CSIS 247 Introduction to Networking

October 2019

Ch 6: IP Addressing

Configuring IPv4 Addresses

Configuring Multiple IP Addresses

- Windows OSes allow assigning multiple IP addresses to a single network connection, via Advanced TCP/IP settings dialog box
- Multiple IP addresses can be useful in these situations:
  - The computer is hosting a service that must be accessed by using different addresses
  - The computer is connected to a physical network that hosts multiple IP networks

Configuring the Default Gateway

- A **default gateway** is almost always used in IP configurations
- The default gateway's address must have the same network ID as the host's network ID
- Just as you can configure multiple IP addresses, multiple gateways can be configured
- Windows attempts to select the gateway with the best metric automatically
- **Metric** is a value assigned to the gateway based on the speed of the interface used to access the gateway

Configuring the Default Gateway

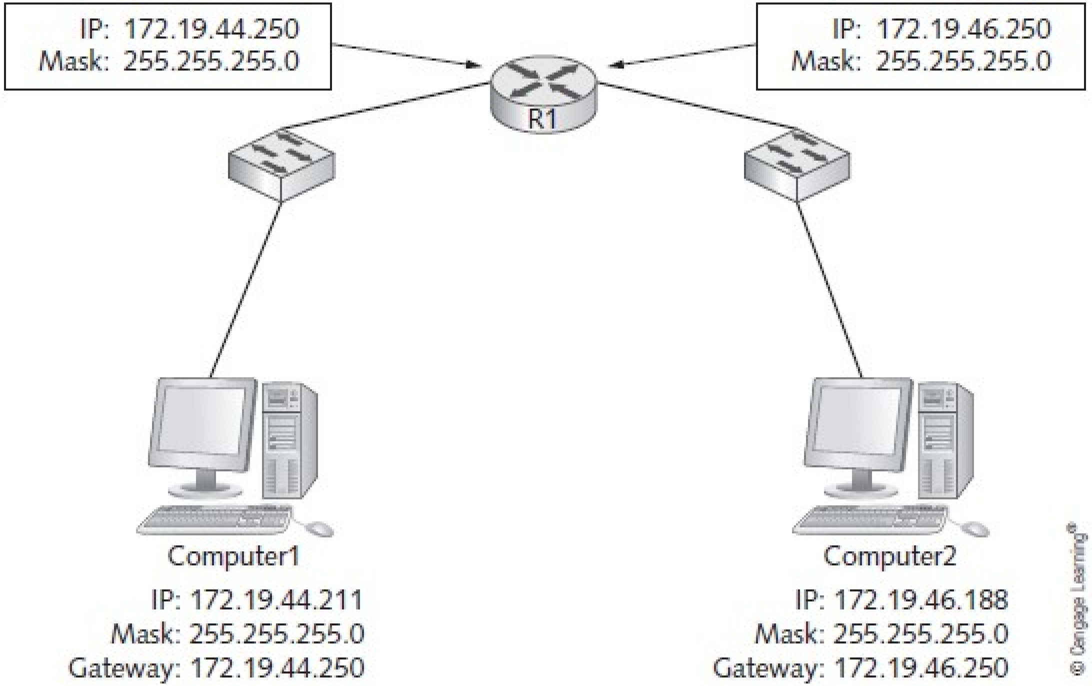
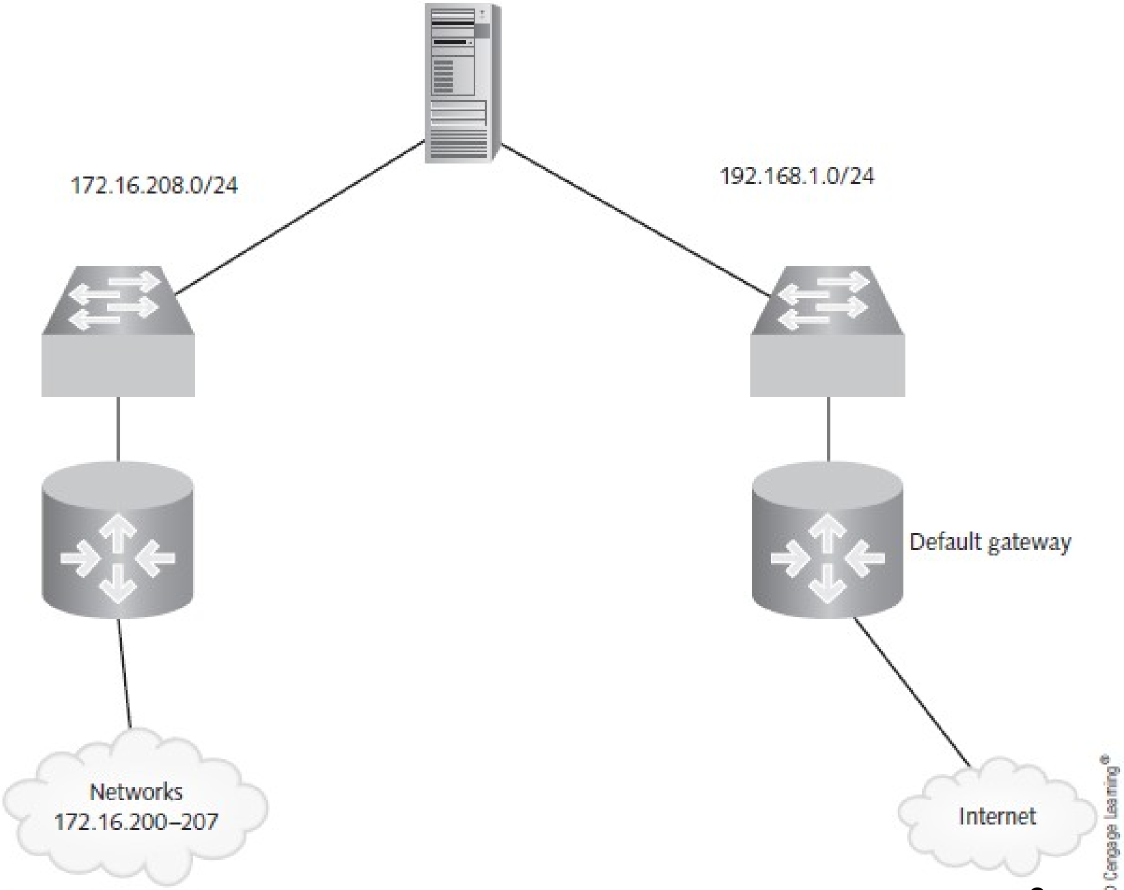


