Objectives

1. Explain virtualization and identify characteristics of virtual network components
2. Create and configure virtual servers, adapters, and switches as part of a network
3. Describe techniques for incorporating virtual components in VLANs
4. Explain methods for remotely connecting to a network, including dial-up networking, virtual desktops, and thin clients
5. Discuss VPNs (virtual private networks) and the protocols they rely on
6. Identify the features and benefits of cloud computing and NaaS (Network as a Service)
Virtualization

- Emulation of a computer, operating system environment, or application:
  - On a physical system
- Virtual machines (VMs)
  - Virtual workstations
  - Virtual servers
  - Can be configured to use different types of:
    - CPU
    - Storage drive
    - NIC

Virtualization (cont’d.)

- VM appears to user no different than physical computer:
  - Running the same software
- Host
  - Physical computer
- Guest
  - Virtual machines
- Hypervisor
  - Manages virtual machines

Figure 10-1
Elements of virtualization
Virtualization (cont’d.)

• Advantages of virtualization
  – Efficient use of resources
  – Cost and energy savings
  – Fault and threat isolation
  – Simple backups, recovery, and replication

• Disadvantages
  – Compromised performance
  – Increased complexity
  – Increased licensing costs
  – Single point of failure

• Virtual network
  – Can be created to consist solely of virtual machines on a physical server
  – Most networks combine physical and virtual elements

Virtual Machines and Adapters

• Virtualization program
  – Assigns VM’s software and hardware characteristics
  – Often easy to use, step-by-step wizard

• Operating system images
  – Available for download online
  • Or on disc from software vendors

• Network connection
  – Requires virtual adapter (vNIC)
Virtual Switches and Bridges

- Virtual bridge or switch
  - Created when first VM’s NIC is selected
  - Connects VM with host
  - Resides in RAM

- Virtual switch
  - Logically defined device
  - Operates at Data Link layer
  - Passes frames between nodes

- Virtual bridge
  - Connects vNICs with a network

Figure 10-4 Virtual servers on a single host connected with a virtual switch

Figure 10-5 Virtual switches exchanging traffic through routers

Courtesy Course Technology/Cengage Learning
Network Connection Types

- Must identify networking mode vNIC will use
- Frequently-used network connection types
  - Bridged
  - NAT
  - Host-only
- Bridged
  - vNIC accesses physical network using host machine’s NIC
  - Obtains own IP address, default gateway, and netmask from DHCP server on physical LAN

Figure 10-6 vNIC accessing a network in bridged mode
Courtesy Course Technology/Cengage Learning
Network Connection Types (cont’d.)

• NAT
  – vNIC relies on host to act as NAT device
  – Obtains IP addressing information from host
  – Virtualization software acts as a DHCP server
  – Default network connection type in VMware, VirtualBox, and KVM

• Host-only
  – VMs on one host can exchange data with each other and the host
  – Cannot communicate with nodes beyond the host
  – Never receive or transmit data with host’s physical NIC
Figure 10-8 vNIC accessing a network in NAT mode
Courtesy Course Technology/Cengage Learning

Figure 10-9 Selecting the NAT option for a vNIC in VirtualBox
Courtesy Course Technology/Cengage Learning
Virtual Appliances

- Alternative to test servers for new software
- Virtual appliance includes:
  - Image of operating system, software, hardware specifications, and application configuration
- Most commonly virtual servers
- Popular functions
  - Firewall
  - E-mail solutions
  - Network management
  - Remote access
Virtual Networks and VLANs

- **Virtual network**
  - Refers to how VMs connect with other virtual and physical network nodes
- **Virtual network management**
  - Nearly identical to physical network management
- **To add VMs to a physical VLAN:**
  - Modify virtual switch’s configuration
    - Steps vary for different virtualization programs

---

**Figure 10-11 Multiple virtual servers connected to multiple VLANs**

*Courtesy Course Technology/Cengage Learning*
Remote Access and Virtual Computing

- Remote access
  - Allows user to connect with LAN or WAN in different geographical location
  - Allows access to shared resources as any other client on LAN or WAN
  - Requires transmission path and appropriate software

- Popular remote access techniques
  - Dial-up networking
  - Microsoft’s Remote Access Service (RAS)
    - Or Routing and Remote Access Service (RRAS)
  - Virtual Private Networks

Dial-Up Networking

- Dialing directly into private network’s or ISP’s remote access server
- Usually refers to connection using PSTN
- Remote access server attached to group of modems
- Client must run dial-up software
- After authentication, user allowed access
- Remote access server can serve multiple users
- Low throughput
- Less popular today
Remote Access Servers

• Accepts connections regardless of Internet connection type
• RRAS (Routing and Remote Access Service)
  – Microsoft’s remote access software
  – Available with Server 2003, 2008, 2008 R2, XP, Vista, and 7 operating systems
  – Enables server to act as a router
  – Includes multiple security provisions

Figure 10-12 Clients connecting with a remote access server

Courtesy Course Technology/Cengage Learning
Remote Access Protocols

- **SLIP (Serial Line Internet Protocol)**
  - Earlier and less sophisticated than PPP
  - Can only carry IP packets
  - Requires significant amount of setup
  - Does not support data encryption
  - Asynchronous transmission
- **PPP (Point-to-Point Protocol)**
  - Known as PPPoE when used over Ethernet
  - Standard for connecting home computers to ISP
    - Via DSL or broadband cable

Remote Virtual Computing

- Allows workstation to remotely access and control another workstation
- Host may allow clients a variety of privileges
- Can send keystrokes and mouse clicks to the host
  - Receive screen output in return
- Thin client
  - Workstation that uses such software to access LAN
  - Requires very little hard disk space or processing power
Remote Virtual Computing (cont’d.)

- Advantages
  - Simple to configure
  - Runs over any connection type
  - Single host can accept simultaneous connections from multiple clients
- Popular programs
  - Microsoft Remote Desktop
  - VNC (Virtual Network Computing)
  - ICA (Independent Computing Architecture)
- Remote desktop
  - Comes with Windows client and server operating systems
- VNC (Virtual Network Computing)
  - Open source system
- ICA (Independent Computing Architecture)
  - Citrix System’s XenApp
  - Can work with virtually any operating system or application
  - Easy to use
VPNs (Virtual Private Networks)

• Logically defined networks over public transmission systems
  – Isolated from other traffic on same public lines
• Requires inexpensive software
• Important considerations
  – Interoperability
  – Security
• Types
  – Site-to-site
  – Client-to-site

• Enterprise-wide VPN
  – Can include elements of client-to-site and site-to-site models
• VPNs tailored to customer’s distance, user, and bandwidth needs
• Two major types of tunneling protocols
  – PPTP (Point-to-Point Tunneling Protocol)
  – L2TP (Layer 2 Tunneling Protocol)

Figure 10-14 Site-to-site VPN
Courtesy Course Technology/Cengage Learning
Cloud Computing

- Internet frequently pictured as a cloud
- Cloud computing
  - Flexible provision of data storage, applications, and services
    - To multiple clients over a network
- Cloud computing distinguishing features
  - Self-service and on-demand
  - Elastic
  - Supports multiple platforms
  - Resource pooling and consolidation
  - Metered service
- Can provide virtual desktops
  - Operating environments hosted virtually
  - Different physical computer than one user interacts with
- NaaS (Network as a Service)
  - Service provider offers customers complete set of networking services
- Types of delivery
  - Public cloud
  - Private cloud
Summary

1. Virtualization: emulation of a computer, operating system environment, or application on a physical system
2. VMs exist as files on physical computer's hard disk
3. Hypervisor software manages resource allocation and sharing among virtual machines
4. Virtual switch allows VMs to communicate with each other and with nodes on a physical LAN or WAN
5. Different methods of remote user access exist
6. Cloud computing provides storage, applications, or services over a network