Microsoft® Official Course

Module3

Understanding Network Infrastructure

Microsoft®

Module Overview

- Network Architecture Standard
- Local Area Networking
- Wide Area Networking
- Wireless Networking
- Connecting to the Internet
- Remote Access

Lesson 1: Network Architecture Standard

- IEEE 802 Standards
- Network Components and Terminology
- Network Architecture
- Network Media Access Control Methods

IEEE 802 Standards

- IEEE 802.3 – Ethernet networks
- IEEE 802.5 – Token ring networks
- IEEE 802.11 – Wireless local area networks
- IEEE 802.15 – Wireless personal area networks
- IEEE 802.16 – Broadband wireless networks

Network Components and Terminology

- Data
- Node
- Client
- Server
- Peer
- Network adapter
- Media
- Hubs/switches/routers
- Transport protocol
- Bandwidth

Network Architecture

Wired

- Ethernet
- Power over Ethernet
- Token ring
- ARCnet
- FDDI
- And more....

Wireless

- Wi-Fi
- Infrared
- Bluetooth
- And more....

Network Media Access Control Methods

Network Media Access Control Method	Action
CSMA/CD	• Checks for media availability • Sends data • Resolves collisions
CSMA/CA	• Monitors media availability constantly • Advertises intent to send • Sends data
Token passing	• Listens for token • Packages data with token • Confirms delivery when token returns
Demand Priority	• Hub controls access • Provides regular and high priority transmissions

Lesson 2: Local Area Networking

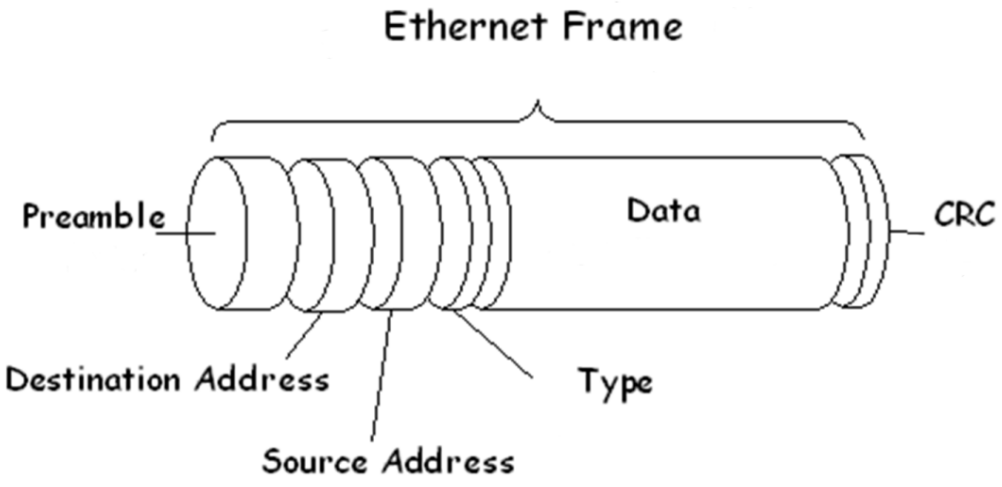
- What Is a LAN?
- How Nodes on a LAN Communicate
- Physical Components of a LAN
- LAN Physical Topology
- What Is a Virtual LAN?

What Is a LAN?

- A LAN is the most common form of computer network

How Nodes on a LAN Communicate

- A media access control (MAC) address is the most basic form of a network identifier for a node on a network

