INFORMATION AND COMMUNICATION TECHNOLOGY

Computer Systems Servicing (CSS)

Set-up Computer Servers

Introduction

Setting-up computer servers is a vital process for ensuring the smooth functioning of networked environments, especially in Local Area Networks (LANs) and Small Office/Home Office (SOHO) systems. This unit emphasizes the key skills needed to configure and deploy servers, which include establishing user access, configuring network services, conducting testing and documentation, and carrying out pre-deployment procedures. Learners will develop proficiency in defining user access levels, implementing network policies and services, and managing peer-to-peer (P2P) network access. Furthermore, the unit addresses server modules and add-ons, operations of network services, and strategies for managing unexpected incidents. There is a strong focus on enterprise policies and testing procedures, documenting reports and findings, and ensuring security compliance prior to deployment. This unit also promotes analytical thinking, problem-solving, and technical skills, while fostering effective communication, adaptability, self-motivation, and teamwork that is crucial skills in the industry standards. By mastering these skills, the learners will be well-prepared to set up and maintain servers, ensuring seamless connectivity, security, and efficiency across various computing environments.

What I Need to Know?

This module consists of four lessons designed to help you achieve your goal of setting up computer servers. The lessons are arranged in chronological order to follow the standard sequence of the topic.

The Lessons includes:

Lesson 1: Set-Up User Access

In this lesson, you will learn about understanding user access levels and network policies, configuring user permissions and security settings, and managing user accounts and access control to ensure proper user access.

Lesson 2: Configure Network

This lesson focuses on setting up and managing network services, configuring network modules and add-ons, and ensuring network security while addressing potential incidents to maintain a secure and efficient network environment.

Lesson 3: "Perform Testing and Documentation"

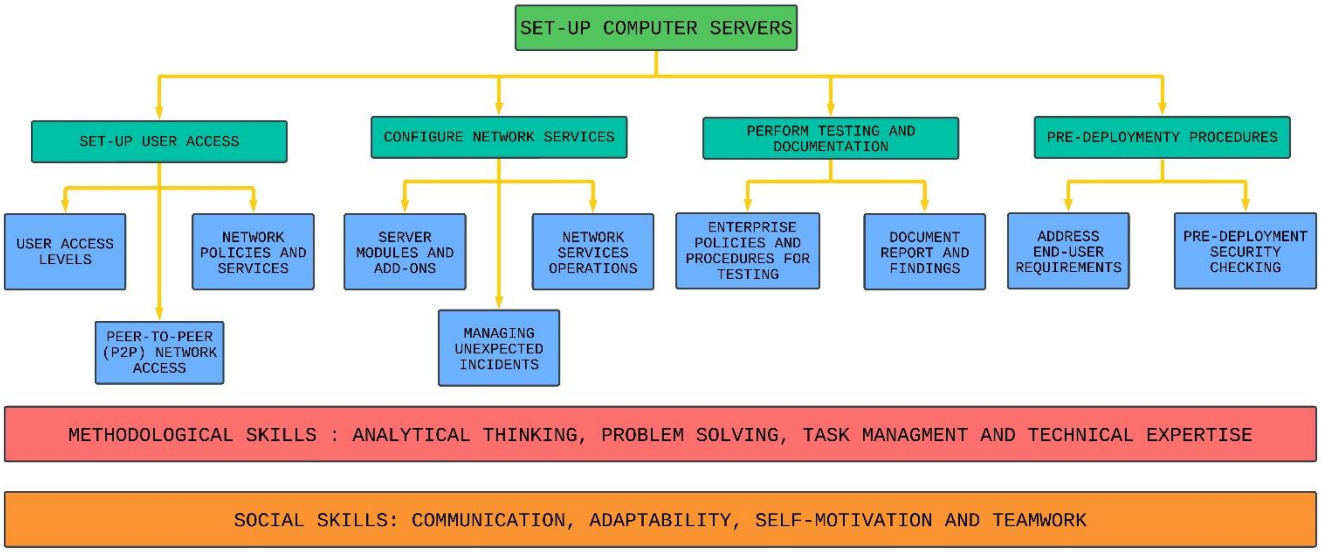
In this lesson, you will gain knowledge on conducting pre-deployment testing and checking requirements, documenting findings and

creating reports, and ensuring end-user security and operational readiness for a smooth deployment process.

