system which runs IPSec client software to an IPSec gateway
- **Gateway-to-gateway**
  - Also called point-to-point
  - Connects two IPSec gateways, which form an IPSec connection that acts as a shared routable network connection
- **Host-to-host**
  - Connects two systems (such as file servers) to each other via IPSec
  - Many modern operating systems, such as Windows 7 or Ubuntu Linux, can run IPSec natively, allowing them to form host-to-gateway or host-to-host connections

LECTURE

Network Architecture and Design

Secure Communications

VPN

SSL and TLS

- Secure Sockets Layer (SSL) was designed to protect HTTP (Hypertext Transfer Protocol) data
- HTTPS uses TCP port 443
- TLS (Transport Layer Security) was meant to replace SSL. SSL v3.0 was deprecated in June 2015.
- The current version of TLS is 1.3, described in RFC 8446, replaced TLS 1.2 (RFC 5246, see: http://tools.ietf.org/html/rfc5246).
- Can be used to tunnel other IP protocols to form VPN connections
- SSL VPNs can be simpler
- SSL client software does not require altering the operating system
- IPSec is difficult to firewall; SSL is much simpler.

LECTURE

Network Architecture and Design

Secure Communications

VPN

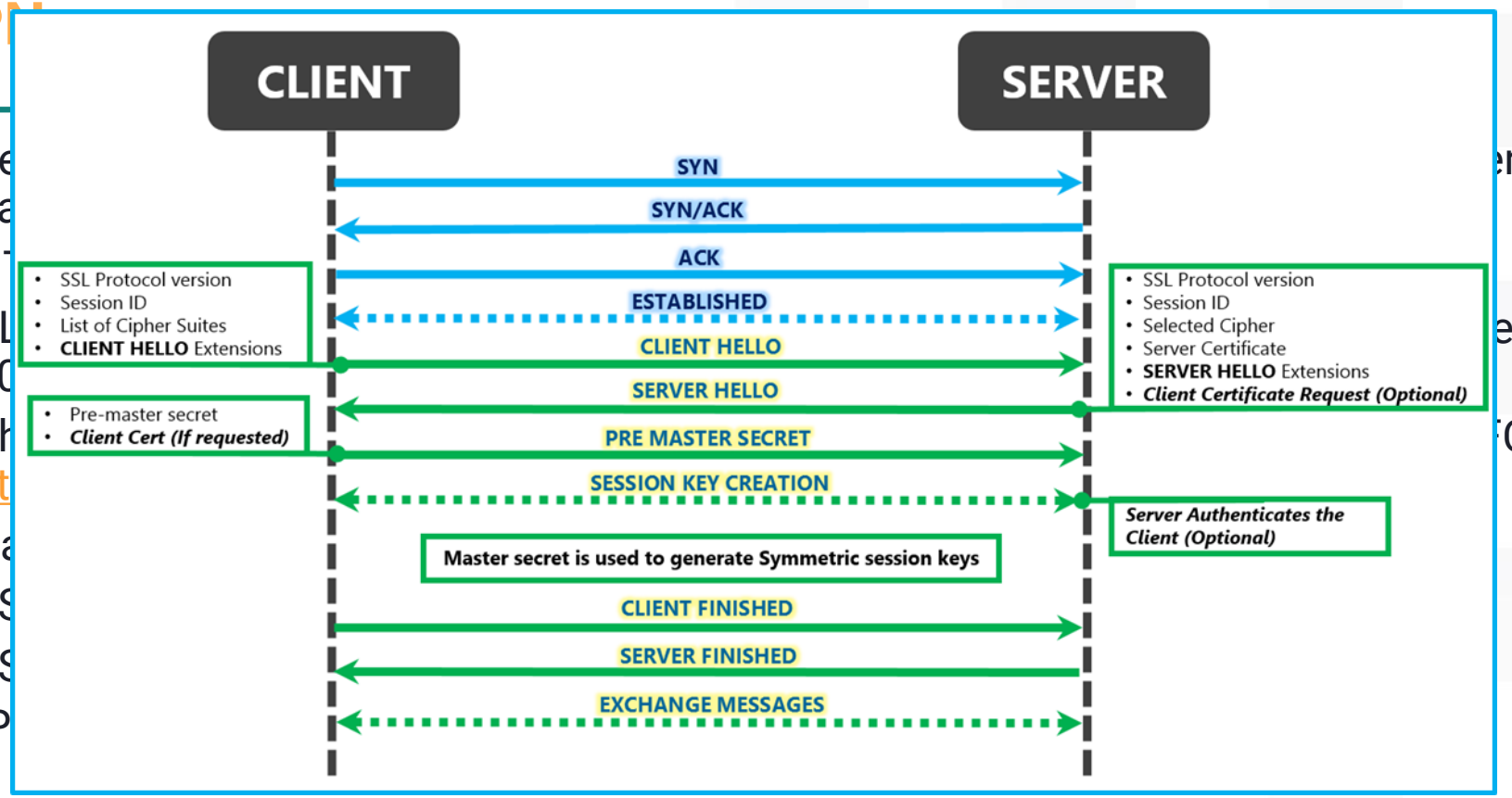
SSL

- Se
- H
- TL
- Th
- Ca
- SS
- SS
- IP

r Protocol)

ecated in June

C 5246, see:



LECTURE

Network Architecture and Design

Remote Access

ISDN

- Integrated Services Digital Network (ISDN)
- An earlier attempt to provide digital service via “copper pair,” the POTS (Plain Old Telephone Service)
- Devices are called terminals
- Basic Rate Interface (BRI) service provides two 64K digital channels (plus a 16K signaling channel) via copper pair
- PRI (Primary Rate Interface) provides twenty-three 64K channels, plus one 16K signaling channel

LECTURE

Network Architecture and Design

Remote Access

DSL

- Digital Subscriber Line (DSL)
- “last mile” solution similar to ISDN: use existing copper pairs to provide digital
- As a general rule, the closer a site is to the Central Office (CO), the faster the available service

Common types of DSL are

- **Symmetric Digital Subscriber Line** (SDSL, with matching upload and download speeds)
- **Asymmetric Digital Subscriber Line** (ADSL, featuring faster download speeds than upload)
- **Very High-Rate Digital Subscriber Line** (VDSL, featuring much faster asymmetric speeds)
- **HDSL** (High-data-rate DSL), which matches SDSL speeds using two pairs of copper; HDSL is used to provide inexpensive T1 service

LECTURE

Network Architecture and Design

Remote Access

DSL

- Digital Subscriber Line (DSL)
- "last mile" solution similar to ISDN: use existing copper pairs to provide digital
- As a gener ...available service

Type	Download Speed	Upload Speed	Distance from CO
ADSL	1.5 to 9 Mbps	16 to 640 Kbps	18,000 feet
SDSL	1.544 Mbps	1.544 Mbps	10,000 feet
HDSL	1.544 Mbps	1.544 Mbps	10,000 feet
VDSL	20-50+ Mbps	Up to 20 Mbps	< 5,000 feet

Common typ

- **Symm** ...nload speeds)
- **Asymı** ...eeds than upload
- **Very High-Rate Digital Subscriber Line** (VDSL, featuring much faster asymmetric speeds)
- **HDSL** (High-data-rate DSL), which matches SDSL speeds using two pairs of copper; HDSL is used to provide inexpensive T1 service

LECTURE

Network Architecture and Design

Remote Access

Cable Modems

- Used by Cable TV providers to provide Internet access via broadband cable TV
- Broadband, unlike baseband, has multiple channels (like TV channels)
- Dedicating bandwidth for network services requires dedicating channels for that purpose
- Unlike DSL, Cable Modem **bandwidth is typically shared** with neighbors on the same network segment

LECTURE

Network Architecture and Design

Remote Access

Callback & Caller ID

- Callback
  - Modem-based authentication system
  - User connects via modem and authenticates. The system hangs up and calls the user back at the preconfigured number.
- Caller ID
  - Similar method: in addition to username and password, it requires calling from the correct phone number
  - Caller ID can be easily forged: many phone providers allow the end user to select any Caller ID number of their choice. This makes Caller ID a weak form of authentication.

LECTURE

Network Architecture and Design

Remote Access

Instant Messaging

- Allows two or more users to communicate with each other via real-time “chat”
- Chat may be one-to-one, or many-to-many via chat groups
- In addition to chatting, most modern instant messaging software allows file sharing, and sometimes audio and video conferencing
- Other chat protocols and networks include AOL Instant Messenger (AIM), ICQ (short for “I seek you”), and Extensible Messaging and Presence Protocol (XMPP) (formerly known as Jabber).
- Organizations should have a policy controlling the use of chat software and technical controls in place to monitor and, if necessary, block their usage.

LECTURE

Network Architecture and Design

Remote Access

Instant Messaging

- IRC (Internet Relay Chat)
  - A global network of chat servers and clients created in 1988
  - Still very popular even today
  - IRC servers use TCP port 6667 by default, but many IRC servers run on nonstandard ports
  - IRC can be used for legitimate purposes, but is also used by malware, which may “phone home” to a command-and-control channel via IRC (among other methods)

LECTURE

Network Architecture and Design

Remote Access

Remote Desktop Console Access

- Been around for a long, long time.
- rlogin and rsh, *nix operating systems, poor security (clear text), TCP 513 and 514
- Virtual Network Computing (VNC), typically TCP 5900
- Remote Desktop Protocol (RDP), TCP 3389

WE MADE IT THROUGH SESSION #7!

Technical, but not too technical.

Please try to catch up in your reading.

- We left off on page 293 in the book.
- Monday (5/10) we'll start:
  Chapter 6: Identity and Access Management.