Figure 6-5 Determining the destination computer's network address with the subnet mask

Multihomed Servers

- A **multihomed server** has two or more NICs, each attached to a different IP network
- Each NIC requires its own IP address for the network to which it's connected



© Cengage Learning®

Figure 6-7 A multihomed server

Using Multihomed Servers

- Reasons for this type of configuration:
  - A server is accessed by internal clients and external clients
  - A server provides resources for computers on multiple subnets of the network
  - A server is configured as a router or VPN server
- Multihomed servers can run into routing issues due to multiple default gateways being configured

Using the `route` Command

- Windows computers maintain a routing table that dictates where a packet should be sent, based on the packet’s destination address
- Use the command **`route print`** `to` display the routing table
- Results are displayed in five columns:
  - **`Network Destination`** – network segments computer is attached to
  - **`Netmask`** -
  - Gateway -
  - Interface -
  - Metric -
- The **`route`** command can be used to change the routing table, and to fix issues caused by using a multihomed server

IP Configuration Command-Line Tools

- Other command line tools available to assist with IP configuration:
  - `netsh`
  - `ipconfig`
  - `ping`
  - `arp`
  - `tracert`
  - `nslookup`
- Additional tools are available, but are generally used to verify correct IP configuration settings and connectivity

netsh

```
C:\Windows\system32>netsh
netsh>interface ip
netsh interface ipv4>show config

Configuration for interface "Ethernet"
    DHCP enabled:                         Yes
    IP Address:                           10.0.2.15
    Subnet Prefix:                        10.0.2.0/24 (mask 255.255.255.0)
    Default Gateway:                      10.0.2.2
    Gateway Metric:                       0
    InterfaceMetric:                      25
    DNS servers configured through DHCP:  10.0.2.3
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Loopback Pseudo-Interface 1"
    DHCP enabled:                         No
    IP Address:                           127.0.0.1
    Subnet Prefix:                        127.0.0.0/8 (mask 255.0.0.0)
    InterfaceMetric:                      75
    Statically Configured DNS Servers:    None
    Register with which suffix:           Primary only
    Statically Configured WINS Servers:   None
Netsh interface ipv4>
```

`netsh.exe` command can be used interactively in “contexts”

- For a list of `netsh` commands, type: `netsh /?`

Using netsh

- The previous slide shows the `interface` context. There are also: **`dhcp`**, **`lan`**, **`netio`**, **`http`**, and **`firewall`** contexts.

- To configure the IP address of the Ethernet interface use:
  - **`netsh interface ipv4 set address “Ethernet” static 10.1.1.1 255.255.0.0`**

- To set the primary DNS server, use:
  - **`netsh interface ipv4 set dns “Ethernet” static 10.1.1.100 primary`**

Using `ipconfig`

`ipconfig` is used to display a computers IP address settings and perform other tasks based on these options:

- **`/all`**
- `/release`
- `/renew`
- `/displaydns`
- `/flushdns`
- `/registerdns`

Using `ping`

- `ping` is used to test the connectivity between two computers, by sending an ICMP Echo Request packet
- If the destination receives the ICMP Echo Request and can respond, it'll reply with an ICMP Echo Reply packet
  - Example: `Reply from 192.168.100.201 bytes=32 time=<1ms TTL=128`
- To see the options available for the `ping` command, type `ping /?` at the command prompt

Using `arp`

- The `arp` command displays or makes changes to the Address Resolution Protocol (ARP) cache, which contains IP address – MAC address pairs
- Can add static ARP entries
- Some options for ARP command:
  - `-a, -g`: displays current ARP entries
  - `-d`: deletes ARP entries
  - `-s`: adds a static ARP entry

Using `tracert`

- Usually called “trace route” because it displays the route packets take between two computers
- Works by sending out packets with a TTL value starting at 1 and increases the value until the destination is reached
- Useful for troubleshooting the routing topology of a complex network and finding bottlenecks
  - Displays the time it took to receive a reply from each router (could indicate where bottlenecks might be)

Using tracert

- Usually called “trace route” - displays the route packets take between two computers

```
traceroute to canonical.com (91.189.94.250), 30 hops max, 60 byte packets
 1  modem.Home (192.168.0.1)  0.540 ms  1.198 ms  1.010 ms
 2  stpl-dsl-gw13.stpl.qwest.net (207.109.2.13)  21.722 ms  21.749 ms  23.073
ms
 3  stpl-agw1.inet.qwest.net (207.109.3.97)  23.076 ms  23.189 ms  23.226 ms
 4  216-160-19-2.mpls.qwest.net (216.160.19.2)  24.652 ms  24.678 ms  25.002
ms
 5  ae-1-3114.edge5.London1.Level3.net (4.69.148.218)  121.709 ms  137.952 ms
122.990 ms
 6  SOURCE-MANA.edge5.London1.Level3.net (212.187.138.82)  124.021 ms  123.106
ms  123.374 ms
 7  bond0.ravi.canonical.com (91.189.88.5)  123.520 ms  118.636 ms  118.489 ms
 8  * * *
```