Lesson 4: Pre-Deployment Procedures

This final lesson covers finalizing server configurations and network settings, conducting peer-to-peer (P2P) network checks, and preparing for enterprise-level deployment while addressing any unexpected issues to ensure a successful deployment.

INSTRUCTIONAL BLUEPRINT



What I Know!

Diving directly into the lesson might be too straight-forward, let's put you into a test on what you already know about **setting up computer servers**! This will help you to refresh your current understanding and identify the areas for improvement all throughout this module.

📌 **How to Access the Pre-Test:**

🔗 Click this link: https://forms.gle/5xjK4PDmMhBDNGNV9

OR

📱 Just kindly scan this QR Code to access the Pre-Test via Google Forms.

Scan this QR→

Make sure to finish the Pre-Test first before jumping into **Lesson 1!**

Lesson 1: Set-up User Access

Access and Protect

Access Control in IT Management

In modern IT environments, managing access to sensitive data is crucial for security and efficiency. Unauthorized access or improper permissions can lead to data breaches, accidental deletions, and operational disruptions. This case study explores the importance of assigning appropriate access levels within an organization.

Scenario:

You are an IT manager at a growing company that handles sensitive data, such as employee records and financial information. Employees have different access needs based on their roles. Recently, a non-administrative employee accidentally deleted a critical file they should not have been able to access. This incident raised concerns about whether access permissions are correctly assigned.

Analysis Activity

INSTRUCTIONS: Based on the given scenario, answer the following questions in your notebook or a piece of paper

1. Understanding the Risks
    - What potential risks arise when employees are given excessive access?
    - How could restricting access affect employees' ability to perform their tasks?
2. Developing a Solution
    - What network policies should be implemented to ensure proper access levels?
    - How can an IT department maintain security without limiting productivity?
3. Personal Reflection
    - Why is protecting sensitive data important in an organization?
    - How do you feel about the balance between security and accessibility in a workplace?

What I Need to Know?

Objectives:

At the end of the lesson, the students should be able to:

1. Identify different network operating system features in relation to network policies and services, user access level configurations, and peer-to-peer network access setup.
2. Perform peer-to-peer (p2p) network access
3. Evaluate the importance of understanding access levels and following network policies and services through an essay.

What To Know

Understanding Set-up User Access: Network Operating System (NOS) features, User Access Level Configuration, Network Policies and Services, and Peer-to-Peer(P2P) Network Access

A **Network Operating System (NOS)** is a specialized software designed to manage network resources, allowing multiple devices to communicate and share resources like files, printers, and internet access. Its **key features** include:

- **User Administration** - Centralized management of user accounts, authentication, and permissions.
- **Resource Sharing** - Enables sharing of files, printers, and applications across the network.
- **Network Security** - Provides user authentication, access control, and encryption for secure data transfer.
- **Backup and Recovery** - Automated backup solutions to ensure data integrity.
- **Scalability** - Supports network growth by accommodating more devices and users without performance degradation.

- **Remote Access** - Allows users to access network resources from remote locations via VPNs or remote desktop services.

The two major types of network operating systems are:

- **Peer-to-Peer**
- **Client/Server**

Nearly all modern networks are a combination of both. The networking design can be considered independent of the servers and workstations that will share it.

Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source (See fig. 1). In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. Nearly all modern desktop operating systems, such as Macintosh OSX, Linux, and Windows, can function as peer-to-peer network operating systems.

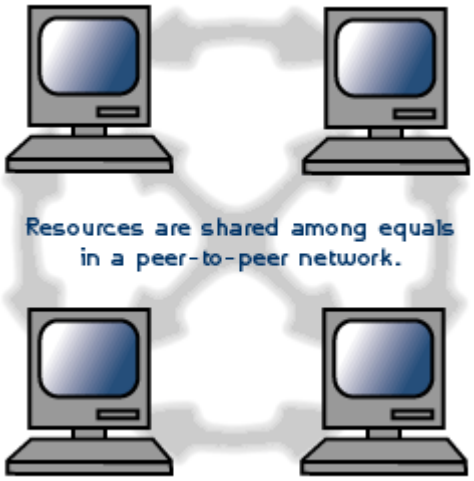


Fig. 1. Peer-to-peer network

Advantages of a peer-to-peer network:

- **Less initial expense** - No need for a dedicated server.
- **Setup** - An operating system (such as Windows XP) already in place may only need to be reconfigured for peer-to-peer operations.

