Chapter 3: Introduction to Servers

Implementation Model

Peer-to-Peer (P2P) Network Model

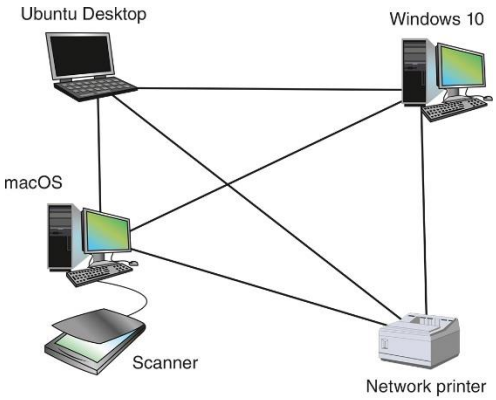


Figure 1-1 In a peer-to-peer network, no computer has more authority than another; each computer controls its own resources and communicates directly with other computers

Client-Server Network Model

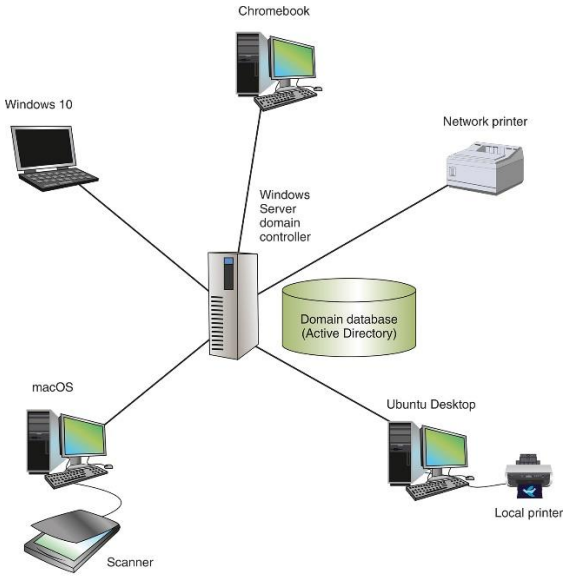


Figure 1-2 A Windows domain uses the client-server model to control access to the network, where security on each computer or device is controlled by a centralized database on a domain controller

Peer to peer

- Advantages
  - Simple configuration
  - Less expensive compared to other network models
- Disadvantages
  - Not scalable
  - Not necessarily secure
  - Not practical for large installations

Client-Server Network Model

- Resources are managed by the NOS via a centralized directory database
- A **Windows domain** is a logical group of computers that a Windows Server can control
- **Active Directory (AD)** is the centralized directory database that contains user account information and security for the entire group of computers
- A user can sign on to the network from any computer on the network and gain access to the resources that AD allows
  - This process is managed by Active Directory Domain Services (AD DS)
- A computer making a request from another is called the **client**

Server in a nutshell

- the lifeblood of any network
- provide the shared resources that network users crave, such as file storage, databases, email, web services, etc.
    - A **network operating system (NOS)** controls access to the entire network
        - A NOS is required by client-server models

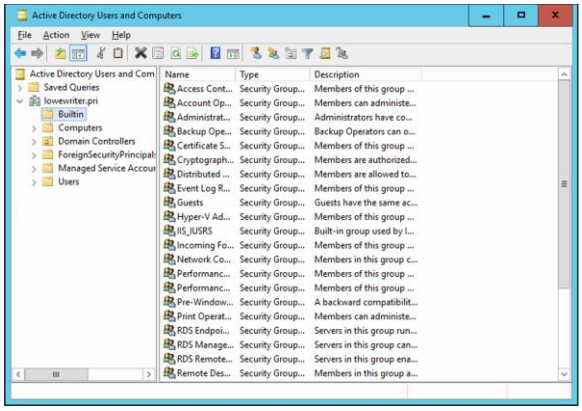
Server operating system

- enables your server computers to function as servers rather than as ordinary Windows clients
- provide essential functions such as providing basic security services, sharing disk storage and printers

Core server operating system features

- Network services
- File-sharing services
- Multitasking
- Directory services (most popular modern directory service is called Active Directory)
- Security services

Active Directory on Windows Server 2019



Active Directory is a standard component of all Windows operating systems, and because it's so popular, most other operating systems support it as well.