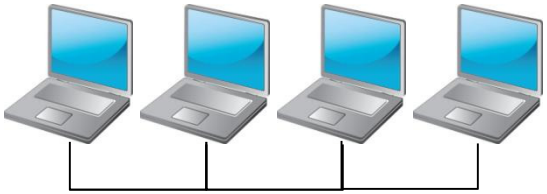


00-22-FB-8A-41-64

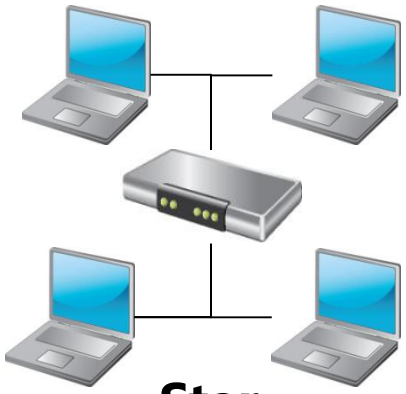
Physical Components of a LAN

- Network adapter
- Wiring
- Hub or switch
- Termination point
- Wiring cabinet

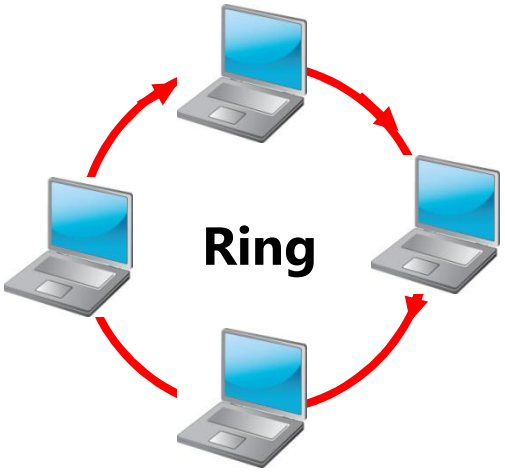
LAN Physical Topology

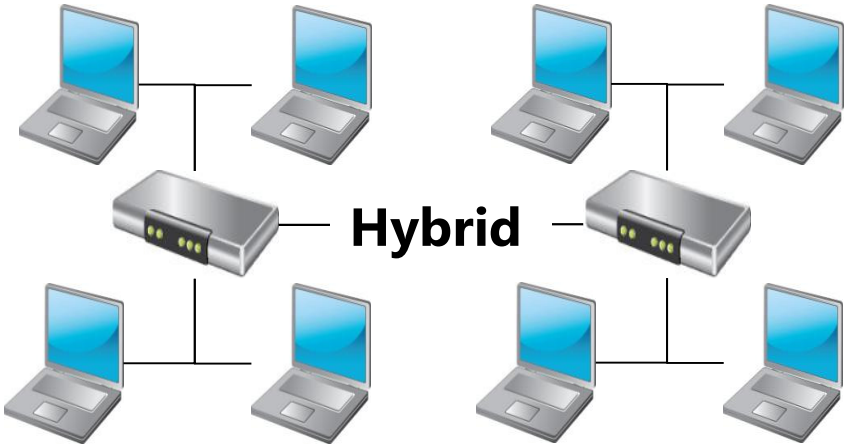


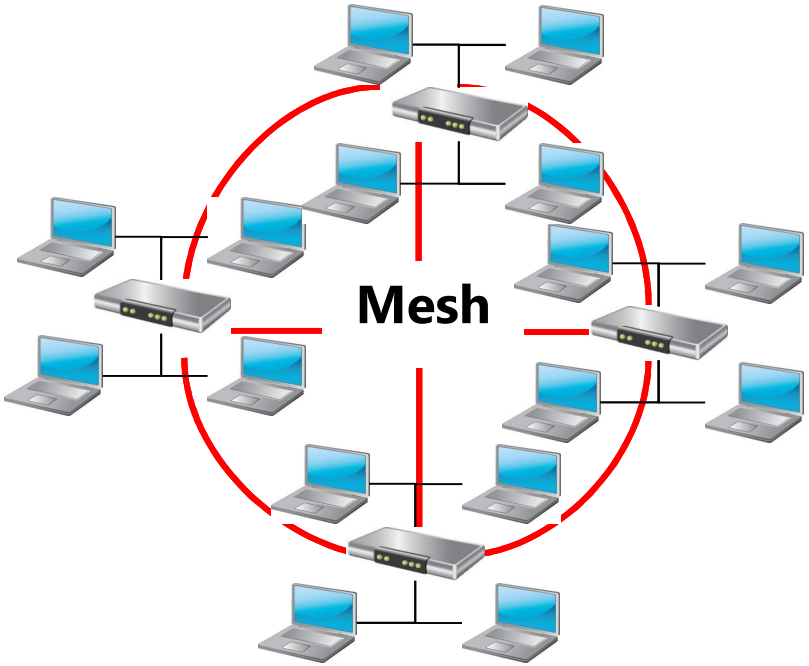
Bus



Star







What Is a Virtual LAN?