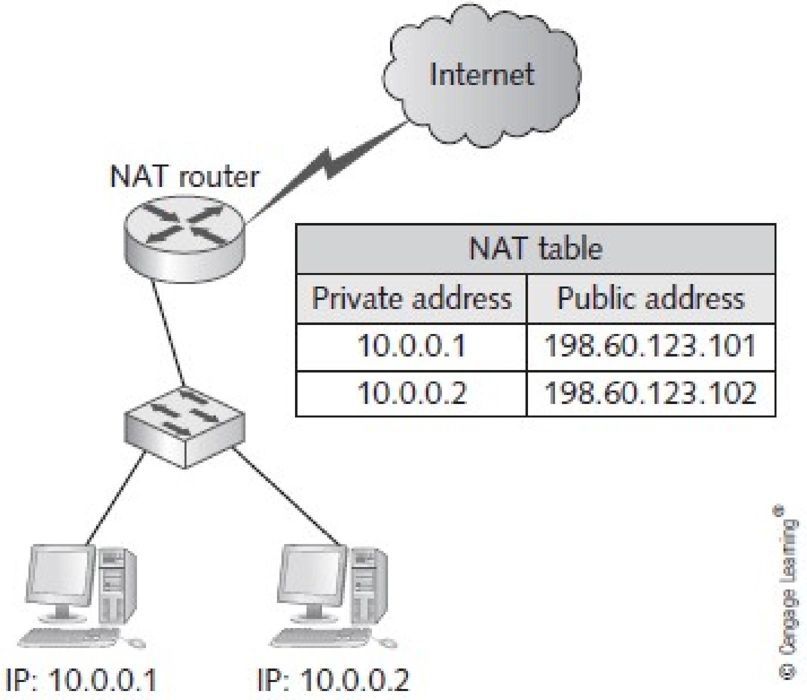
Using `nslookup`

- Used to test and troubleshoot DNS operation
- Can be used in command mode or interactive mode
- In command mode, you type `nslookup` *`host`* to query for the host’s address
- In interactive mode, you can simply type *`host`* to get the host’s address
- Typing a question mark at the interactive mode prompt gives a list of available options

Network Address Translation

- **NAT** allows an organization to use private IP addresses while connected to the Internet
- The NAT process translates a workstation’s private address (as a packet leaves the corporate network) into a valid public Internet address
  - When data returns to the workstation, the address is translated back to the original private address
  - Nat is usually handled by a network device connected to the Internet, such as a router
  - Address translation is kept track of in a NAT table

Network Address Translation



NAT table	
Private address	Public address
10.0.0.1	198.60.123.101
10.0.0.2	198.60.123.102

© Cengage Learning®

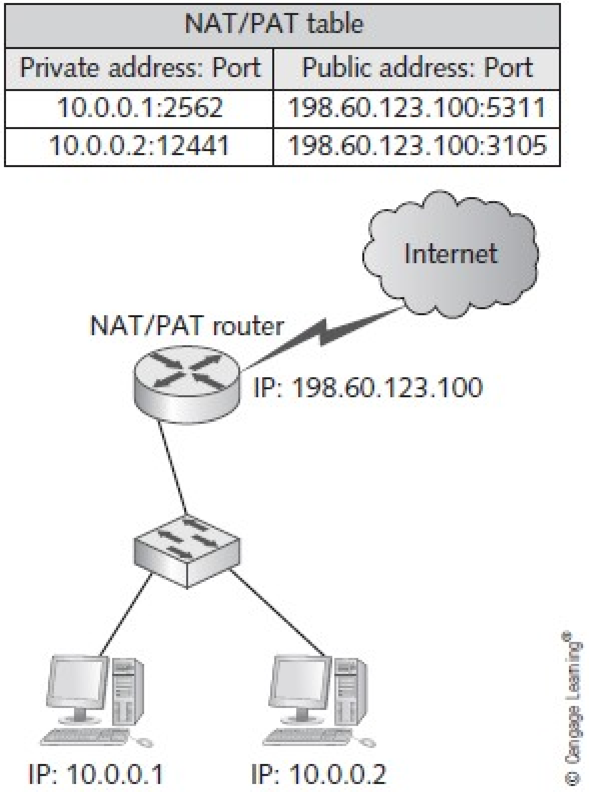
Figure 6-8 Private addresses translated to public addresses with NAT

Port Address Translation

Port Address Translation (PAT)

- Allows several hundred workstations to access the Internet with a single public Internet address
- Each packet contains source and destination IP addresses along with source and destination port numbers
- A single public IP address is used for all workstation, but different source port numbers are used for each communication session

Port Address Translation



NAT/PAT table	
Private address: Port	Public address: Port
10.0.0.1:2562	198.60.123.100:5311
10.0.0.2:12441	198.60.123.100:3105

© Cengage Learning®

Figure 6-9 PAT uses the port number to allow using a single public IP address

Summary

- CIDR largely replaces the IP address class system
- Subnetting enables an administrator to divide a large network into smaller networks that require a router for communication
- Commands for working with IP address configurations include `netsh`, `ipconfig`, `ping`, `arp`, `route`, `tracert`, and `nslookup`
- Network Address Translation (NAT) enables an organization to use private IP addresses while connected to the Internet

Ch 11: Network Operating Systems

Windows Server:
Active Directory
Domains

Clients and Servers

- What should I install on a computer? A client OS or a server OS?