Server Software – categorized

1. **Web Servers**:
    1. Apache HTTP Server
    2. Nginx
    3. Microsoft Internet Information Services (IIS)
    4. LiteSpeed Web Server
2. **Database Servers**:
    1. MySQL
    2. PostgreSQL
    3. Microsoft SQL Server
    4. Oracle Database
    5. MongoDB (NoSQL)

3. **File Servers**:
    1. Windows File Server
    2. Samba
    3. FTP Servers (e.g., vsftpd, FileZilla Server)
4. **Email Servers**:
    1. Microsoft Exchange Server
    2. Postfix
    3. Sendmail
    4. Exim
5. **Proxy Servers**:
    1. Squid
    2. Nginx (can also function as a reverse proxy)
    3. HAProxy
6. **DNS Servers**:
    1. BIND (Berkeley Internet Name Domain)
    2. Microsoft DNS Server
    3. PowerDNS
7. **Streaming Servers**:
    1. Wowza Streaming Engine
    2. Adobe Media Server
    3. Icecast
8. **Collaboration Servers**:
    1. Microsoft SharePoint Server
    2. Zimbra Collaboration Suite
    3. Nextcloud
9. **Game Servers**:
    1. Minecraft Server
    2. Valve's Source Dedicated Server (SRCDS)
    3. Unreal Engine Server
10. **Remote Access Servers**:
    1. Virtual Private Network (VPN) servers (e.g., OpenVPN, Cisco AnyConnect)
    2. Remote Desktop Services (RDS) servers (e.g., Windows Remote Desktop Services, Citrix Virtual Apps and Desktops)
11. **Monitoring Servers**:
    1. Nagios
    2. Zabbix
    3. Prometheus
12. **Container Orchestration Servers**:
    1. Kubernetes
    2. Docker Swarm
    3. Apache Mesos
13. **Continuous Integration/Continuous Deployment (CI/CD) Servers**:
    1. Jenkins
    2. GitLab CI/CD

3. CircleCI

14. **Authentication Servers**:
    1. Active Directory Domain Services (AD DS)
    2. LDAP Servers (e.g., OpenLDAP)
    3. OAuth Servers (e.g., Keycloak)
15. **Backup Servers**:
    1. Veeam Backup & Replication
    2. Bacula
    3. Amanda

What's Important in a Server

- Scalability
- Reliability
- Availability
- Service and support

Scalability is the ability to increase the size and capacity of the server computer without unreasonable hassle. Purchasing a server computer that just meets your current needs is a major mistake because (rest assured) your needs will double within a year. If at all possible, equip your servers with far more disk space, RAM, and processor power than you currently need.

The old adage "you get what you pay for" applies especially well to server computers. Why spend $5,000 on a server computer when you can buy one with seemingly similar specifications at a discount electronics store for a mere $1,000? The main reason: **reliability**. When a client computer fails, only the person who uses that computer is affected. When a server fails, however, everyone on the network is affected. The less-expensive computer is probably made of inferior components that are more likely to fail, and does not have redundant components built in. (For example, many server computers have two power supplies, two CPUs, two or more network interfaces, and other redundant components.)

This concept is closely related to **reliability.** When a server computer fails, how long does it take to correct the problem and get the server up and running again? Server computers are designed so their components can be easily diagnosed and replaced, which minimizes the downtime that results when a component fails. In some servers, components are hot swappable (certain components can be replaced without shutting down the server). Some servers are fault-tolerant so that they can continue to operate even if a major component fails.

Service and support are often overlooked factors when picking computers. If a component in a server computer fails, do you have someone on

site qualified to repair the broken computer? If not, you should get an on-site maintenance contract for the computer. Don't settle for a maintenance contract that requires you to take the computer in to a repair shop or, worse, mail it to a repair facility. You can't afford to be without your server that long. Get a maintenance contract that provides for on-site service and repair of your server, 24 hours a day, 7 days a week.

Components of a Server Computer

- Motherboard
- Processor
- Memory
- Hard drives
- Network interface
- Video
- Power supply

The hardware components that make up a typical server computer are similar to the components used in less-expensive client computers. However, server com puters are usually built from higher-grade components than client computers for the reasons given in the preceding section. The following paragraphs describe the typical components of a server computer

The network connection is one of the most important parts of any server. Ideally, your server should have at least two network interfaces. Additional network interfaces not only improve the performance of your server, but also make it more reliable: If one of the network interfaces should fail, the others can pick up the ball. If possible, the server's network interfaces should be 10 Gbps interfaces. Then, you can use 10 Gbps switches to connect the servers to each other and to your access switches. With many users contending for access to the servers simultaneously, 1 Gbps interfaces can easily become a performance-limiting bottleneck.