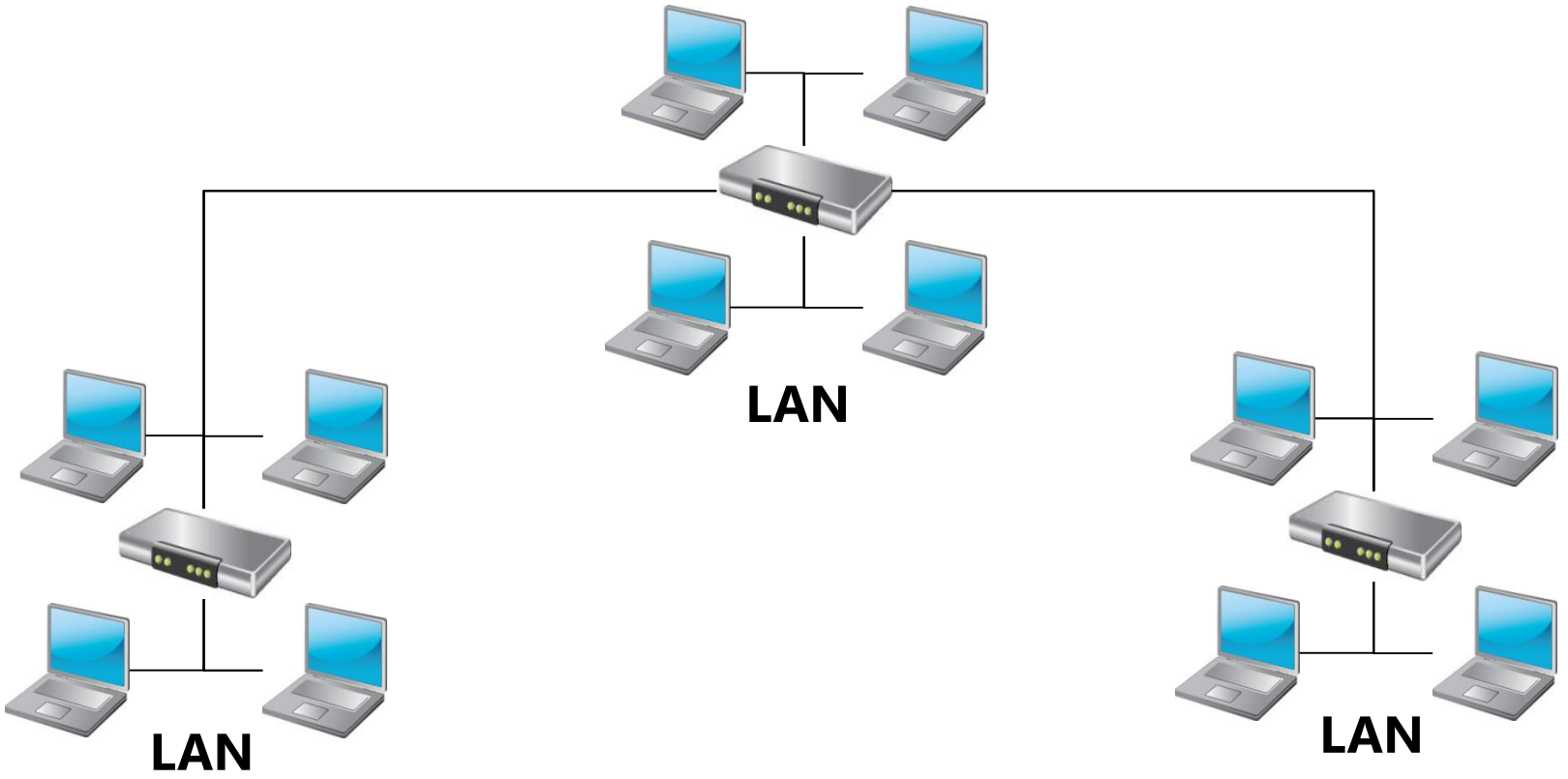
- Manage network traffic
- Group physically dispersed nodes into logical LANs
- Increase the number of nodes without needing to rewire the network
- Reconfigure the network without needing to move nodes
- Isolate network traffic

Lesson 3: Wide Area Networking

- What Is a WAN?
- Physical Components of a WAN
- What Are WAN Standards?
- What Are the T-Carrier and E-Carrier Standards?
- Optical Carrier Standards
- What Is ISDN?
- Other WAN-Based Connection Technologies

What Is a WAN?

- A WAN is a geographically distributed network composed of multiple LANs joined into a single large network



Physical Components of a WAN

- Bridge
- Router
- Leased line
- Backbone

What Are WAN Standards?

- T-Carrier
- E-Carrier
- Optical Carrier
- ISDN
- DSL
  - Symmetric
  - Asymmetric

What Are the T-Carrier and E-Carrier Standards?

T-Carrier Standards:

- Used in North America

E-Carrier Standards:

- Used globally except North America

Standard	Bandwidth	Typical Media
T1	1.544 Mbps	Copper
T3	44.736 Mbps	Fiber
E1	2.048 Mbps	Copper
E3	34.368 Mbps	Fiber

Optical Carrier Standards

- OC-X standards refer to a set of specifications for digital data over specifically designed fiber-optic networks

Standard	Bandwidth
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1244.16 Mbps
OC-48	2488.32 Mbps
OC-192	9953.28 Mbps
OC-768	39,813.12 Mbps

What Is ISDN?