Disadvantages of a peer-to-peer network:

- **Decentralized** - No central repository for files and applications.
- **Security** - Does not provide the security available on a client/server network.

Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers (See fig. 2). The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. UNIX/Linux and the Microsoft family of Windows Servers are examples of client/server network operating systems.

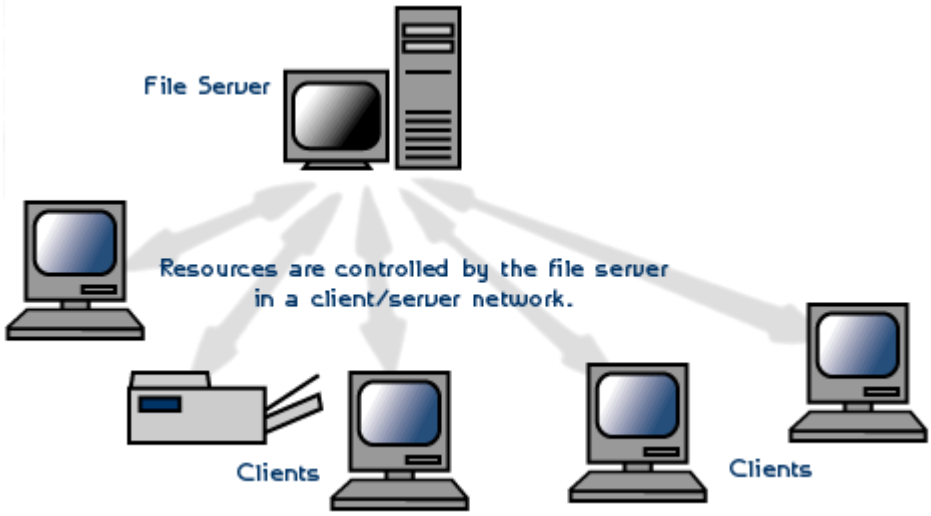


Fig. 2. Client/server network

Advantages of a client/server network:

- **Centralized** - Resources and data security are controlled through the server.
- **Scalability** - Any or all elements can be replaced individually as needs increase.
- **Flexibility** - New technology can be easily integrated into system.
- **Interoperability** - All components (client/network/server) work together.
- **Accessibility** - Server can be accessed remotely and across multiple platforms.

Disadvantages of a client/server network:

- **Expense** - Requires initial investment in dedicated server.
- **Maintenance** - Large networks will require a staff to ensure efficient operation.
- **Dependence** - When server goes down, operations will cease across the network.

Types of User Roles and Permissions:

1. Administrator (Root/Superuser)

- Full control over the server
- Ability to install/remove software, configure settings, manage users

2. Power User/Privileged User

- Elevated access but limited compared to an administrator
- Can perform advanced configurations but restricted from critical system changes

3. Standard User

- Limited access to basic functionalities
- Cannot install software or change critical settings

4. Guest User

- Minimal access for temporary or testing purposes
- Usually has read-only permissions

5. Service Accounts

1. Used by applications and services, not humans
2. Limited access to only necessary system functions

The **proper configuration of the user access levels** is essential for the network security and for its operational efficiency. This involves the following:

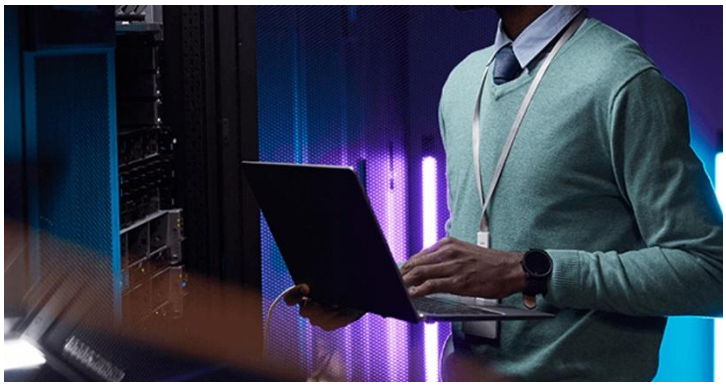
1. **User Authentication** – Verifies user identity through credentials such as usernames, passwords, or biometric data, often managed via directory services like Active Directory.
2. **Access Control** – Implements role-based permissions (e.g., administrator, standard user, guest) to regulate access to network resources.
3. **Group Policies** – Allows administrators to enforce rules for user groups and devices, such as restricting software installations or enforcing password policies.
4. **Network Access Control (NAC)** – Ensures that only authorized devices and users can connect to the network, incorporating pre-admission security compliance checks and continuous post-admission monitoring.

Network policies define the access control mechanisms and usage rules for network resources. The key components of it include:

1. **Authentication Policies** – Establish procedures for verifying the user identities, including multi-factor authentication (MFA).
2. **Authorization Policies** – Determine the access rights based on user roles and organizational policies.
3. **Quality of Service (QoS)** – Prioritizes network traffic, ensuring optimal performance for critical applications such as Voice over IP (VoIP) and video conferencing.
4. **Firewall Rules** – Regulate inbound and outbound traffic to prevent the unauthorized access and cyber threats.
5. **Network Policy Server (NPS)** – A Windows Server feature that enforces organizational-wide connection policies for VPNs and wireless access points.

What To Do?

Do you get a glimpse of it? Let's have an exercise! Here's the scenario:



Imagine you are working as a **Network Administrator** for a small business. Your job is to ensure that the company's network runs smoothly, remains secure, and allows employees to access the necessary resources efficiently. Every day, you receive IT support requests from employees experiencing different network-related issues.

Instructions:

- Prepare an A4-sized document to serve as your IT support log.
- In the document, copy the table below containing network-related issues reported by employees.\

Employee Request	Network Tool/Feature to Use	Explanation/ Justification
"I forgot my password and can't log in to my workstation. Can you help me reset it?"		
"Our team needs to share large project files, but email attachments are too limited. What's the best way to share files securely over the network?"		
"I'm working remotely and need to access my files and applications from home. How can I securely connect to the office network?"		
"Our network has been slow, and video calls keep lagging. Is there a way to prioritize video conferencing over other network traffic?"		
"We need to ensure that only authorized employees can access the company's Wi-Fi. How can we secure our wireless network?"		

After reading all the requests, choose the correct network tool, feature, or setting for each case and explain why you selected it. Think about how it will help resolve the issue efficiently and securely.

In this exercise, you took on the role of a **Network Administrator**, making key decisions about which network tools and configurations to use for different real-world problems. Selecting the appropriate feature or tool is essential for ensuring **network security, efficiency, and user accessibility** in any organization. By understanding how these solutions work, you'll be able to troubleshoot and manage network issues effectively.

What To Consider?

Always remember:

✓ The right network configuration ensures security, efficiency, and accessibility.

✓ Incorrect settings can lead to security vulnerabilities, network failures, or unauthorized access.

✓ Proper handling and selection of network tools and policies is a fundamental skill in network administration.

Apply and Perform!

Performance Task: P2P Network Access Setup

Scenario:

Imagine you are an IT technician setting up a peer-to-peer (P2P) network for a small office with two computers. The goal is to enable secure file sharing while ensuring that different users have the appropriate access to the shared folder based on their roles.

Task:

Set up a P2P network and configure a shared folder with the following access levels:

- **Admin:** Full access (read, write, modify, and delete files).
- **Manager:** Read and write access to specific files.
- **Employee:** Read-only access to certain files.
- **Guest:** No access to the shared folder.

Instructions:

1. **Set up the P2P network:**
   - Connect both computers via a switch, router, or direct connection (e.g., Ethernet cable or Wi-Fi).
   - Configure IP addresses (use static IPs or enable Dynamic Host Configuration Protocol (DHCP)).
   - Ensure that both computers are in the same workgroup (for Windows) or same network (for Linux/macOS).
2. **Enable File Sharing:**
   - On one computer, create a shared folder for the office files.
   - Enable file sharing settings to allow other computers to access it.
3. **Configure Role-Based Access:**
   - Assign permissions to users based on their roles:
     - Admin: Full control.
     - Manager: Modify permissions for specific files only.
     - Employee: Read-only access.
     - Guest: No access.

