CSIS 247 Introduction to Networking

October 2019

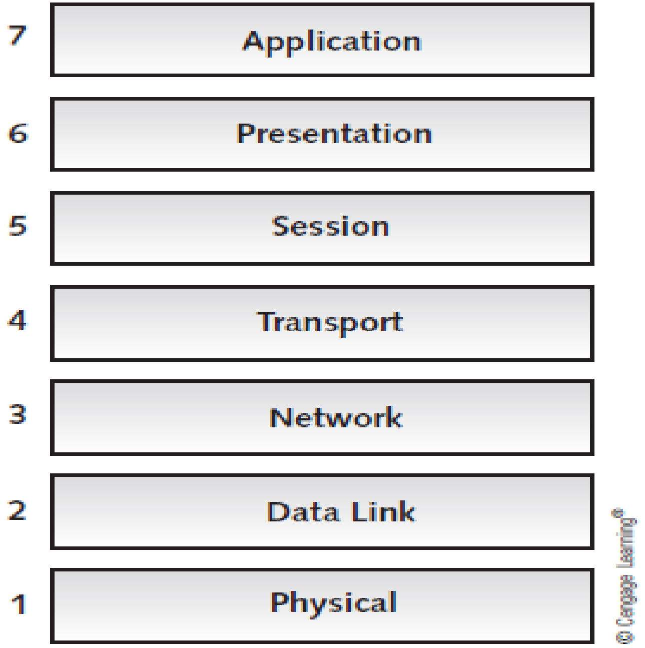
Ch 7: Network Reference Models and Standards

OSI Layer model
IEEE 802 protocols

The OSI Network Reference Model

Open Systems Interconnection (OSI) model

- proposed by the International Organization for Standards
- provides a common framework for developers and students of networking to work with and learn from



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

© Cengage Learning®

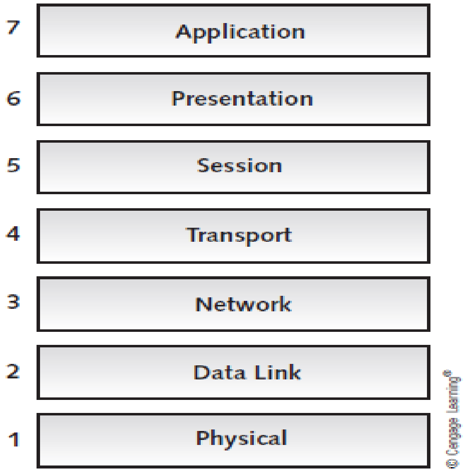
Figure 7-1 The seven layers of the OSI reference model

The OSI Network Reference Model

The **OSI** model is

- not specific to any protocol suite and can be applied to most networking protocols
- a seven-layer organization of how data travels from place to place on a network

A layered approach to a complicated process reduces its complexity and turns it into a series of interconnected tasks



7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

© Cengage Learning®

Figure 7-1 The seven layers of the OSI reference model

Structure of the OSI Model

- Each OSI layer has well-defined functions
  - The functions of each layer communicate and interact with the layers immediately above and below it
  - Example: The Transport layer works with the Network layer below it and the Session layer above it

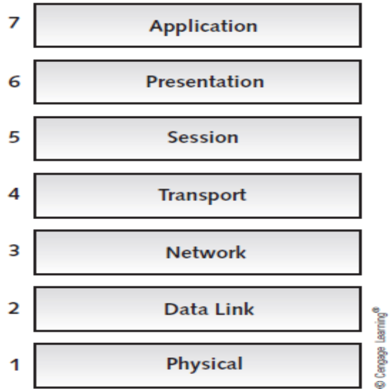
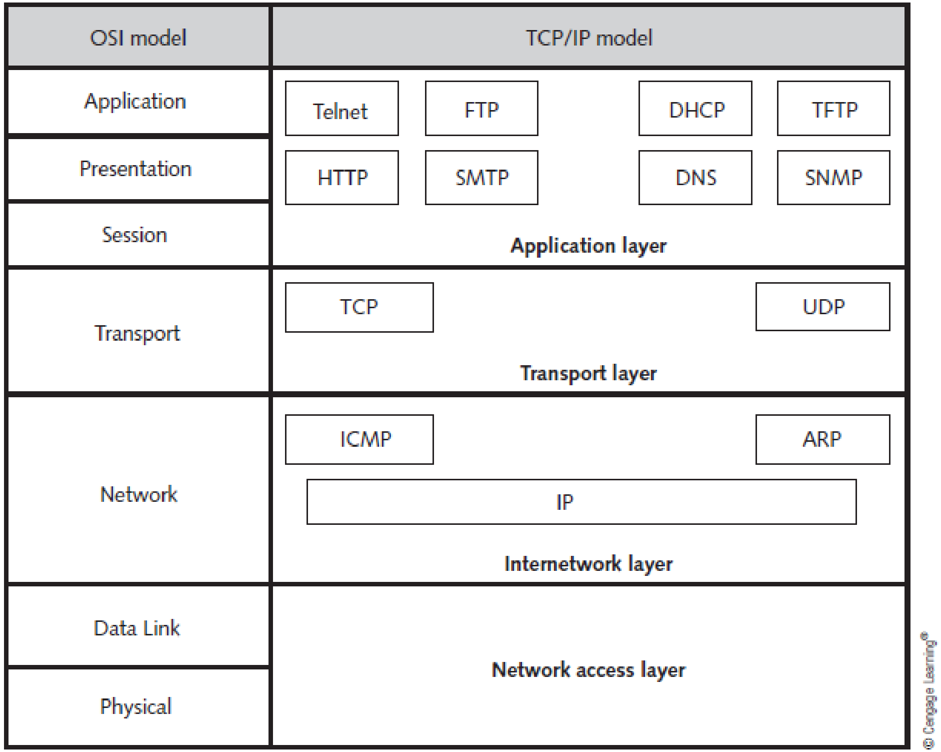


Figure 7-1 The seven layers of the OSI reference model

OSI and TCP/IP Models

We saw the TCP/IP model in previous chapters; here's how the two models line up:

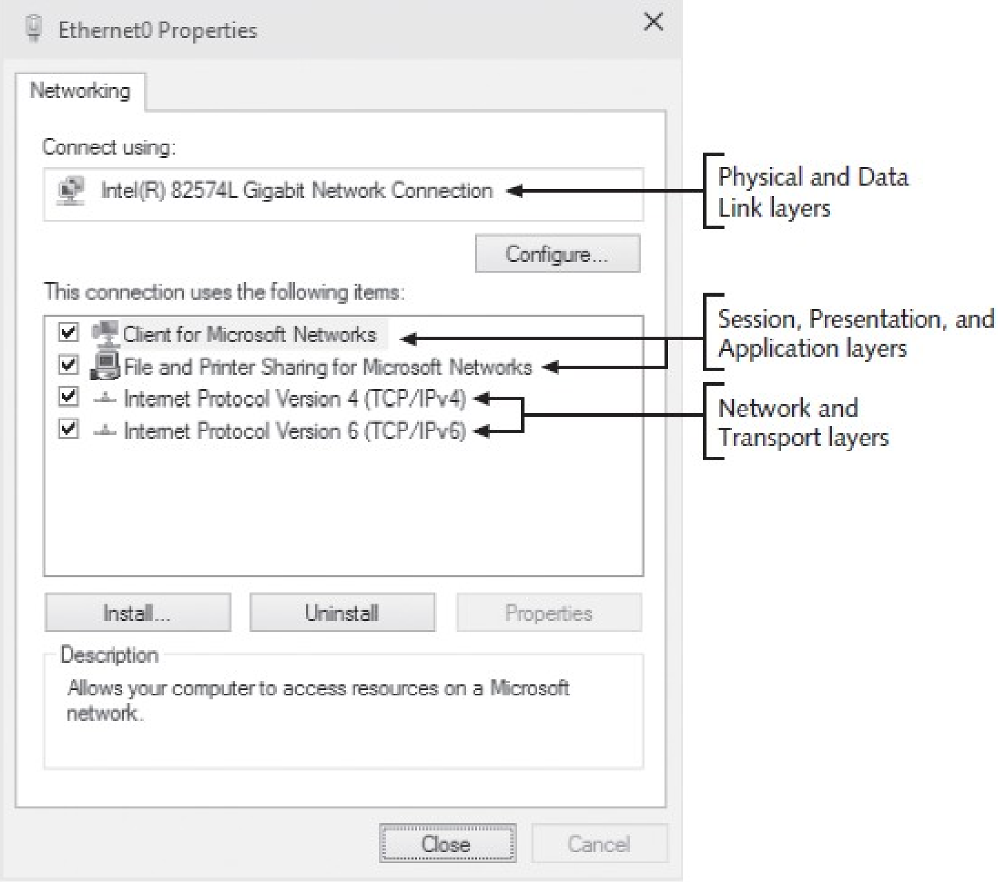


OSI model	TCP/IP model
Application	Telnet FTP DHCP TFTP HTTP SMTP DNS SNMP **Application layer**
Presentation	
Session	
Transport	TCP UDP **Transport layer**
Network	ICMP ARP IP **Internetwork layer**
Data Link	**Network access layer**
Physical	

© Cengage Learning®

Figure 7-2 Comparing the OSI model and the TCP/IP model

Structure of the OSI Model



Connect using:

Intel(R) 82574L Gigabit Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol Version 4 (TCP/IPv4)

☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Allows your computer to access resources on a Microsoft network.