Considering Server Form Factors

- Tower case
  - Traditional, for small size projects and deployment
- Rack mount
  - are designed to save space when you need more than a few servers in a confined area
- Blade servers
  - designed to save even more space than rack-mount servers
  - A typical blade chassis holds six or more servers, depending on the manufacturer

- One of the key benefits of using blade servers is that you don't need a separate power supply for each server. Instead, the blade enclosure provides power for all its blade servers

Rack-mount servers are designed to save space when you need more than a few servers in a confined area. A rack-mount server is housed in a small chassis that's designed to fit into a standard 19-inch equipment rack. The rack allows you to vertically stack servers to save space.

Considering Virtualization

- in many (if not most) modern network environments, a single physical computer system is used to run more than one virtual machine (VM)
- the reason that server computer hardware often has such high-performance specifications, such as dual processors with multiple cores each and a large amount of RAM (256GB or more)

Note: When a single physical computer is responsible for running multiple virtual servers, the physical server must have sufficient capacity to run all its virtual servers.

Considering your licensing options

- Two types of licenses are required to run a Windows Server operating system:
  - a server license, which grants you permission to run a single instance of the server,
  - and Client Access Licenses (CALs), which grant users or devices permission to connect to the server. When you purchase Windows Server, you ordinarily purchase a server license plus some number of CALs

Licensing options cont...

- two distinct types of CALs: per-user and per device.
  - Per-user CALs limit the number of users who can access a server simultaneously, regardless of the number of devices (such as client computers) in your organization.
  - By contrast, per-device CALs limit the number of unique devices that can access the server, regardless of the number of users in your organization.

Chapter 4: File Sharing & Workgroups

File Sharing

Automated Network

- The most basic network connectivity that facilitates network sharing services such as DHCP
- Built in on various OSes and especially in Windows OS
- Windows uses a collection of computers connected together within a small network called a **workgroup**

Dynamic Host Configuration Protocol (DHCP) - the service that recognizes computers and other devices that want to join the network,

"this service provides each with a unique address so that all the devices on the network can identify one another"

Workgroup

- Its purpose is to facilitate resource sharing, such as files, folders, printers, and internet access, among the connected computers.
- Unlike a domain (see topic 4), which requires a dedicated server and complex administration, a workgroup operates without centralized control or hierarchy.
- To set up a workgroup, one just needs every PC to be in the same name of the workgroup within the same physically connected network

Characteristics

- **Equal Standing**: In a workgroup, all computers are considered equal. There is no central server or master computer.
- **User Autonomy**: Each computer maintains its own user accounts and security settings. Users can easily share and access resources without relying on a central server.
- **Network Size**: Workgroups are suitable for small networks, such as home networks or small offices. They typically consist of anywhere from two to twenty computers.
- **Local Area Network (LAN)**: All computers within the workgroup must be connected to the same LAN or wireless network

Advantages and Limitations

Pros

- **Simplicity**: Setting up a workgroup is straightforward and requires minimal technical knowledge. It allows quick resource sharing without complex configurations.
- **Flexibility**: Workgroups can be easily expanded or modified. New computers can join the workgroup, and existing ones can be removed without disrupting network operation.
- **Resource Sharing**: Users can specify which files, folders, or printers are shared with other workgroup members and control access levels (read or write).

Cons

- **No Centralized User Management**: Workgroups lack centralized user authentication or management. Each computer maintains its own user accounts, which can lead to duplication.
- **Administrative Burden**: Managing multiple user accounts across workgroup computers can be administratively burdensome.

Setting up workgroup

- On a Windows client:
    1. Goto System > About [click "Domain or workgroup" link]
    2. Click "Change" button
    3. Specify your desired Workgroup name
    4. Apply then Restart Windows Client

Note: Make sure to rename your **PC name** also and you must choose a unique name for each client in your workgroup.