  → Depends on the role the computer will play in your network

Client OSs usually come with

- user software e.g. Web browsers, Word
- helper software e.g. DNS and DHCP clients, file-sharing clients

Server OSs can include client software but also have server components:

- Web servers
- DNS and DHCP servers
- file-sharing servers

Role of a Client OS

- The main purpose of the client OS is to run applications - which often access network resources

Desktop computers typically need network client software:

- DHCP client
- DNS client
- HTTP client (Web browser)
- File-sharing client
- E-mail client

File Sharing Client

Windows: common ways to access shared storage are using the **Universal Naming Convention (UNC) path** or **mapping a drive**

UNC path example:

\\server-name\sharename\subfolder\file.extension

Drive mapping using the **net** command example:

```
Net use drive-letter:\\server-name\sharename
```

The *`drive-letter`* should be a single unused driver letter (`A-Z`), followed by a colon (:)

The `Net` command can be entered at a command prompt, logon script or batch file

Role of a Server OS

- A Server OS is optimized to run network services in the background to speed up responses to client

In a typical network, a server provides:

- Centralized user account and computer management
- Centralized storage
- Infrastructure services, such as name resolution and address assignment
- Server and network fault tolerance

Centralized User Account and Computer Management

- A server-based network is centralized management of network resources, which includes the following functions:
  - □ User authentication and authorization
  - □ Account management
  - □ Security policy management

Authentication: process of identifying who has access to OS resources; most common form: username & password

Authorization: process of granting or denying an authenticated user access to resources

Account Management

- Most OSes incorporate account management for authentication and authorization
- The server versions of Windows includes a centralized account management, authentication, and authorization system called **Active Directory**
- When Active Directory is installed on a server, the server becomes a domain controller and users and computer with accounts are referred to as domain members

Security Policy Management

- Accounts in Active Directory are used to distribute and enforce policies (called **group policies**) for network use and security

- For example, policies can control:
  - what icons appear on a user’s desktop
  - password restrictions
  - what applications a user/group can run

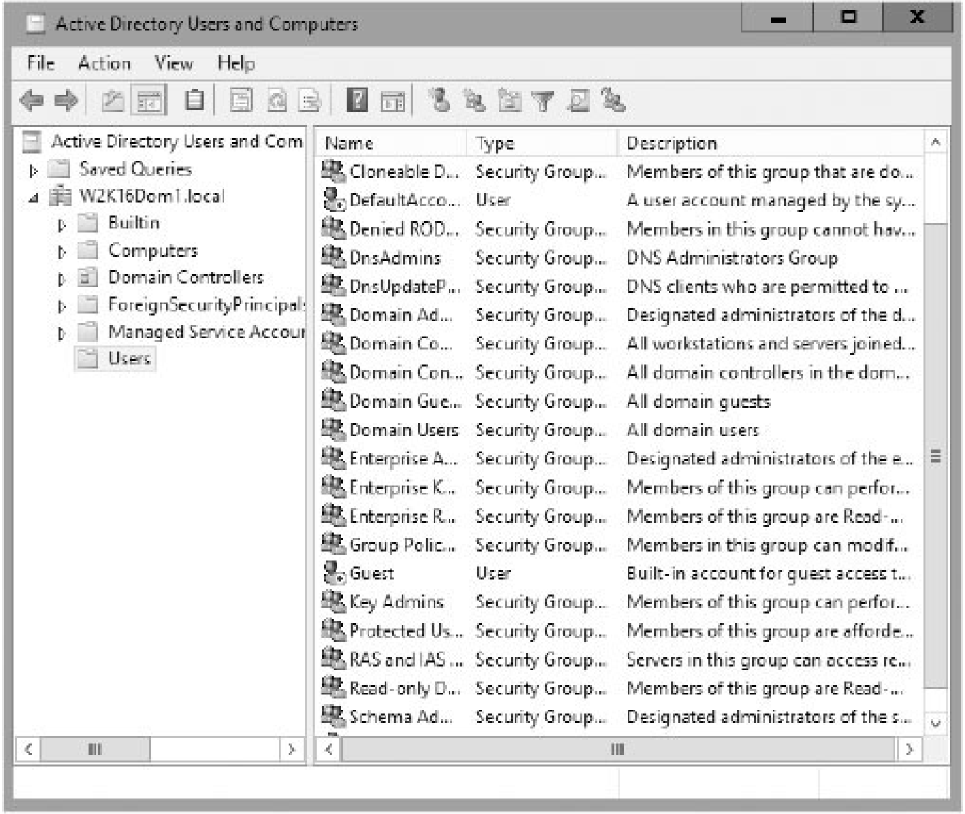
Domains and Active Directories

- A Windows Domain is a collection of users and computers
- A Domain is managed by a server called the “Domain Controller”

- The software on a Domain Controller (DC) that tracks all the users, computers, and services the DC manages is called “Active Directory”