Physical and Data Link layers

Session, Presentation, and Application layers

Network and Transport layers

Figure 7-3 Layers of the OSI model in the Ethernet0 Properties dialog box

Structure of the OSI Model

- Each layer provides services to the next higher layer until the data reaches the Application layer
  - Application layer has the job of providing services to user applications

- Each layer on one computer behaves as though it were communicating with the same layer on the other computer
- This is known as **peer communication** between layers

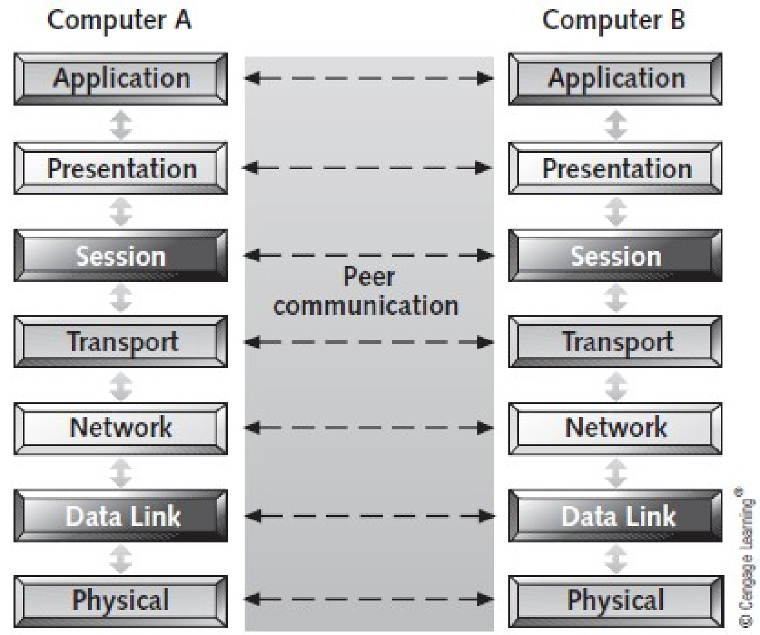


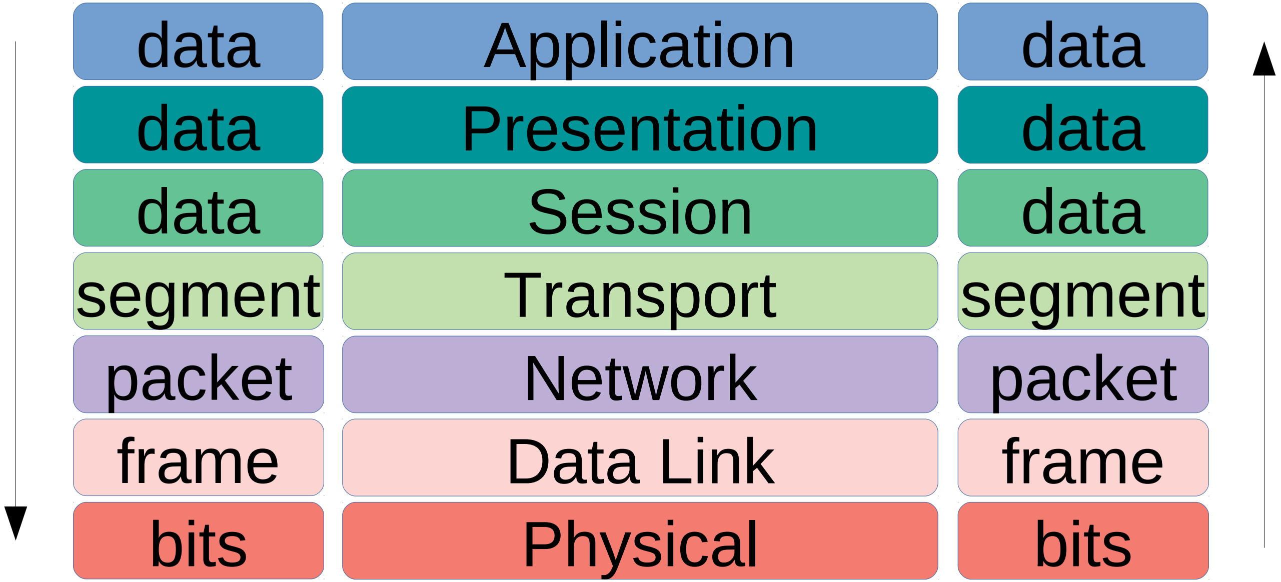
Figure 7-4 Peer communication between OSI layers

Structure of the OSI Model

- Data sent → makes its way **down** the protocol stack (model):
  - Data is divided into units called protocol data units (PDU)
  - Layers may add their own formatting to the PDU – a header (encapsulation)
- Data arrives at the receiving end → passed **up** the protocol stack:
  - Each layer reads its PDU data and strips its header information (called deencapsulation) and passes the PDU to the next higher layer
  - Packet leaves the Application layer in a format the receiving application can read

Sending vs Receiving Protocol Data Units

Data sent makes its way **down** the protocol stack



data	Application	data
data	Presentation	data
data	Session	data
segment	Transport	segment
packet	Network	packet
frame	Data Link	frame
bits	Physical	bits

At the receiving end data is passed **up** the protocol stack

Application Layer

- The Application layer (Layer 7) provides interfaces for applications to access network services
  - File sharing, message handling, and database access
- Components at the Application layer have both a client component and a server component
- Common protocols found at Layer 7 include HTTP, FTP, SMB/CIFS, TFTP, and SMTP
- Possible problems at this layer include missing or misconfigured client or server software and incompatible or obsolete commands used to communicate between a client and server

Presentation Layer

- The Presentation layer (Layer 6) handles data formatting and translation
- For outgoing messages
  - Converts data into a format specified by the Application layer
- For incoming messages
  - Reverses the conversion if required by the receiving application
- A software component known as a “redirector” operates at this layer
  - Intercepts requests for service from the computer, requests that can’t be handles locally are redirected across the network to a network resource that can handle the request

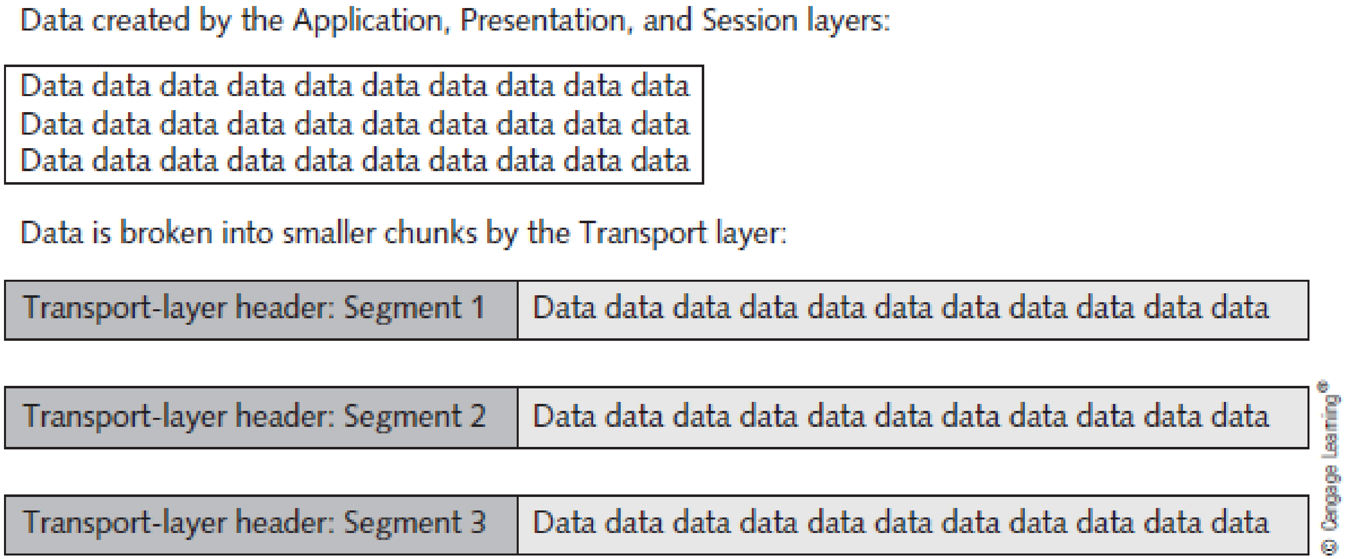
Session Layer

- Session layer (Layer 5) permits two computers to hold ongoing communications, called a “session”
- This layer handles communication setup ahead of data transfers and session teardown when the session ends
- Common network functions at this layer:
  - Name lookup, user logon and logoff
- Manages the mechanics of ongoing conversations such as identifying which side can transmit data when and for how long
- Checkpointing is performed at this layer
  - Example: keeping the audio in sync with video