- Use Windows File Sharing (NTFS permissions) or Linux commands to enforce these permissions.

4. **Document Your Process:**
    - List the tools and settings you used (e.g., network settings, file-sharing configurations).
    - Explain why each role was assigned specific access permissions.
    - Provide screenshots (if applicable) or describe any challenges faced during setup.

In this exercise, you played the role of an **IT technician**, making critical decisions about **network security and access control**. Assigning the correct permissions ensures that files are **protected** while still allowing users to perform their necessary tasks. Understanding **role-based access** is essential for securing **organizational networks** and preventing **unauthorized data access**.

The Criteria for the Performance Task

Criteria	Excellent (10 pts)	Proficient (8 pts)	Developing (6 pts)	Needs Improvement (4 pts)	Weight
Accuracy	P2P network is correctly set up with appropriate IP configuration and role-based access control applied precisely.	Network is mostly functional, with minor misconfigurations that do not significantly impact functionality.	Network is partially functional but has noticeable errors in configuration or access control.	Network setup is incorrect or missing critical components.	40%
Clarity of Documentation	Steps are clearly written, detailed, and logically sequenced; easy to follow for replication.	Steps are mostly clear but may lack some minor details or structure.	Steps are somewhat unclear, lacking necessary details or logical flow.	Steps are vague, incomplete, or difficult to follow.	30%
Visual Evidence	Screenshots or video are clear, well-annotated, and fully demonstrate correct setup and access settings.	Screenshots or video are included but may lack annotations or minor details.	Screenshots or video are unclear, missing key steps, or poorly organized.	No visual evidence provided, or visuals do not match the documented steps.	30%

What to Check

Now that you've explored the contents and activities of this lesson, it's time to reflect on what you've learned. Answer this short quiz to assess your understanding of **user access level configurations**, their classifications, proper selection, and implementation in a network environment. Apply what you've learned and carefully consider each question. Good luck!

📌 **How to Access the Short Quiz:**

🔗 Click this link: https://forms.gle/X313QwAnMtbHLn1CA

OR

📱 Just kindly scan this QR Code to access the Short Quiz via Google Forms.

Scan this →

SCAN ME

What I have learned

Reflect on the activities and discussions from this lesson about setting user access and network security. Think about how these concepts make you feel and why you believe they are important, not just from a technical perspective, but also from a personal and ethical standpoint.

Guide Questions:

1. Why do you think it's important to assign the correct access level to each role? Consider how your own values of responsibility, trust, and respect for others' privacy influence your view on this topic.

2. How do network policies, such as authentication and data security, impact your sense of responsibility and commitment to protecting resources? Reflect on how these practices make you feel about your role in safeguarding data and maintaining smooth operations, whether in a personal, professional, or organizational context.

3. Share examples from the activities or real-life situations where you felt strongly about the importance of these practices. How did these experiences shape your understanding of security and the ethical responsibility it involves?

References:

FCIT. (n.d.). *Chapter 6 on network operating systems*. Retrieved March 5, 2025, from https://fcit.usf.edu/network/chap6/chap6.htm

Lenovo. (n.d.). *Glossary: Overview of NOS features*. Retrieved March 5, 2025, from What is a network operating system | Can NOS work with any networking protocol? | Lenovo US

TechTarget. (n.d.). *Network operating system (NOS) definition and functionalities*. Retrieved March 5, 2025, from What is a Network Operating System? | Definition from TechTarget

Microsoft. (n.d.). *Network Policy Server documentation*. Retrieved March 5, 2025, from Network Policy Server (NPS) | Microsoft Learn

DataScientest. (n.d.). *Guide to NOS features*. Retrieved March 5, 2025, from A complete guide to network operating systems

PrepBytes Blog. (n.d.). *Types and functions of NOS*. Retrieved March 5, 2025, from Network Operating System: Types and Functions