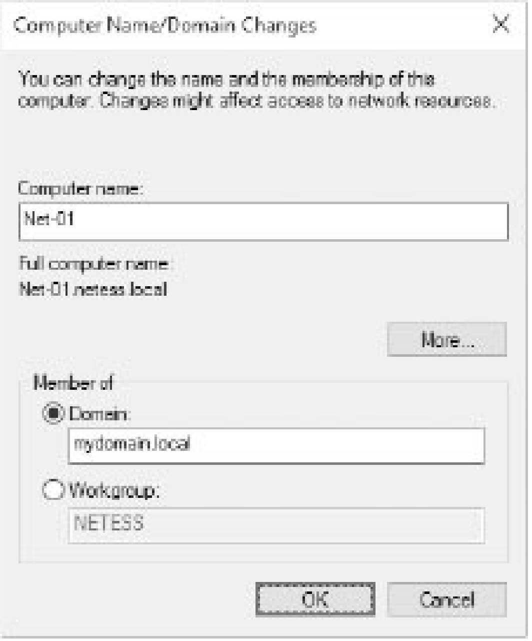
- Every DC server has to have AD installed on it.
- An AD is a database of “objects” plus rules for using these objects

Active Directory Account Management



Name	Type	Description
Cloneable D...	Security Group...	Members of this group that are do...
DefaultAcco...	User	A user account managed by the sy...
Denied ROD...	Security Group...	Members in this group cannot hav...
DnsAdmins	Security Group...	DNS Administrators Group
DnsUpdateP...	Security Group...	DNS clients who are permitted to ...
Domain Ad...	Security Group...	Designated administrators of the d...
Domain Co...	Security Group...	All workstations and servers joined...
Domain Con...	Security Group...	All domain controllers in the dom...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrators of the e...
Enterprise K...	Security Group...	Members of this group can perfor...
Enterprise R...	Security Group...	Members of this group are Read-...
Group Polic...	Security Group...	Members in this group can modif...
Guest	User	Built-in account for guest access t...
Key Admins	Security Group...	Members of this group can perfor...
Protected Us...	Security Group...	Members of this group are afforde...
RAS and IAS ...	Security Group...	Servers in this group can access re...
Read-only D...	Security Group...	Members of this group are Read-...
Schema Ad...	Security Group...	Designated administrators of the s...

Figure 11-10 The Active Directory Users and Computers management console



You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: Net-01

Full computer name: Net-01.netess.local

Member of

● Domain: mydomain.local

○ Workgroup: NETESS

Figure 11-11 Making a computer a domain member

Centralized Storage

- We store data in a network for:
  - File sharing
  - e-mail, user files, databases, backups, etc.
- Network use specialized devices to help manage their storage:
  - Network-attached storage devices
  - Storage area networks
  - Cloud-based storage

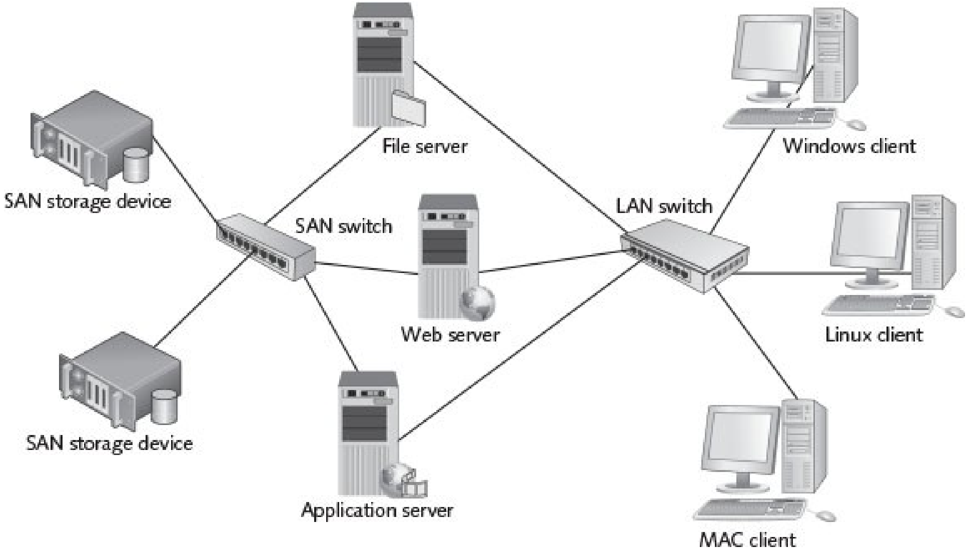
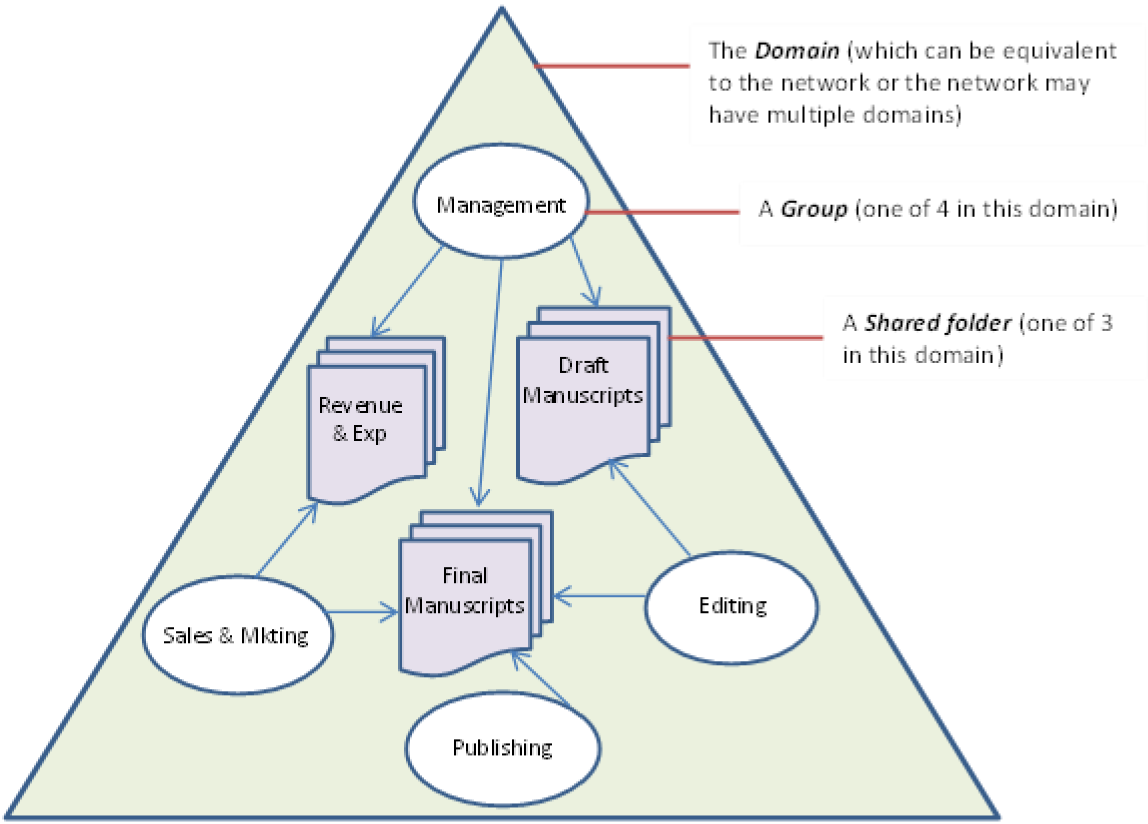