Transport Layer

The Transport layer (Layer 4) manages data transfer from one application to another across a network

- Breaks data down into smaller chunks called “segments”



Data created by the Application, Presentation, and Session layers:

Data data data data data data data data data data
Data data data data data data data data data data
Data data data data data data data data data data

Data is broken into smaller chunks by the Transport layer:

Transport-layer header: Segment 1	Data data data data data data data data data data data
Transport-layer header: Segment 2	Data data data data data data data data data data data
Transport-layer header: Segment 3	Data data data data data data data data data data data

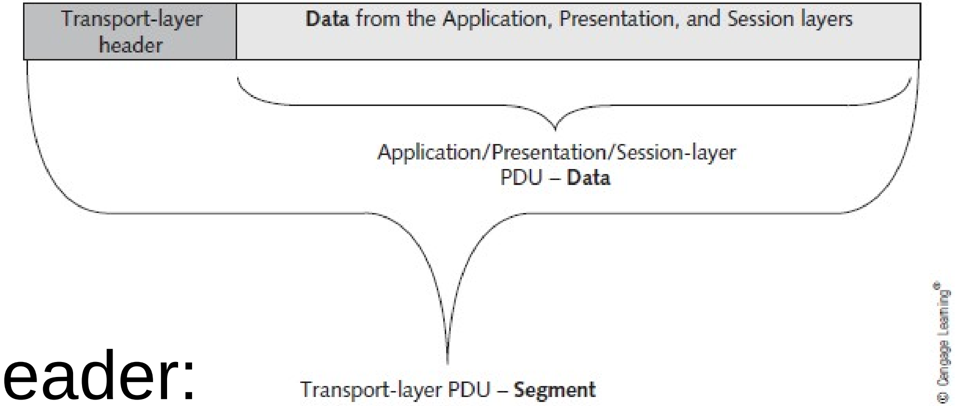
© Cengage Learning®

Figure 7-5 The Transport layer breaks data into segments

Transport Layer

- Segmenting data is important: every network technology has a maximum frame size called the **maximum transmission unit (MTU)**
- Flow control and acknowledgements used for reliability
- At receiving end, segments resequenced into the original sent data

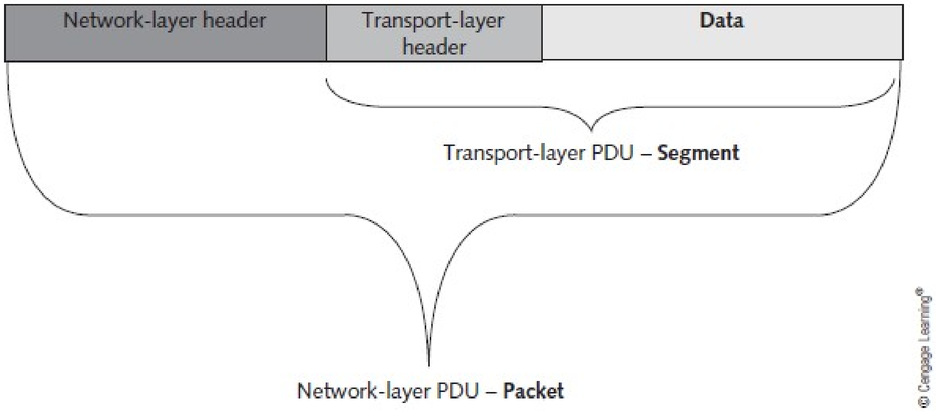
Transport Layer


Transport-layer header
Data from the Application, Presentation, and Session layers
Application/Presentation/Session-layer PDU – **Data**
Transport-layer PDU – **Segment**

© Cengage Learning®

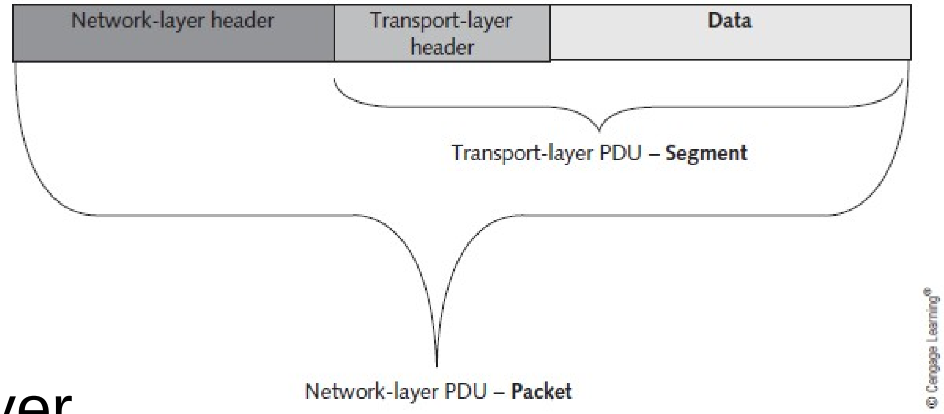
- Key fields in the Transport-layer header:
  - *Source and destination port numbers*
  - *Sequence and acknowledgement numbers*
  - *Window size*
- Problems at this layer include segments that are too large for the medium between source and destination networks
  - Forces the Network layer to fragment the segments, which causes performance degradation

Network Layer



The Network layer (Layer 3) handles logical addressing, translates logical network addresses (IP addresses) into physical addresses(MAC addresses), and performs best path selection and routing in an internetwork

Network Layer



Routers operate at this layer

- **Access control** is handled at this layer during the routing process:
  - □ Before forwarding an incoming packet, a router will consult its list of rules to determine whether it should be permitted through
- Software working at this layer include IP, ARP and ICMP
- Problems that occur at the Network layer:
  - Incorrect IP addresses or subnet masks
  - Incorrect router configuration
  - Router operation errors

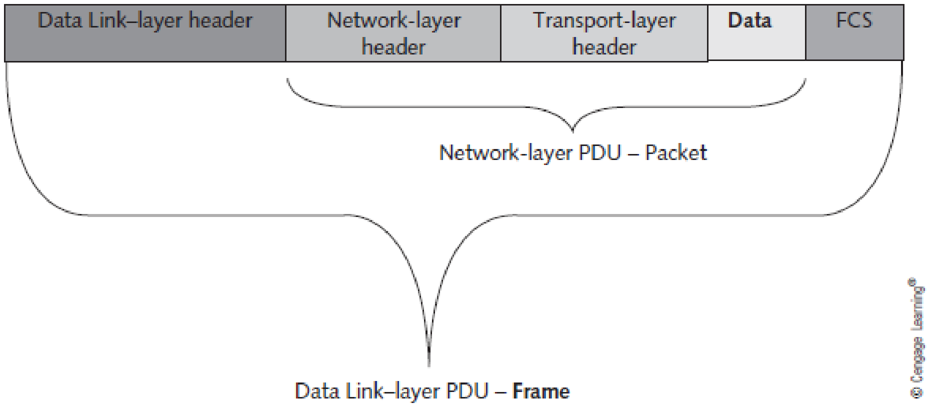
Data Link Layer (Layer 2)

- Intermediary between the Network layer and Physical layer

- Works with frames

- Defines how computers access the network medium (also called media access control)
  - MAC address is defined at this layer

Data Link Layer



A layer 2 frame consists of both a header and a trailer component

- Trailer component is labeled “FCS” (frame check sequence) and contains the CRC error-checking code

Data Link Layer

- The software component operating at this layer is in the NIC driver
- Hardware components that operate at this layer include NICs and switches
- Problems at this layer include collisions and invalid frames
  - Can be caused by collisions, poor network design, line noise, or NIC driver problems