ISDN is:

- Dial-on demand
- Typically used as a backup connection

Standard	Bandwidth
BRI	128 Kbps
PRI	1.536 Mbps

Other WAN-Based Connection Technologies

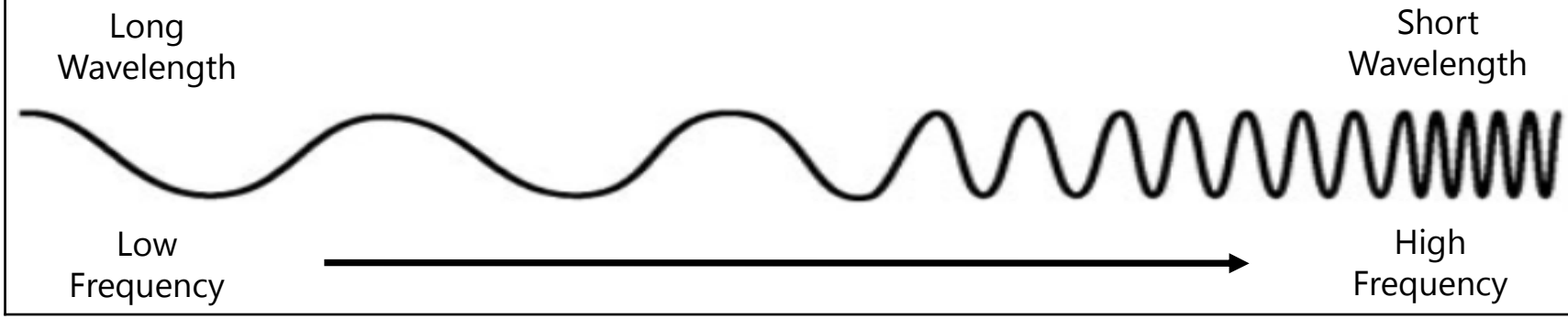
- Cable
- 2G/3G/4G Wireless
  - GSM
  - UMTS
  - LTE

Lesson 4: Wireless Networking

- What Is Wireless Networking
- Wireless Networking Components
- What Is 802.11?
- Infrared and Bluetooth
- Attenuation and Interference
- Securing Wireless Networks

What Is Wireless Networking

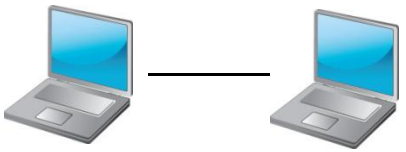
Microwaves/Radio/TV	Visible and near Visible spectrum			X-Rays	Gamma Rays
• Mobile Phones • Wireless Routers • Microwave Ovens • Radar • AM/FM Radio • UHF/VHF	<u>Infrared</u> • TV Remote • Night vision	Visible Light	<u>Ultraviolet</u> • Dental • Suntans • Detecting forged notes	• Medical • Baggage Screening	• Cosmic Rays • Medical Treatments



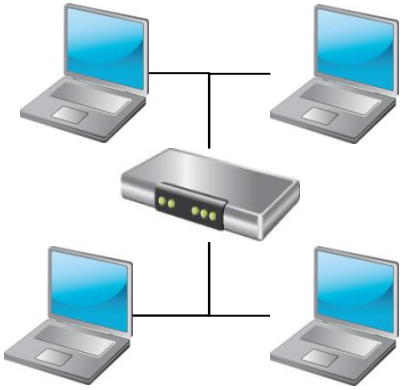
Wireless Networking Components

- Wireless network adapter
- Access point
- Ad-hoc network
- Infrastructure network
- SSID

Ad hoc Network



Infrastructure Network



What Is 802.11?

- The IEEE 802.11 working group of standards defines the aspects of Wide Area Networks (WANs)

Standard	Frequency	Data Rate	Indoor Range	Outdoor Range
802.11a	5 GHz	54 Mbps	50 feet	100 feet
802.11b	2.4 GHz	11 Mbps	150 feet	300 feet
802.11g	2.4 GHz	54 Mbps	150 feet	300 feet
802.11n	2.4–2.5 GHz	600 Mbps	300 feet	600 feet

Infrared and Bluetooth

- Infrared uses infrared (IR) technology
- Bluetooth uses wireless radio frequency technology