Figure 11-12 A storage area network

Ch 12: Network Management and Administration

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

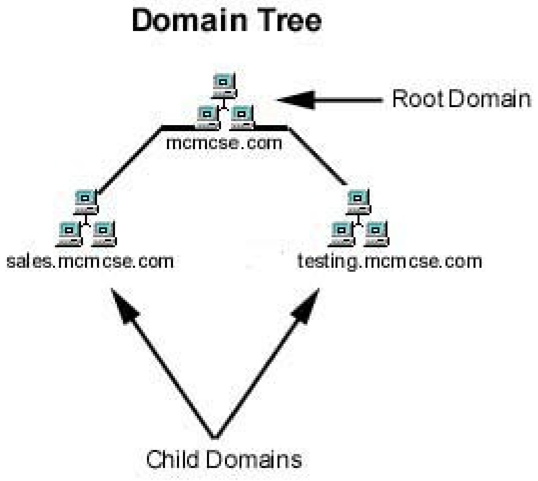
Hierarchical view of Active Directory



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)

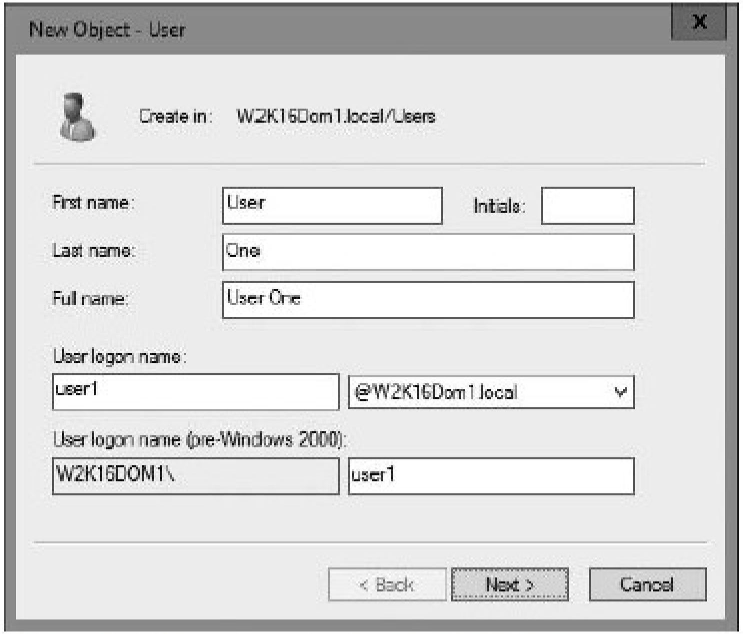
Creating a User Account

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:

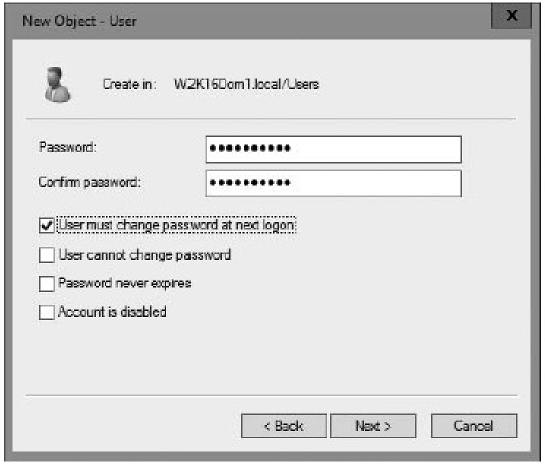
user1 @W2K16Dom1.local

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)