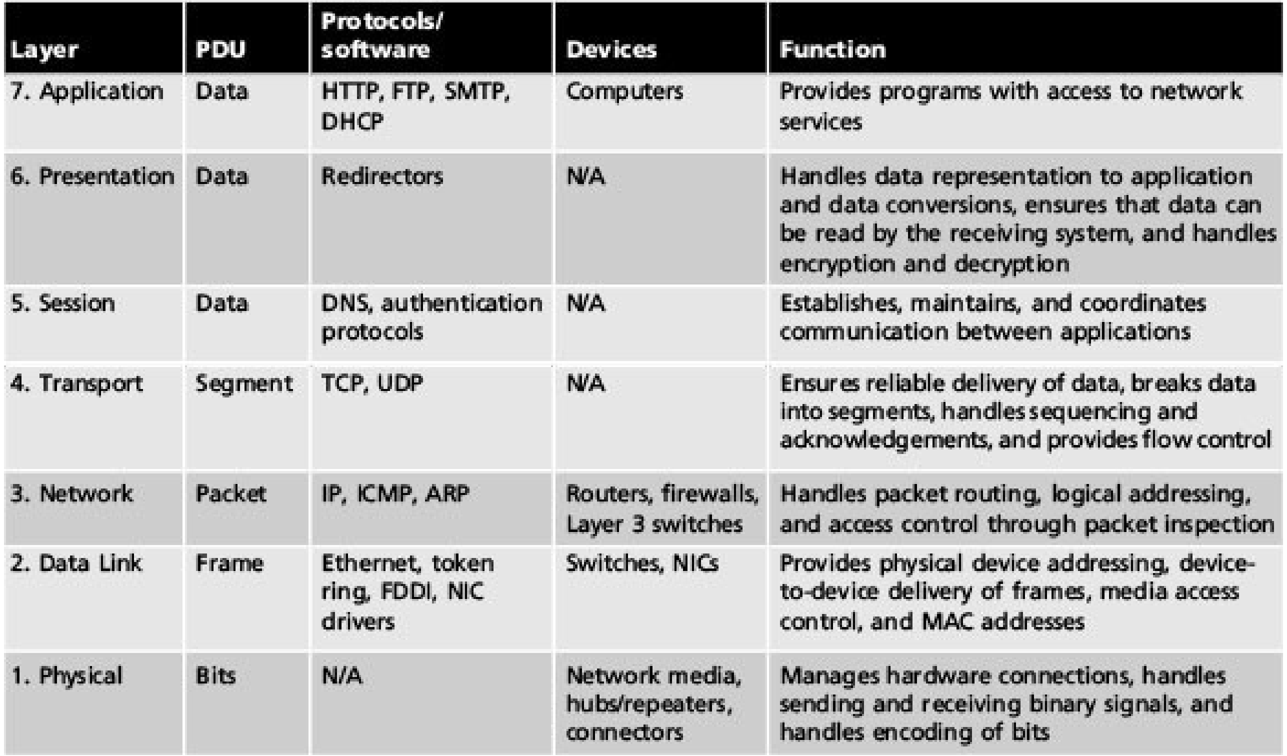
Physical Layer

- The Physical layer (Layer 1) converts bits into analog signals for outgoing messages and analog signals into bits for incoming messages
  - Wire media uses electrical pulses, fiber-optic uses light pulses and wireless media uses radio waves
- Details for creating a physical network connection are specified at this layer
  - Example: type of connectors used to attach the medium to the NIC

Physical Layer

- **Encoding** (representing 0s and 1s using an analog physical signal) happens at this layer
  - Such as electrical voltage or a light pulse
- Components at this layer include all the cable and connectors used on the medium, repeaters and hubs
- Problems occurring here are often related to:
  - Incorrect media termination
  - EMI or noise that scrambles the signals
  - NICs and hubs are misconfigured or malfunctioning

Summary of the OSI Model



Layer	PDU	Protocols/ software	Devices	Function
7. Application	Data	HTTP, FTP, SMTP, DHCP	Computers	Provides programs with access to network services
6. Presentation	Data	Redirectors	N/A	Handles data representation to application and data conversions, ensures that data can be read by the receiving system, and handles encryption and decryption
5. Session	Data	DNS, authentication protocols	N/A	Establishes, maintains, and coordinates communication between applications
4. Transport	Segment	TCP, UDP	N/A	Ensures reliable delivery of data, breaks data into segments, handles sequencing and acknowledgements, and provides flow control
3. Network	Packet	IP, ICMP, ARP	Routers, firewalls, Layer 3 switches	Handles packet routing, logical addressing, and access control through packet inspection
2. Data Link	Frame	Ethernet, token ring, FDDI, NIC drivers	Switches, NICs	Provides physical device addressing, device-to-device delivery of frames, media access control, and MAC addresses
1. Physical	Bits	N/A	Network media, hubs/repeaters, connectors	Manages hardware connections, handles sending and receiving binary signals, and handles encoding of bits

Table 7-2 OSI model summary

IEEE 802 Networking Standards

- The Institute of Electrical and Electronics Engineers (IEEE) defined LAN standards to ensure that network interfaces and cabling from multiple manufacturers would be compatible
  - This effort was called Project 802 to indicate the year (1980) and the month (Feb) of its inception
- IEEE 802 predates the OSI Model
- Most of the standards affect the elements from the lower two levels of the OSI Model
  - Describes how NICs can access and transfer data across a variety of networking media and what's involved in attaching these devices in a network

IEEE 802 Specifications

The IEEE numbers the collections of 802 documents starting with 802.1, 802.2, etc…