Feature	Infrared	Bluetooth
Range	≤ 3 m	≤ 10 m
Data Transfer	≤ 4 Mbps	≤ 24 Mbps
Pass Through Walls	No	Yes
Power Consumption	Low	Very Low

Attenuation and Interference

- Attenuation
  - Weakening of the wireless signal
  - Reduced range or frequency and loss of data
- Interference
  - Interaction with other electromagnetic waves
  - Reduced signal integrity and loss of data

- Assess areas for access point suitability and be aware of potential sources of interference

Securing Wireless Networks

- Common encryption methods:
  - WEP
  - Wi-Fi Protected Access (WPAv1 and WPAv2)
    - WPA-Personal (Shared Key)
    - WPA-Enterprise (Per-user keys)
  - Smart Card Certificates

- Other methods:
  - MAC filtering
  - USB tokens
  - Hidden SSID

Lesson 5: Connecting to the Internet

- What Is the Internet?
- Intranets and Extranets
- What Is a Firewall?
- Proxy and Reverse Proxy Servers

What Is the Internet?

- The Internet is a system of interconnected networks that spans the globe

Internet

Intranets and Extranets

Intranets are:

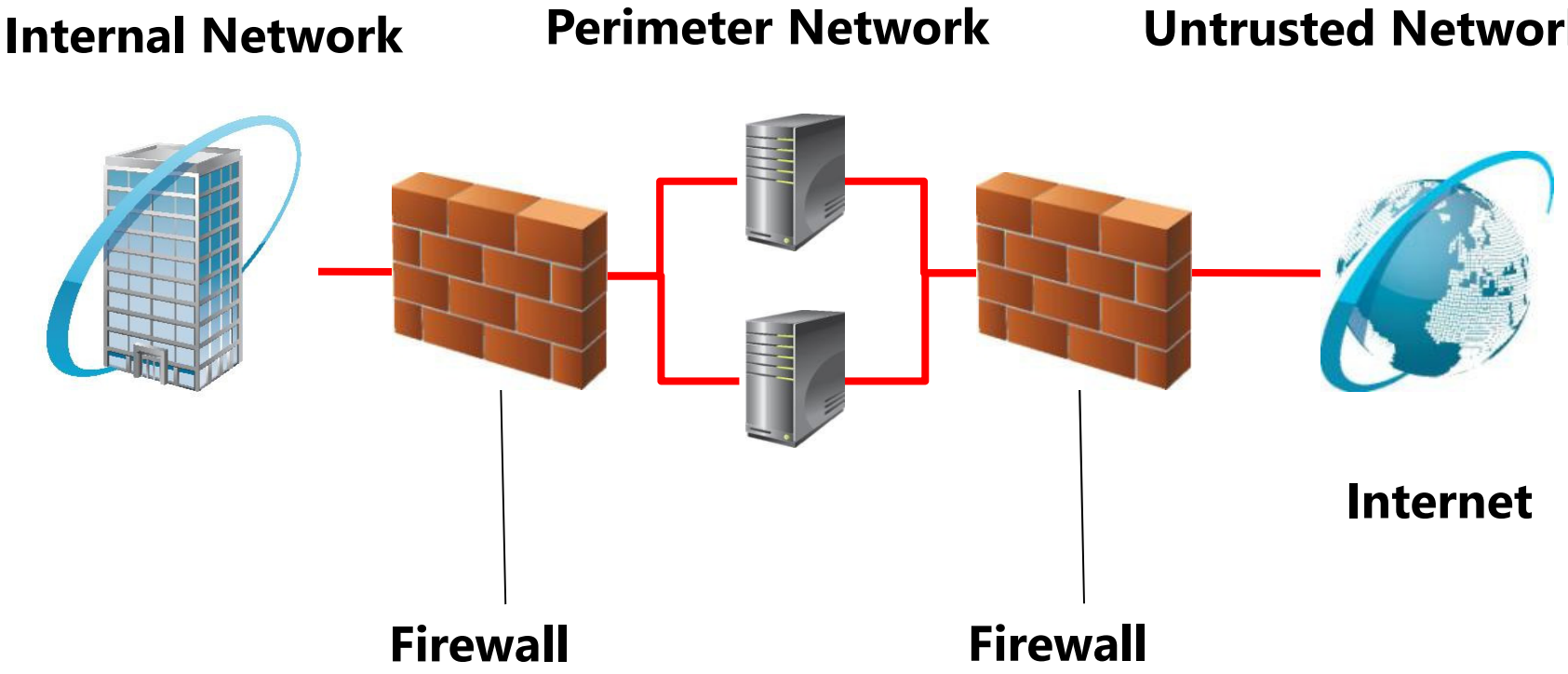
- A group of services hosted on a network
- A private structure
- Internet-like service provision

Extranets are:

- Similar services to Intranet
- Exposed to networks outside of the Intranet
- Services that require extra security measures

What Is a Firewall?