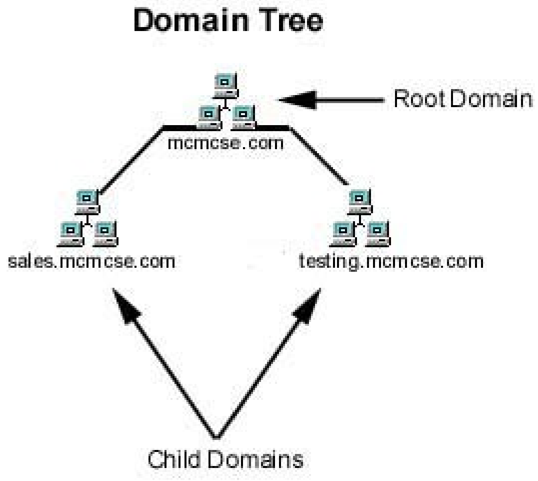
Group scope has three options:

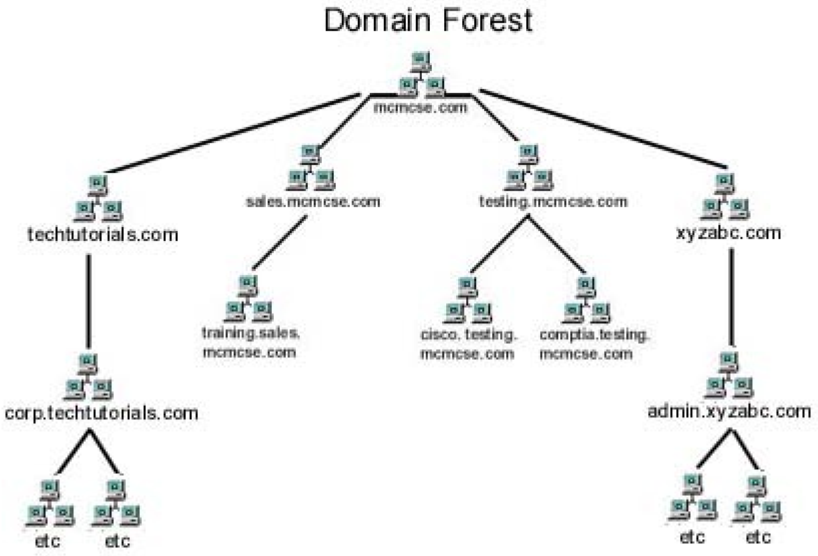
Domain local – Can be used to assign permissions to resources only in the domain in which the group is created

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

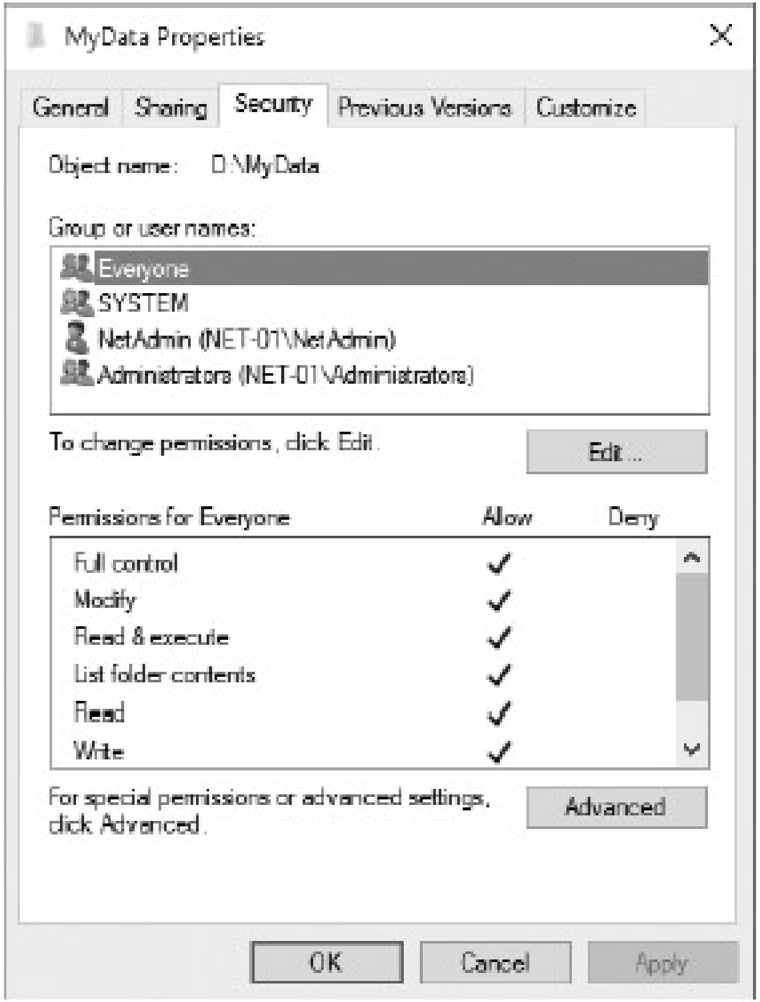
- Two modes for accessing files on a networked computer:
  - Network (sometimes called remote)
  - Interactive (sometimes called local)
- Share permissions are applied when a user attempts network access to shared files
- NTFS permissions always apply
  - Whether file access is attempted interactively 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.