Network visibility on workgroups

- On a Windows client:
    1. Goto -> Control Panel\Network and Internet\Network and Sharing Center
    2. [Click] Change Advance Network Settings
    3. For either Private or Public networks (as needed)
        1. Network Discovery = On
        2. Set up network connected devices automatically (private) = On
        3. File and Printer Sharing = On
    4. All network

1. Public folder sharing = On/Off as needed
2. File Sharing Connections = 128bit encryption (recommended)
3. Password protected services = On/Off as needed

5. Apply then restart Windows Client

Folder visibility on workgroups

On a Windows client:

- Select desired folder to share -> [right click]
- Goto Security -> Edit permissions
- Add entry for “Everyone”
- Edit the Everyone entry’s permissions as needed (might be Full control)
- Apply sharing on sharing tab
- Apply then Refresh

Chapter 5: DTF, Introduction to Domain Controllers, Active Directory, Domain Services

Domains, Trees, Forest

Network Domain

- A network domain is an administrative grouping of multiple private computer networks or local hosts within the same infrastructure
- Requires a dedicated server and complex administration
- Domains can be identified using a domain name; domains which need to be accessible from the public Internet can be assigned a globally unique name within the Domain Name System (DNS).

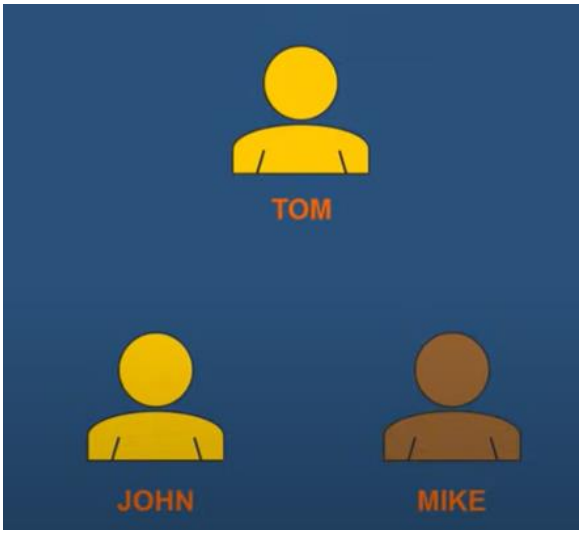
Domain Name System

WORLD OF COMPUTERS

- Identify individual devices using numbers

HUMANS

- Identify individuals using names



Network Domain – con't

- A domain controller is a server that automates the logins, user groups, and architecture of a domain, rather than manually coding this information on each host in the domain.
- It is common practice, but not required, to have the domain controller act as a DNS (domain name system) server. That is, it would assign names to hosts in the network based on their IP addresses. All the devices on the network can identify one another"

Characteristics

- **Hierarchical and Distributed** : In a network domain, all devices depend on the central server or master computer.
- **Scalable deployment**: computers can easily be deployed by the numbers and can be configured from the DC server.
- **Network Size**: network domains are suitable for medium to large networks, such as enterprise organizations and large corporations. They typically number in the thousands
- **WAN:** All computers within the domain must be connected to the same organization be it local or worldwide

Advantages and Limitations

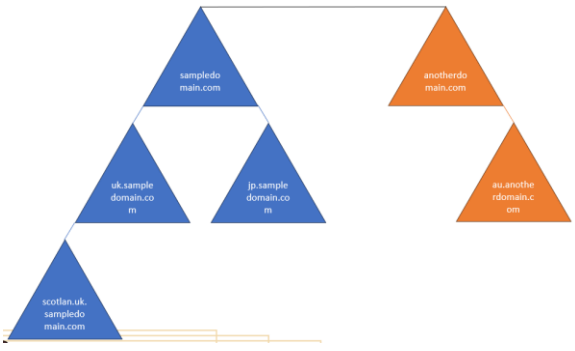
Pros

- **Enhanced Security and Isolation**: Domains provide controlled access, reducing security risks.
- **Improved Network Performance:** Efficient resource allocation enhances network speed.
- **Scalability and Flexibility**: Domains adapt as the organization grows.
- **Simplified Network Management:** Centralized administration streamlines tasks.
- **Fault Isolation and Troubleshooting:** Domains aid in identifying and resolving issues.
- **Compliance and Regulatory Requirements:** Domains help meet industry standards.

Cons

- **High level planning**: Managing multiple user accounts across the network domain needs a high level of understanding of the network structure.
- **Initial setup**: The beginning of the network setup is tedious and lasts a long process but afterwards it becomes exponentially less burdensome

Trees & Forests



Conclusion

"Network domains play a crucial role in managing and organizing network resources efficiently. They allow for better control, security, and scalability within complex network infrastructures."