- A *firewall* is used to protect a private network from security risks inherent to connecting to an untrusted network



Proxy and Reverse Proxy Servers

Proxy servers:

- Filter client access to resources
- Locally cache information

Reverse proxy servers:

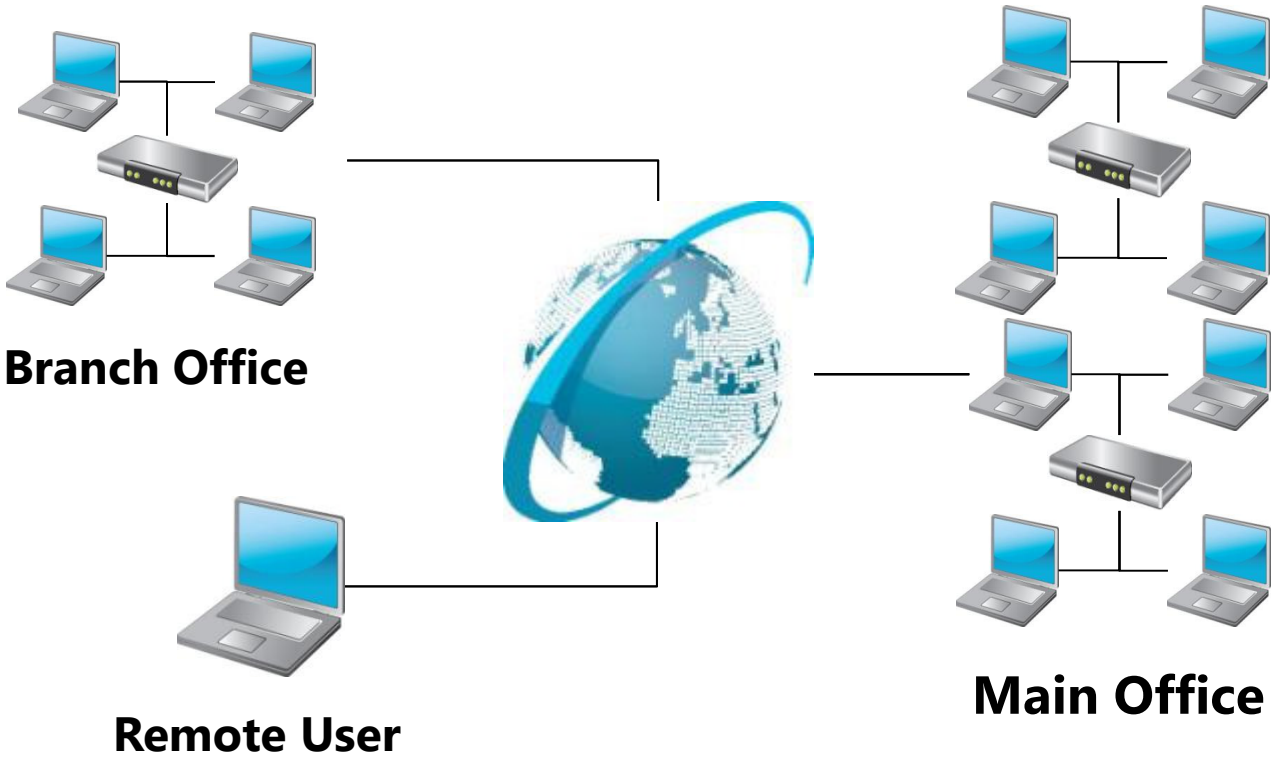
- Redirect extranet requests from external to extranet servers
- Limit and secure communication from external sources across the firewall
- Allow for load balancing

Lesson 6: Remote Access

- What Is Remote Access?
- Encryption and Authentication
- Virtual Private Networks and Direct Access
- RADIUS
- Network Access Protection

What Is Remote Access?