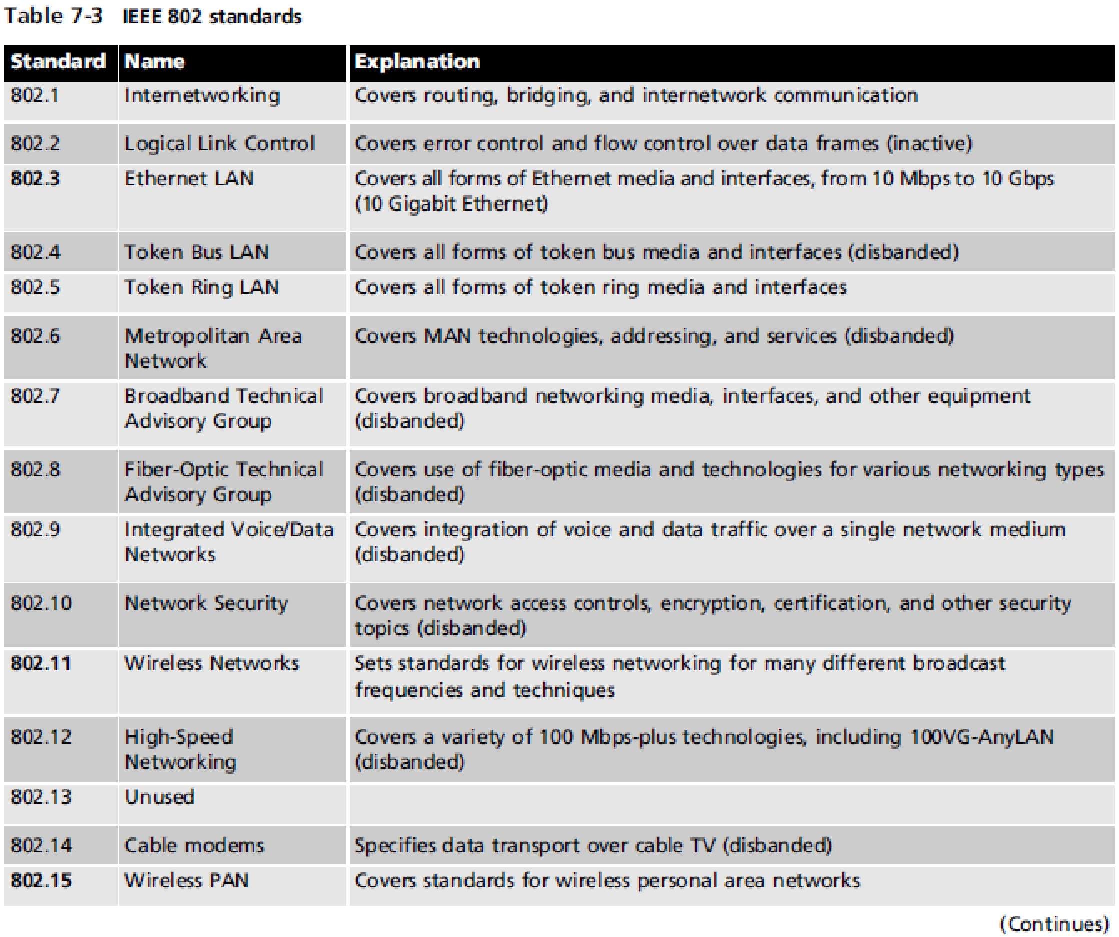


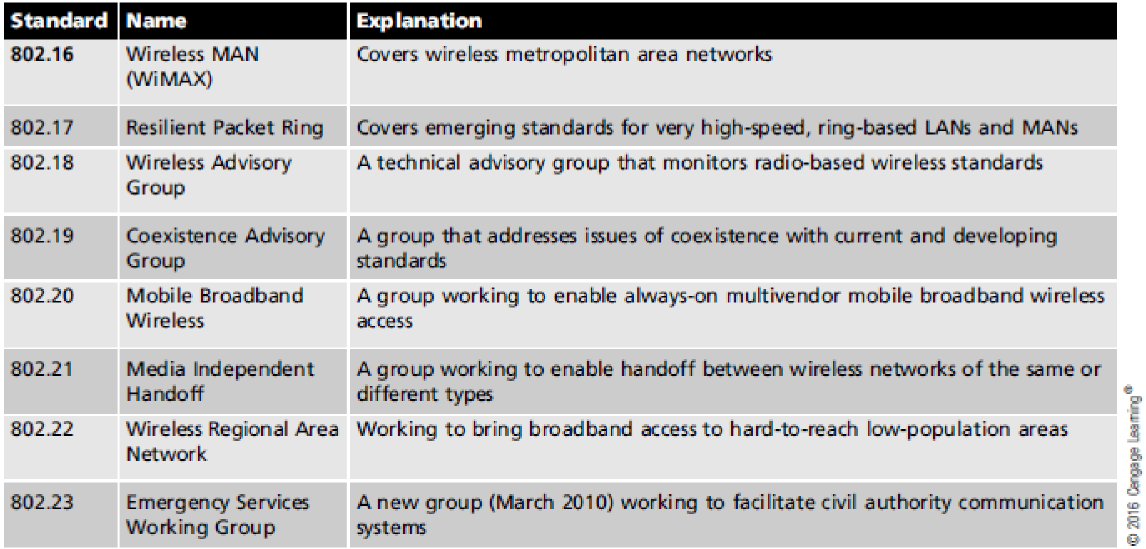
Table 7-3 IEEE 802 standards

Standard	Name	Explanation
802.1	Internetworking	Covers routing, bridging, and internetwork communication
802.2	Logical Link Control	Covers error control and flow control over data frames (inactive)
802.3	Ethernet LAN	Covers all forms of Ethernet media and interfaces, from 10 Mbps to 10 Gbps (10 Gigabit Ethernet)
802.4	Token Bus LAN	Covers all forms of token bus media and interfaces (disbanded)
802.5	Token Ring LAN	Covers all forms of token ring media and interfaces
802.6	Metropolitan Area Network	Covers MAN technologies, addressing, and services (disbanded)
802.7	Broadband Technical Advisory Group	Covers broadband networking media, interfaces, and other equipment (disbanded)
802.8	Fiber-Optic Technical Advisory Group	Covers use of fiber-optic media and technologies for various networking types (disbanded)
802.9	Integrated Voice/Data Networks	Covers integration of voice and data traffic over a single network medium (disbanded)
802.10	Network Security	Covers network access controls, encryption, certification, and other security topics (disbanded)
802.11	Wireless Networks	Sets standards for wireless networking for many different broadcast frequencies and techniques
802.12	High-Speed Networking	Covers a variety of 100 Mbps-plus technologies, including 100VG-AnyLAN (disbanded)
802.13	Unused	
802.14	Cable modems	Specifies data transport over cable TV (disbanded)
802.15	Wireless PAN	Covers standards for wireless personal area networks

(Continues)

IEEE 802 Specifications

Table 7-3 IEEE 802 standards (continued)

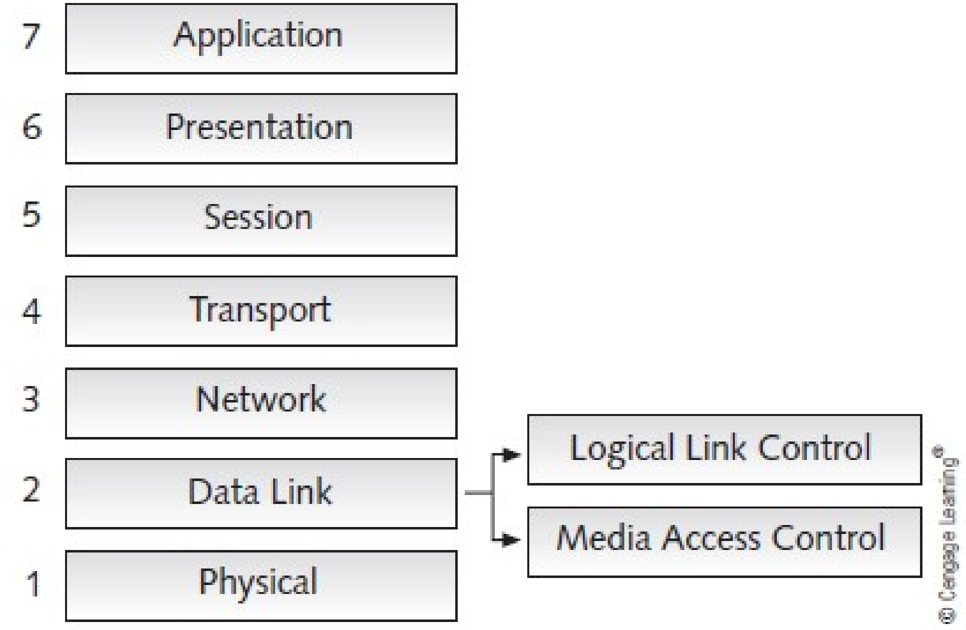


Standard	Name	Explanation
802.16	Wireless MAN (WiMAX)	Covers wireless metropolitan area networks
802.17	Resilient Packet Ring	Covers emerging standards for very high-speed, ring-based LANs and MANs
802.18	Wireless Advisory Group	A technical advisory group that monitors radio-based wireless standards
802.19	Coexistence Advisory Group	A group that addresses issues of coexistence with current and developing standards
802.20	Mobile Broadband Wireless	A group working to enable always-on multivendor mobile broadband wireless access
802.21	Media Independent Handoff	A group working to enable handoff between wireless networks of the same or different types
802.22	Wireless Regional Area Network	Working to bring broadband access to hard-to-reach low-population areas
802.23	Emergency Services Working Group	A new group (March 2010) working to facilitate civil authority communication systems

- When a technology is enhanced each new enhancement is specified by letters after the number
  - For example: 802.3 is the original Ethernet and 802.3u specifies 100BaseT Ethernet
- These tables list the major 802 categories
  - The 802.3 and 802.11 are the most widely used technologies of Ethernet and Wi-Fi, as of this point

IEEE 802 Extensions to the OSI Reference Model

The two lowest layers of the OSI model define how computers attach to specific network media



© Cengage Learning®

Figure 7-9 The IEEE 802 standard divides the OSI Data Link layer into two sublayers

IEEE 802 expands the OSI model: separates Data Link layer into 2 sublayers:

- Logical Link Control (LLC) sublayer – controls data-link communication, defines the use of logical interface points used to communicate to the Network layer
- Media Access Control (MAC) sublayer – manages access to the physical medium and communicates with the Physical layer

Summary

- The OSI reference model and IEEE Project 802 define a frame of reference for networking and specify the operation of most networking technologies in current use
- The OSI reference model separates networking into seven layers, each with its own purposes and activities

Summary of OSI Model layer functions

- Application – Provides access to network resources
- Presentation – Handles data formatting and translation
- Session – Manages ongoing conversations between two computers
- Transport – Breaks long data streams into smaller chunks (segments)
- Network – Provides best path selection and IP addressing
- Data Link – Defines how computers access the media
- Physical – Converts bits into signals and defines media and connectors

Summary

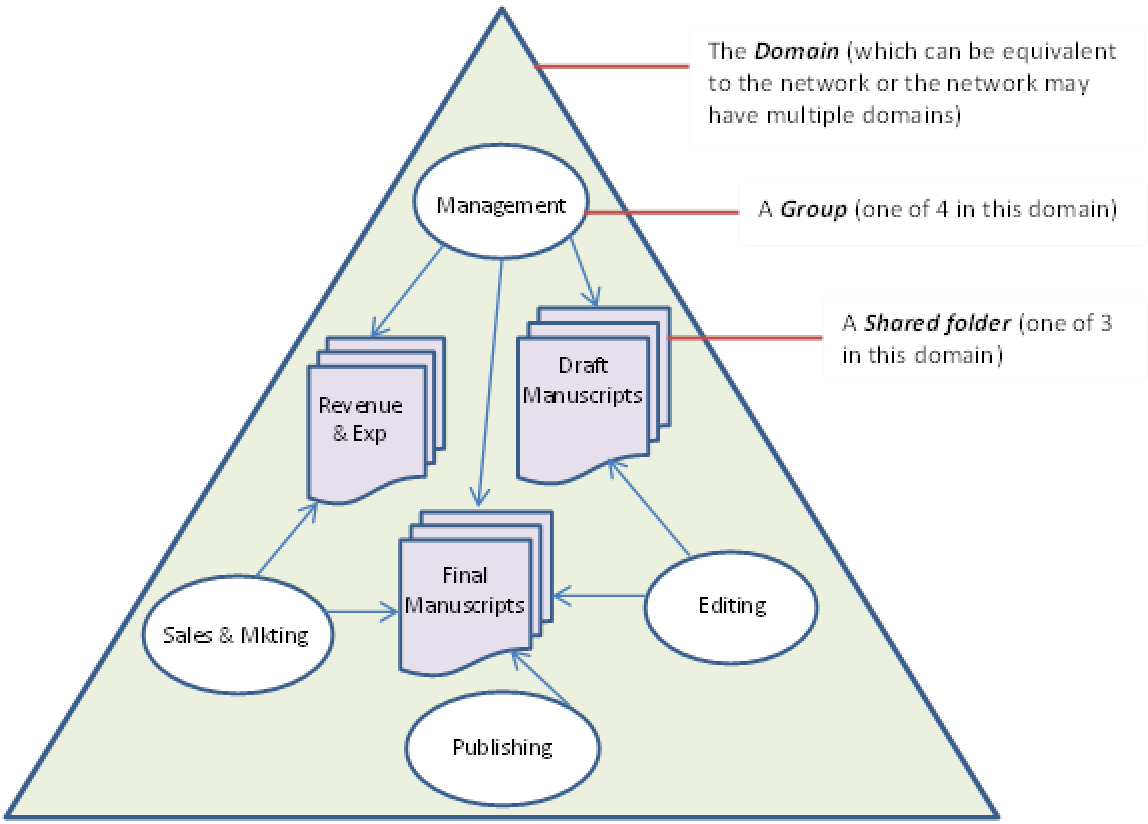
The IEEE 802 project defines a set of networking standards to ensure that network interfaces and cabling from multiple manufacturers would be compatible.