Domains Controllers

Domain controller

- Windows Domains have been around since Windows NT (1993)
- Allows administrators to manage large computer networks
- Generally, contain a large number of computers on the same network

Windows Domain controller

- It is referred to as "DC"
- Any server with AD DS role (Active Directory with Domain Service)
- Responds to security authentication requests
- Contains Active Directory & Group Policy
- Might contain Multiple Domain Controllers but just one primary controller

The server's job is to handle authentication requests across the domain

Domain controllers hold the tools like Active Directory & Group Policy, so if you need to create new user accounts and change the -main policies this is all done from the domain controller

You can have several or multiple domain controllers, but you can only have one primary controller, the primary reason for having one or more DC is fault tolerance so if one of the DCs is malfunctioning there would be a backup one to take the slack

Domain controller con't

- Directory Service called "Active Directory Users and Computers"
    - Users Account (usernames and passwords)
    - Computers
    - Printers
    - File Shares

Domain Controllers uses a tool called Active Directory Users and Computers commonly referred to as AD or active directory

This tool is use not to only manage user and computer accounts but also acts as a directory service for resources on your network like printers or file share

When a domain user searches for a new printer to install, they will find all the printers that have been added to the domain controller with active directory

Active Directory (A Domain Controller Tool)

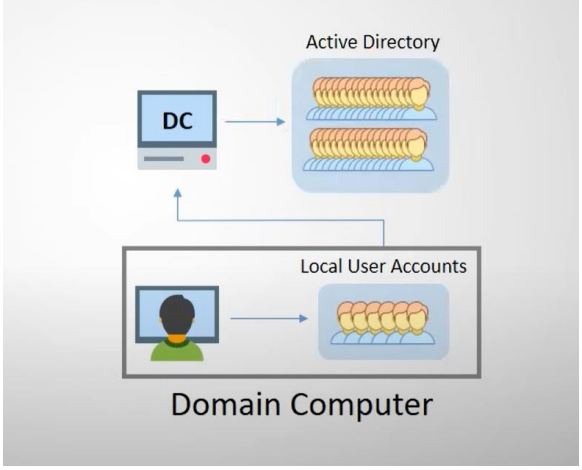
DC – Active Directory

- Log on Attempt

1st – Local user accounts

2nd – Domain Controller

(Active Directory)



When a user connected to network domain logs in, the 1st thing that the computer do is to first look the matching user locally in the computer itself, if it does not find one then it reaches out to its domain controller and attempts to find a user account in the directory service Active Directory

DC – Active Directory

- Contains objects
    - Users
    - Computers
    - Printers
    - File shares
    - Groups
- Groups object
    - Domain Admins
    - Domain Users
    - Many more…
- **OUs (Organizational Units) are used to group objects**

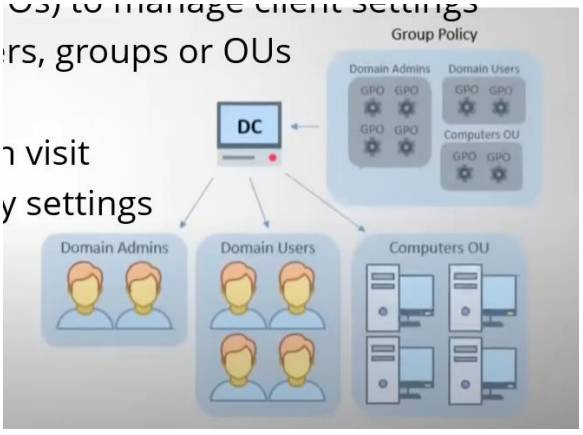
AD is a tool to manage domain users, computers, printers file shares groups and more. All these things are all considered AD objects

Groups contain members which can be any valid AD object a user, a computer, etc.

By default, there are several groups that come with AD like domain admins, domain users, all of these AD objects are stored within folders called Organizational Units

Group Policy Management (A Domain Controller Tool)

- Used to manage all domain user and computer settings remotely
- Uses Group Policy Objects (GPOs) to manage client settings
- Target specific users, computers, groups or OUs
- Install software remotely
- Manage what website they can visit
- Manage and configure security settings
- Configure profiles, etc.



Conclusion

- A Windows Domain allows management of large computer networks
- Use at least ONE Windows Server called DC (Domain Controller)
- A DC is any server with the AD DS (Active Directory Domain Services) role
- DCs respond to authentication requests across the domain
- DCs have the tools AD (Active Directory) and GP (Group Policy)
- AD contains Objects and OUs' (Organizational Units)
- GP contains GPOs (Group Policy Objects) that manage AD objects