- Remote access methods typically use an intermediary and possibly untrusted connection method, such as the Internet, to indirectly gain access to a central private network



Encryption and Authentication

Encryption is:

- Scrambling data to prevent unauthorized access

Authentication is:

- Providing a means of verifying the identify of the user or node

- Authorization is:
  - Determining the appropriate level of access to a resource for an authenticated resource

Virtual Private Networks and Direct Access

- VPN
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer Two Tunneling Protocol (L2TP)
  - Secure Socket Layer (SSL) Tunneling Protocol
  - IP HTTPS
  - Ipsec
- DirectAccess

RADIUS

- Remote Authentication Dial-in User Service (RADIUS) allows for the exchange of authentication information between various elements of a remote access solution
  - Authenticate
  - Authorize
  - Account

Network Access Protection

- NAP does not protect networks from malicious software or users
- NAP provides components that help administrators enforce network compliance policies, and can check for:
  - Updated antivirus
  - Firewall status
  - Spyware protection
  - Automatic update status

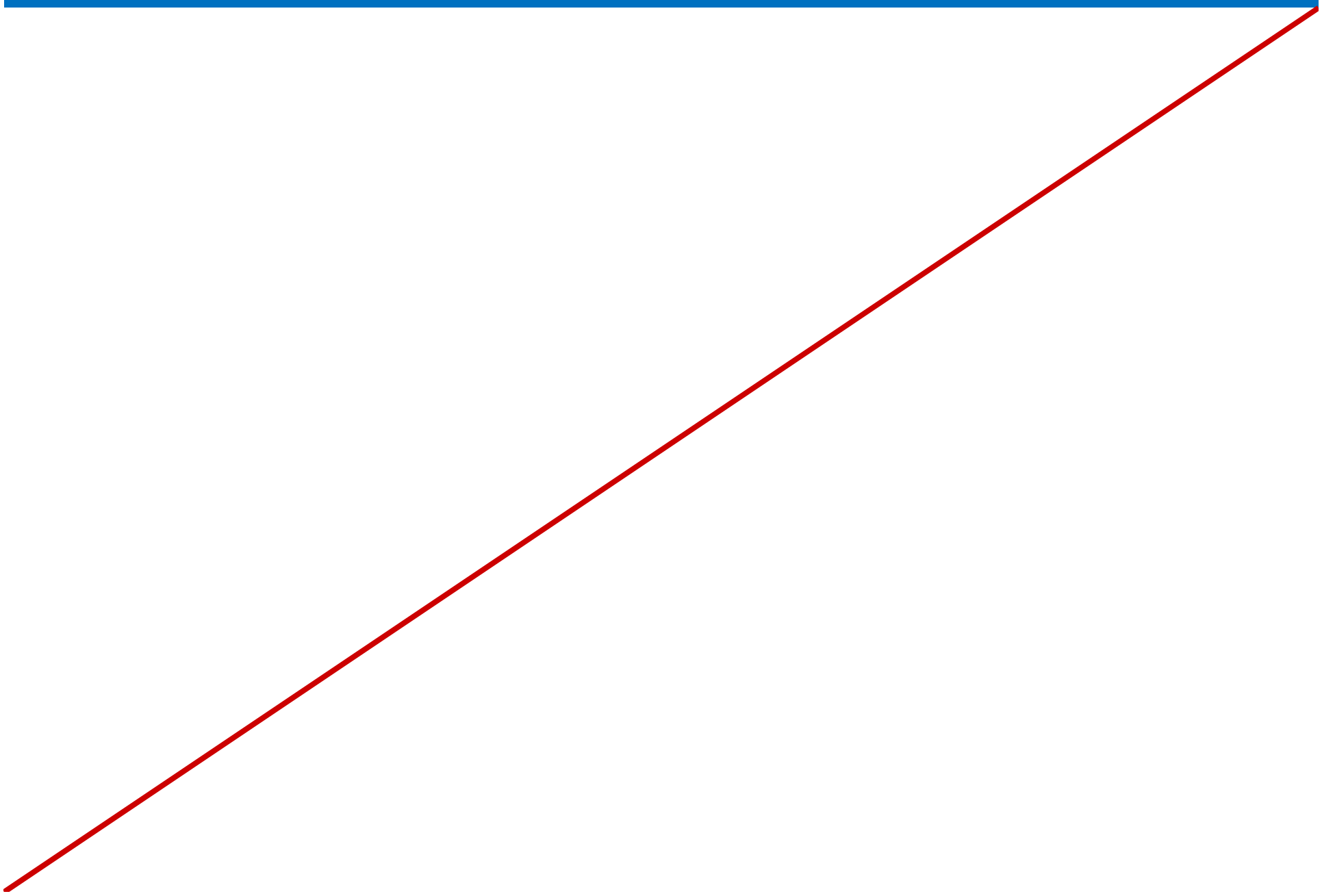
Lab: Selecting Network Infrastructure Components