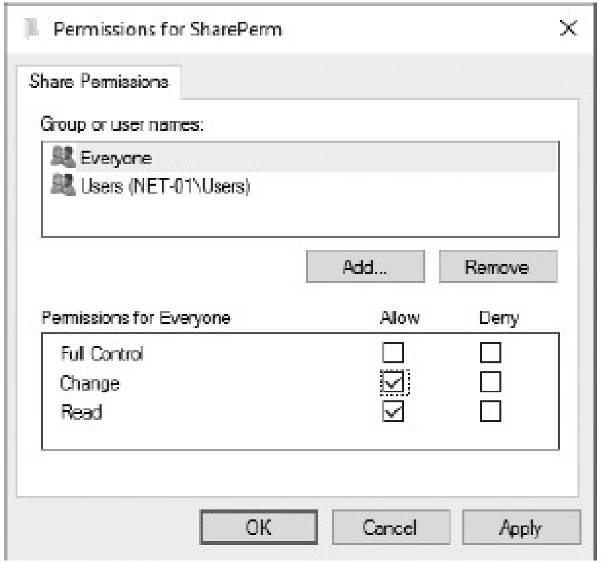
Permissions for Everyone	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

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*



Group or user names:

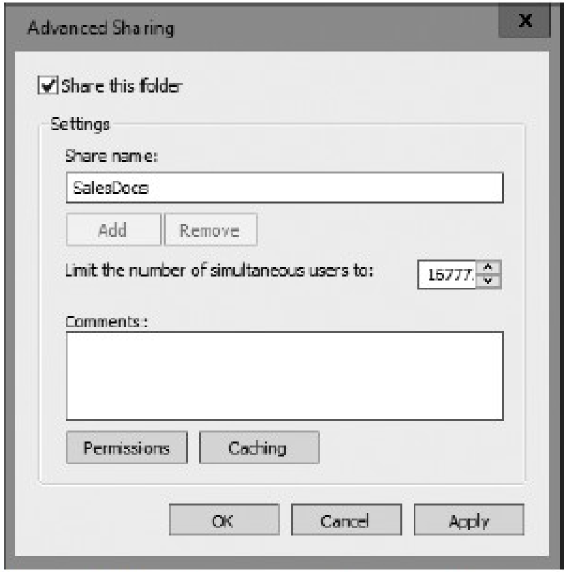
- Everyone
- Users (NET-01\Users)

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

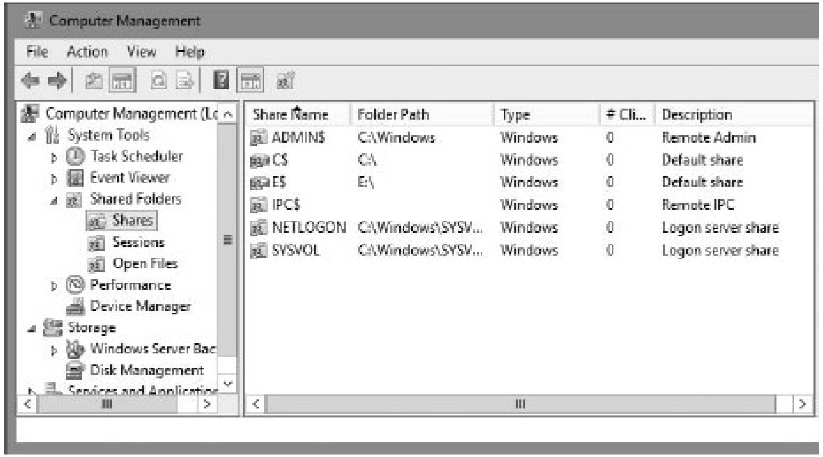
Comments:

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

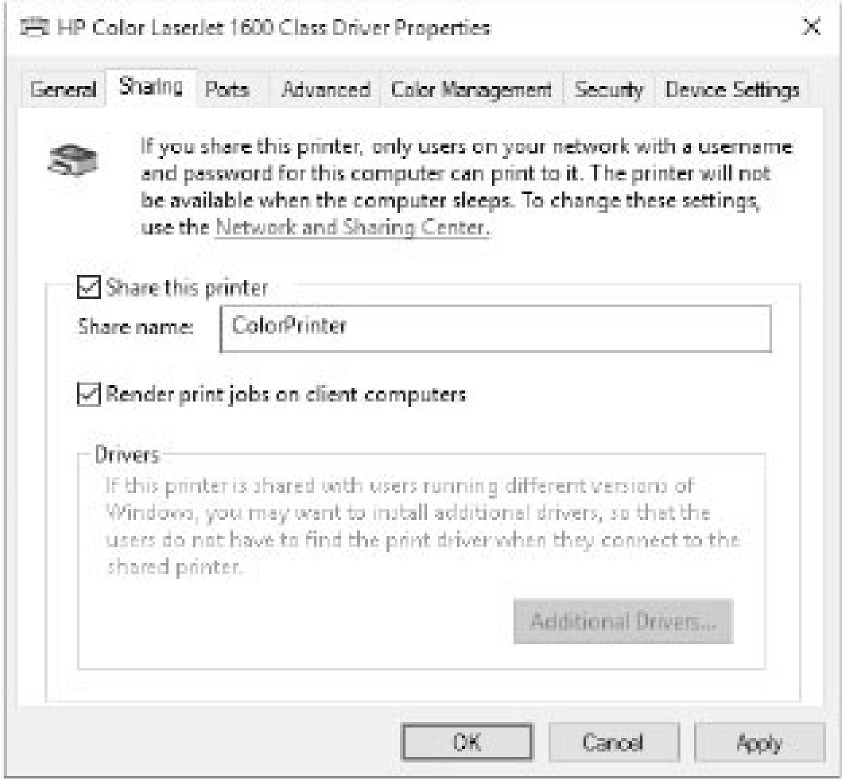
- *File and Storage Services* — A Server Manager component, a more advanced method for creating shares

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

Benefits of Sharing Printers

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



HP Color LaserJet 1600 Class Driver Properties

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

Drivers

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