IEEE 802.2 specifies a Logical Link Control (LLC) and Media Access Control (MAC) sublayer

Ch 12: Network Management and Administration

Windows Server Active Directory
Users and Groups
Storage and Files
Shared Files and Printers

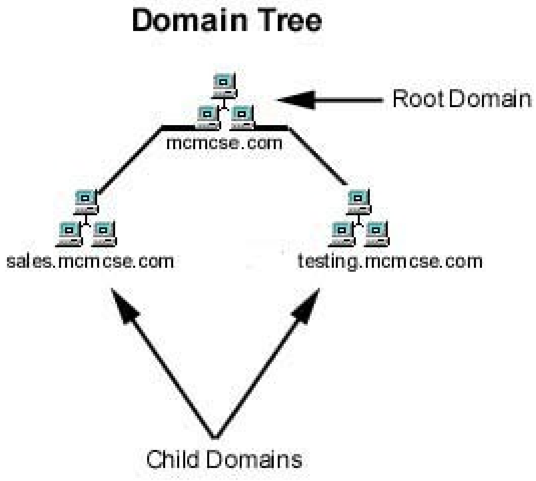
Hierarchical view of Active Directory



The *Domain* (which can be equivalent to the network or the network may have multiple domains)

A *Group* (one of 4 in this domain)

A *Shared folder* (one of 3 in this domain)



Users and Groups

- User accounts have two main functions:
  - Provide a method for users to authenticate themselves to the network
  - Provide detailed information about a user
- Group accounts are used to organize users so that assignment of resource permissions and rights can be managed more easily than working with dozens or hundreds of individual user accounts

Windows Accounts

When Windows is first installed, two users are created:

- `Administrator` and `Guest` (usually disabled)

The `Administrator` account has full access to a computer

Windows domain users are created in Active Directory Users and Computers

You can create folders for organizing users and groups (called organization units or OUs)

Creating a User Account

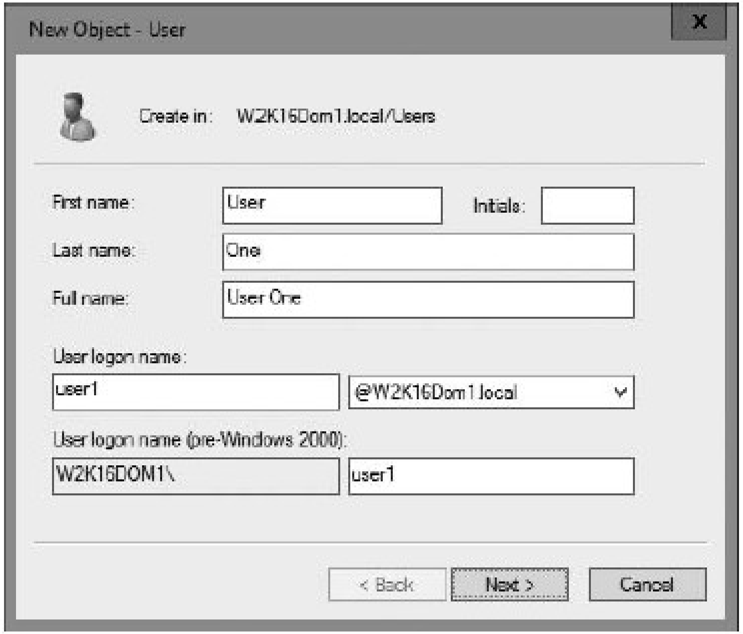
To create a new Active Directory (AD) user:

In the “AD Users and Computers” window,

right-click Users folder → New → User.

Everything we create in AD is an “object”

→ a New Object – User Dialog box appears



Create in: W2K16Dom1.local/Users

First name: User

Initials:

Last name: One

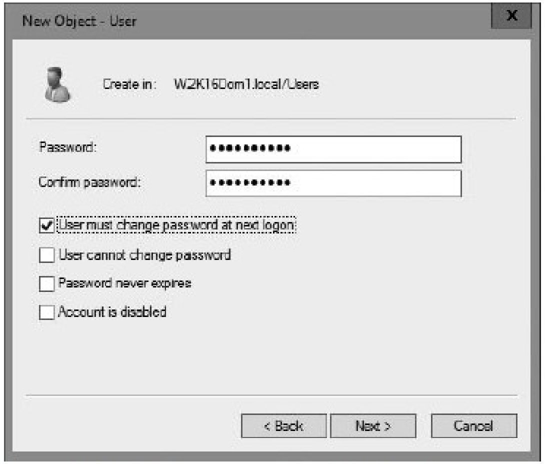
Full name: User One

User logon name: user1 @W2K16Dom1.local

User logon name (pre-Windows 2000): W2K16DOM1\ user1

Figure 12-2 Creating a user in Active Directory

Many settings for things like password policies:



Create in: W2K16Dom1.local/Users

Password: •••••••••••

Confirm password: •••••••••••

☑ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Figure 12-3 Setting the password and additional account options

and many more!

Creating Groups

A Group only requires a name in order to be created (other options can be configured later)

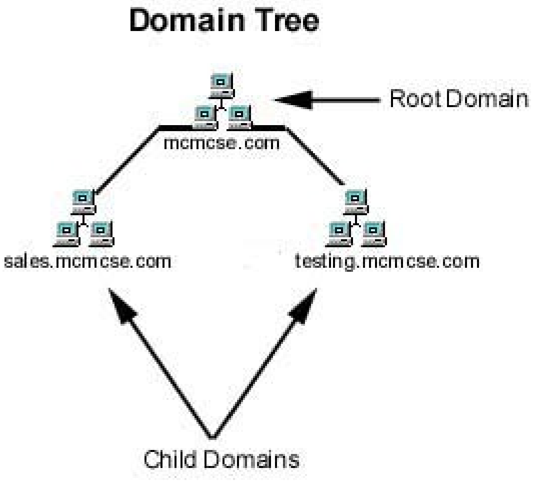
Group scope has three options:

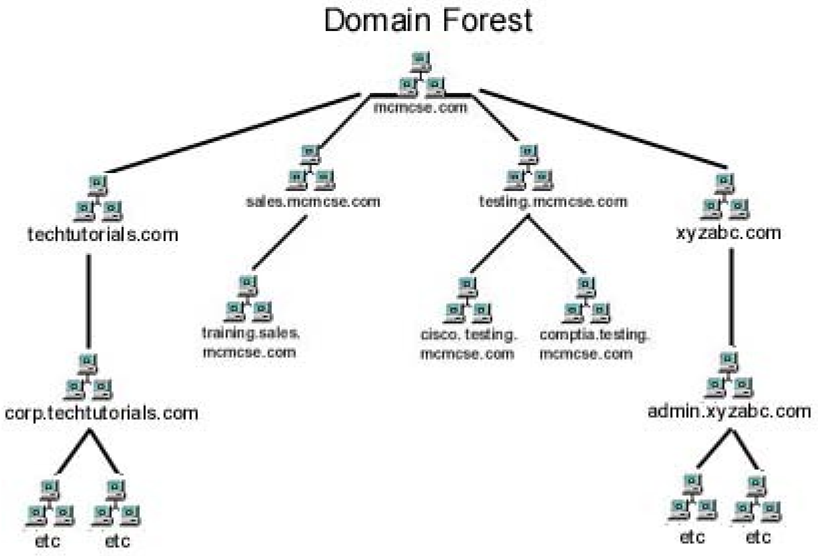
Domain local – Can be used to assign permissions to resources only in the domain in which the group is created

Global – The default option and contains users from the domain in which they are created but can be assigned permissions to resources in other domains

Universal – Used in multidomain networks; users from any domain can be members and be assigned permission to resources in any domain

Hierarchical view of Active Directory





Storage and File System Management

- Network admins need to:
  - Make sure space is available to store files needed
  - Manage access to file storage
  - Prevent users from storing inappropriate types of data on company servers
- Locally attached storage – a device, such as a hard disk, that is connected to a storage controller on the server

Volumes and Partitions

- A **volume** is part or all of the space on one or more disks that contains (or is ready to contain) a file system
  - In Windows, volumes are assigned a drive letter
  - In Linux, volumes are accessed as though they were a folder
- The term **partition** is sometimes used interchangeably with volume but don’t always describe the same thing
  - In Windows, a basic disk can be divided into one to four partitions
  - A **primary partition** can be formatted with a file system and assigned a drive letter (considered a volume)
  - An **extended partition** is divided into one or more logical drives that can be formatted and assigned a drive letter (considered a volume)

Volumes and Partitions

- Only a primary partition can be the **active partition** (partition that can hold boot files)
- The active primary partition storing the Windows boot loader is referred to as the **system partition**
- The partition or logical drive holding the Windows OS files is called the **boot partition**
- A **dynamic disk** can be divided into one or more volumes; the term partition is not used in this context

The FAT file system

- The File Allocation Table (FAT) file system has two variations:
    - FAT16 is usually referred to as FAT and has been around since the mid-1980s
        - Supported by most OSs
    - FAT32 was released with Windows 95 OSR2 in 1996
- FAT16 is limited to 2 GB partitions in most cases
- FAT32 allows partitions up to 2 TB but in Windows 2000 and later, Microsoft limits them to 32 GB because the file system becomes noticeable slower with larger partition sizes