- Exercise 1: Determining Appropriate Network Components

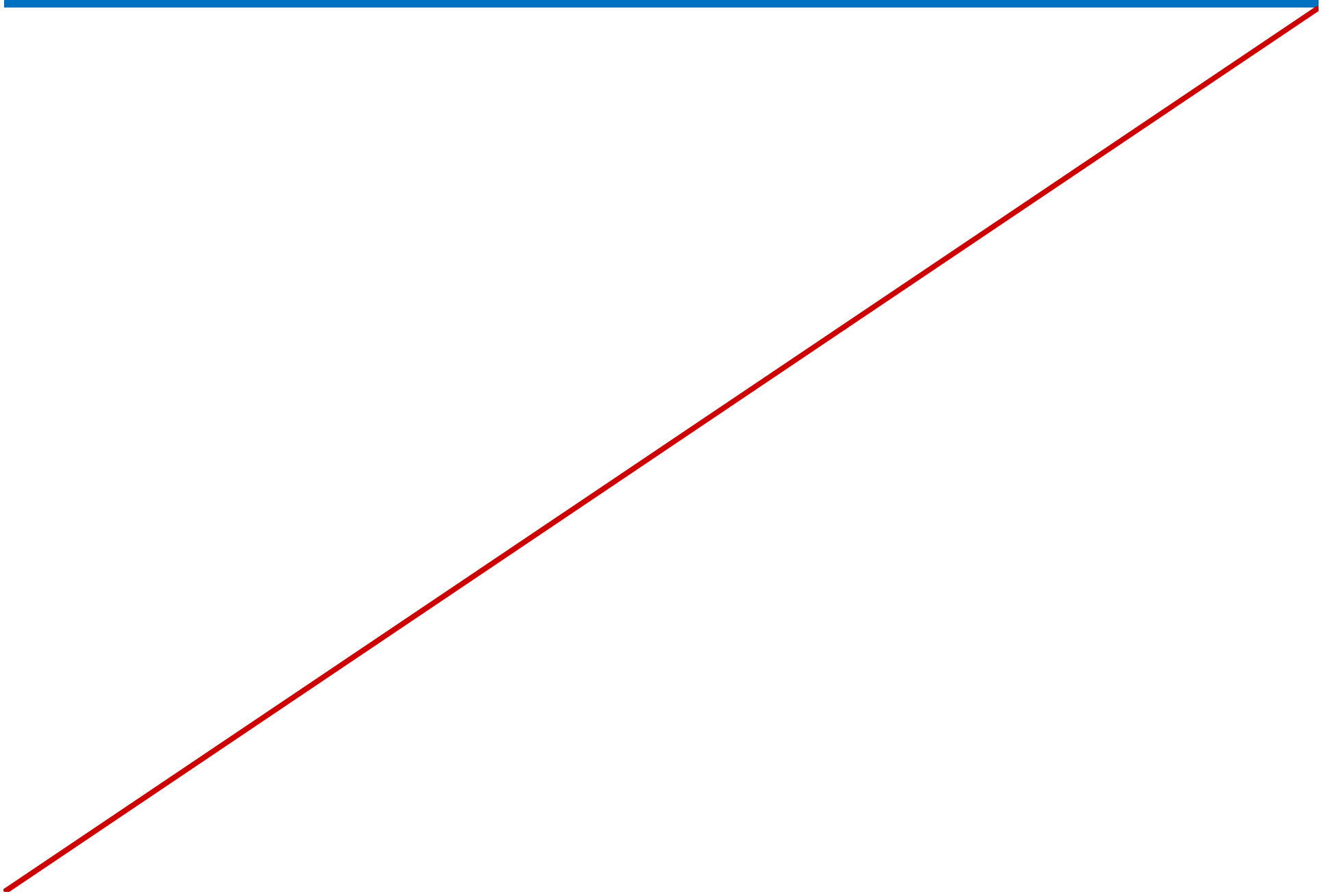
Logon Information
No virtual machines are required for this exercise.

Estimated Time: 30 minutes

Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.



Lab Scenario

A. Datum Corporation has recently decided to decentralize its marketing department, currently located in New York. In addition to the New York location, a new marketing office is being built in Seattle to house the media design staff.

You are responsible for choosing the LAN design and general components for the new office and ensuring that the two offices are connected in a way that allows staff in the Seattle office to access the information they need from the New York office.

You have received email messages from the Seattle office manager outlining the duties assigned to the new office, a list of employees that will be using the Seattle office, and the primary job functions of those employees.

Lab Review

- What other options exist to connect the home office employees if their role changes and requires consistent access to information on the Seattle LAN?
- What infrastructure should be used to connect the conference room portion of the Seattle location?

Module Review and Takeaways

- Review Questions