The NTFS file system

- NTFS is a file system that Microsoft introduced in 1993 with Windows NT to improve on FAT.
- Features in NTFS that are not available in FAT:
  - *Disk quotas* – limit amount of data users' files can occupy
  - *Volume mount points* – No need for a drive letter to access
  - *Shadow copies* – allows users to restore older file versions or files that were accidentally deleted
  - *File compression* – files can be compressed
  - *Encrypting File System* – makes encrypted files inaccessible to everyone except the user who encrypted the file
    - Including users who have been granted permission to the file

NTFS permissions

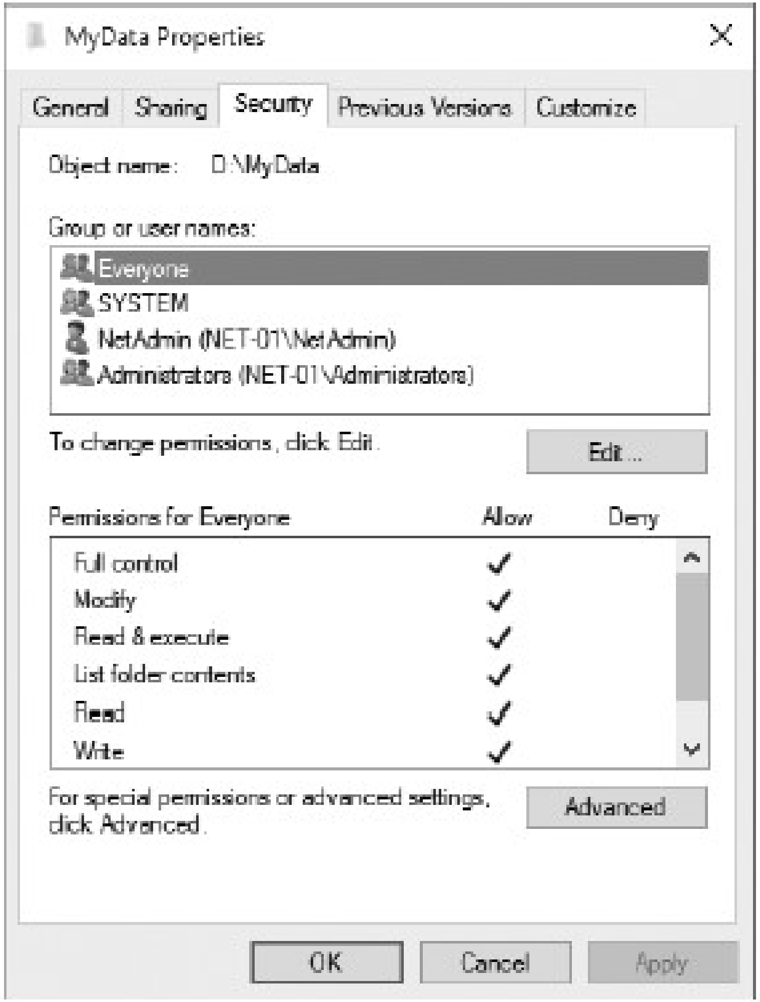
- Two modes for accessing files on a networked computer:
  - Network (sometimes called remote)
  - Interactive (sometimes called local)
- Share permissions are applied when a user attempts network access to shared files
- NTFS permissions always apply
  - Whether file access is attempted interactively or remotely through a share
- Permissions can be viewed as a gatekeeper to control who has access to folder and files

NTFS permissions

- General security rule for assigning permissions:
  - Give a user the least access necessary for their job
- NTFS permissions can be configured on folders and files
- By default, when permissions are configured on a folder, subfolders and files in that folder inherit the permissions but can be changed by the admin
- To view or edit permissions on an NTFS folder, access the Security tab of the Properties dialog box

NTFS standard permissions for files and folders

- *Read*
- *Read & execute*
- *List folder contents*
- *Write*
- *Modify*
- *Full control*



Object name: D:\MyData

Group or user names:

- Everyone
- SYSTEM
- NetAdmin (NET-01\NetAdmin)
- Administrators (NET-01\Administrators)

To change permissions, click Edit.

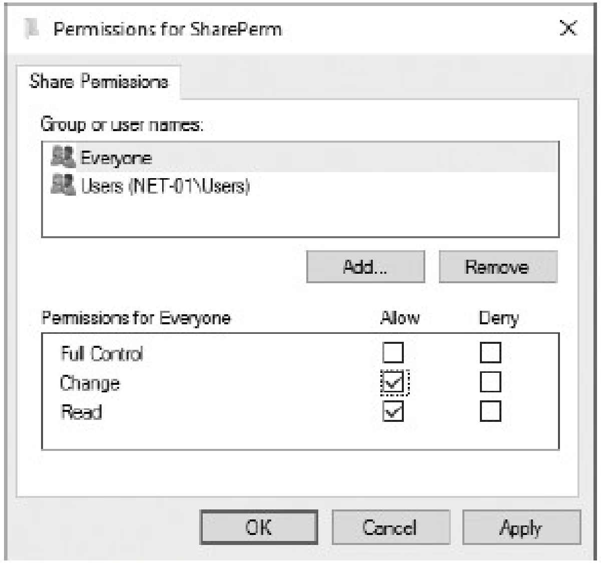
Permissions for Everyone	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Figure 12-15 NTFS permissions

Sharing Files in Windows

- Windows users are subject to both Share and NTFS permissions when accessing network files
- Share permissions are somewhat simpler than NTFS permissions with only 3 options:
  - *Read*
  - *Change*
  - *Full Control*



Permissions for SharePerm

Share Permissions

Group or user names:

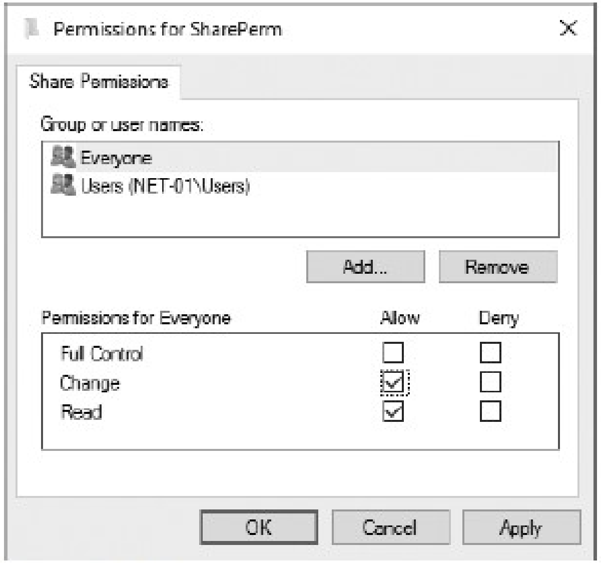
- Everyone
- Users (NET-01\Users)

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

Figure 12-20 Viewing share permissions

Groups with NTFS Permissions

- To simplify administration, we can grant permissions using groups.
- By assigning NTFS permissions to a group, we grant permissions to one or more people simultaneously, reducing the number of entries in each access list, as well as the amount of effort required to grant multiple people access to certain files or folders.



Group or user names:

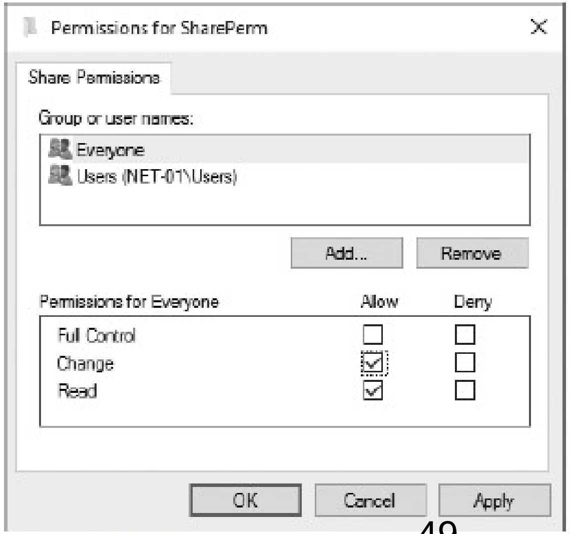
Everyone
Users (NET-01\Users)

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

Figure 12-20 Viewing share permissions

Types of NTFS Permissions

- Two types of permissions used in NTFS:
  - Explicit permissions: Permissions granted directly to a file or folder.
  - Inherited permissions are granted to a folder (parent object or container) and flow into child objects (subfolders or files inside the parent folder).
- Besides granting the Allow permissions, we can also grant the Deny permission.



Group or user names:

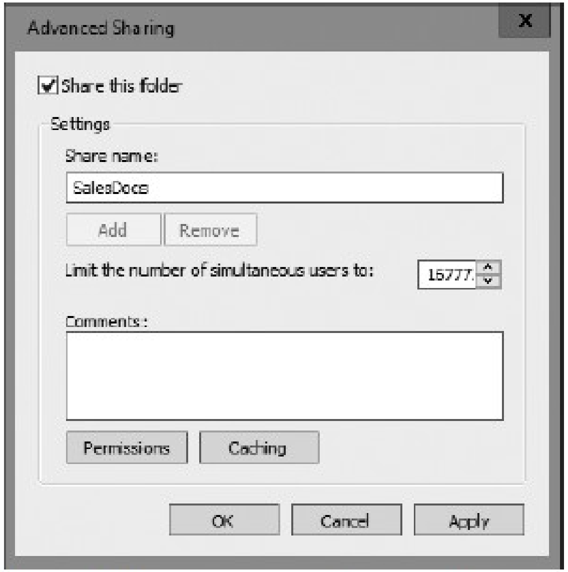
- Everyone
- Users (NET-01\Users)

Permissions for Everyone	Allow	Deny
Full Control	☐	☐
Change	☑	☐
Read	☑	☐

Figure 12-20 Viewing share permissions

Sharing Files in Windows

- Ways to configure shares:
  - *File Sharing Wizard:* right-click a folder → Share with → choose specific people
  - *Advanced Sharing dialog box:* click Advanced Sharing in the Sharing tab of a folder's Properties dialog box



Advanced Sharing

☑ Share this folder

Settings

Share name: SalesDocs

Limit the number of simultaneous users to: 16777

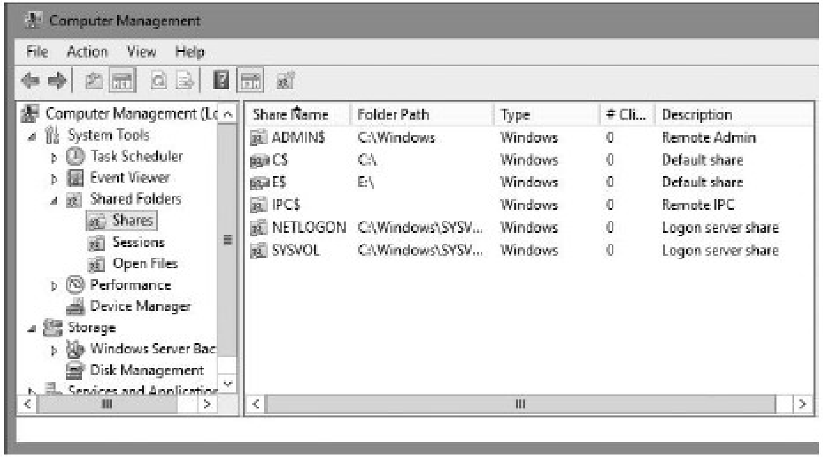
Comments:

Figure 12-22 The Advanced Sharing dialog box

Sharing Files in Windows

Ways to configure shares:

- *Shared Folder snap-in* — an MMC component



Share Name	Folder Path	Type	# Cli...	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
E$	E:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC
NETLOGON	C:\Windows\SYSV...	Windows	0	Logon server share
SYSVOL	C:\Windows\SYSV...	Windows	0	Logon server share

Figure 12-23 The Shared Folders snap-in

- *File and Storage Services* — A Server Manager component, a more advanced method for creating shares

Share Permissions

The “share permissions” available are:

- Full control
- Change
- Read

Since a user can be a member of many groups, it is possible for one to have several sets of explicit permissions for a particular folder or file.

When this occurs, the permissions are **combined** to form the **effective permissions**, which are the actual permissions when logging in and accessing a file or folder.

Network Printing

One basic network service is network printing:

allows users of different computers to share the same printer.

Cost-effective solution when we have multiple employees in different locations.

As an administrator, you can install two types of printers: local and network.

Sharing Printers in Windows

Components of a shared printer:

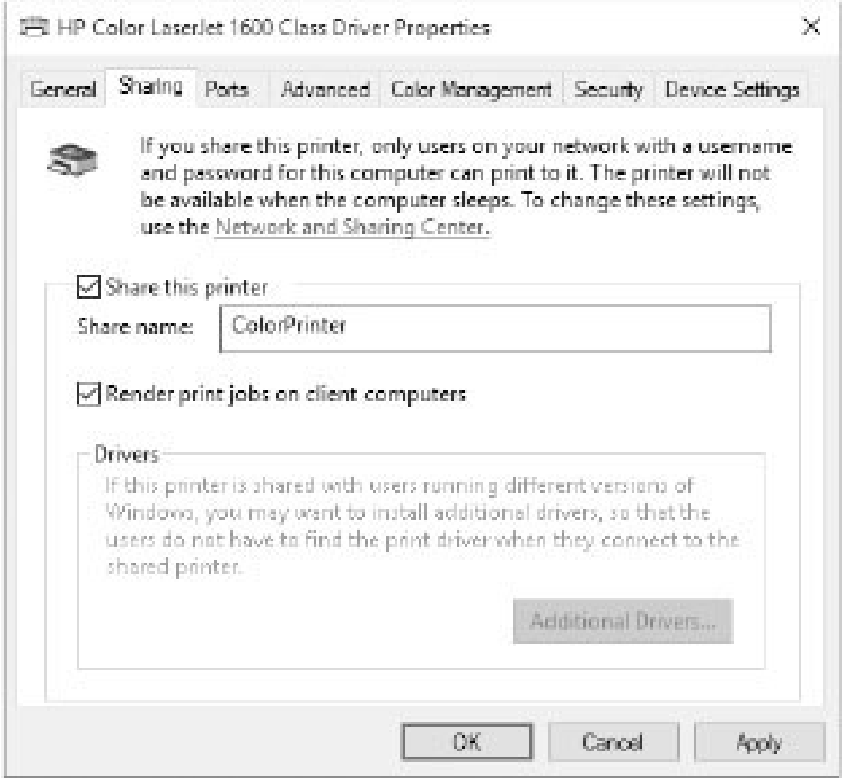
- *Print device* – Two basic types of print device:
  - Local print device: Connected to an I/O port on a computer
  - Network print device: A printer attached to and shared by another computer
- *Printer* – The icon in the Printers folder that represents print devices
- *Print server* – A Windows computer sharing a printer
- *Print queue* – Storage for print jobs awaiting printing

A printer on the network, uses a “Standard TCP/IP Port”.

The TCP/IP printer port uses host port 9100 to communicate.

Benefits of Sharing Printers

- *Access control*
- *Printer pooling*
- *Printer priority*
- *Print job management*
- *Availability control*



If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

☑ Share this printer

Share name: ColorPrinter

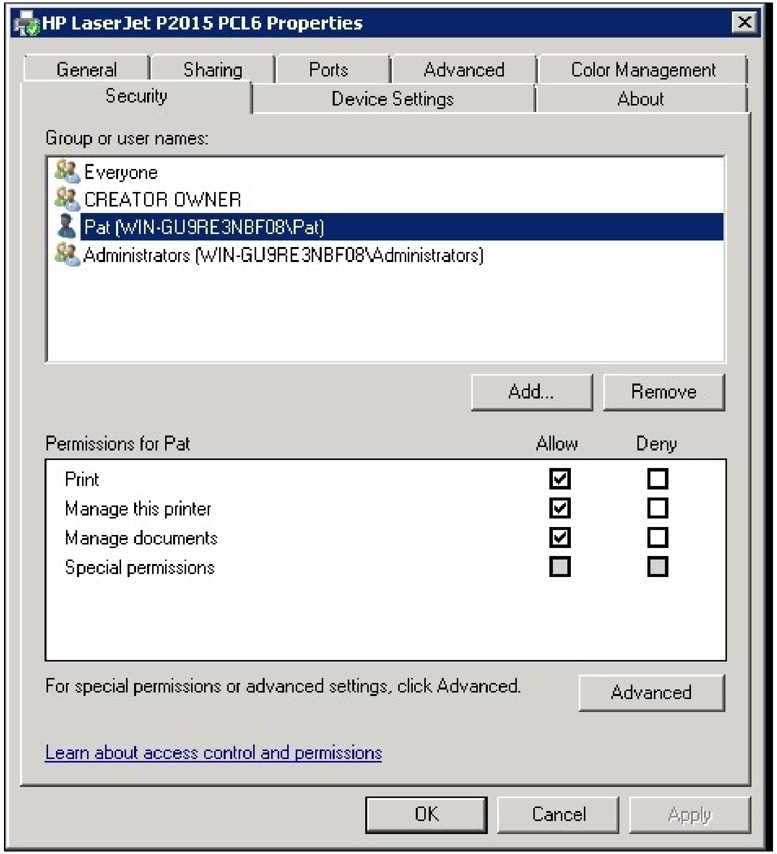
☑ Render print jobs on client computers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

Figure 12-24 The Sharing tab for a print server

Printer Permissions

- Printers are “objects”.
- We can assign permissions to a printer to specify who can:
  - use the printer
  - manage it
  - manage the print jobs.



Group or user names:

- Everyone
- CREATOR OWNER
- Pat (WIN-GU9RE3NBF08\Pat)
- Administrators (WIN-GU9RE3NBF08\Administrators)

Permissions for Pat	Allow	Deny
Print	☑	□
Manage this printer	☑	□
Manage documents	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions