Unit 5: Static IP Configuration & Advanced Server Management
1. Static IP Configuration
Steps to Assign a Static IP Address

1. Open Network Settings
Go to your device's **Control Panel / Settings → Network & Internet → Change Adapter Options** (Windows) or equivalent network settings on your system.

2. Select Network Adapter
Right-click your active connection (Wi-Fi or Ethernet) and choose **Properties**.

3. Open IPv4 Settings
Scroll and click **Internet Protocol Version 4 (TCP/IPv4)**, then press **Properties**.

4. Choose Manual Configuration
Select **"Use the following IP address"** instead of automatic (DHCP).

5. Enter IP Details
Fill in the required fields:

i. IP Address (e.g. 192.168.1.50)
ii. Subnet Mask (e.g. 255.255.255.0)
iii. Default Gateway (e.g. 192.168.1.1)

6. Enter DNS Servers
Add preferred DNS (e.g. 8.8.8.8 and 8.8.4.4 for Google DNS).

7. Save Settings
Click **OK / Apply**, then close all windows.

8. Restart Connection (if needed)
Disable and re-enable the network adapter or restart the device to apply changes.

1.2 Subnet Mask Configuration
The subnet mask is a critical network setting that defines how an IP address is divided into the network portion and the host portion. It determines which devices are considered part of the same local network and which require routing.

I. Understand the Purpose
The subnet mask tells a device:

i. Which part of the IP address identifies the network
ii. Which part identifies the host (individual device)
iii. Whether a destination is local or needs a router

II. Identify the Network Requirement
Before configuration:

i. Determine how many devices will be on the network
ii. Decide if the network is small, medium, or large
iii. Choose an appropriate subnet mask based on required hosts

Example of a Common Subnet Mask

i. Subnet Mask: 255.255.255.0
ii. Used in a typical Class C network

This means:

i. Network portion: First 24 bits (e.g. 192.168.1)

ii. Host portion: Last 8 bits
iii. Host capacity: Up to 254 usable devices (1–254)

IV. Configure the Subnet Mask on a Device

I. Open Network Settings
i. Go to the device's network configuration panel
ii. Access IPv4 settings

II. Enter IP Address
Example: 192.168.1.10

III. Enter Subnet Mask
Input: 255.255.255.0

IV. Set Default Gateway
Example: 192.168.1.1 (router address)

V. Configure DNS (if required)
Example: 8.8.8.8 or network-provided DNS

V. Verify Configuration

I. Check IP settings
Use command: ipconfig (Windows) or ifconfig / ip a (Linux)

II. Test connectivity
i. Ping gateway: ping 192.168.1.1
ii. Ping external site: ping google.com

VI. Confirm Network Behavior

i. Devices in the same subnet should communicate directly
ii. Devices outside the subnet require routing through a gateway
iii. Incorrect subnet mask may cause unreachable devices or routing failures

VII. Key Reminder

Choosing the correct subnet mask ensures:
i. Efficient network segmentation
ii. Proper communication between devices
iii. Reduced network congestion and routing errors

1.3 Default Gateway Setup

The default gateway is a router address that allows devices on a subnet to communicate with external networks.

Example: If a server has IP 192.168.1.50, the default gateway might be set to 192.168.1.1 to route packets outside the local network.

Incorrect default gateway settings can cause loss of internet or external network access.

1.4 DNS Configuration

Domain Name System (DNS) servers translate human-readable domain names into IP addresses.

Static IP devices must be configured with DNS server IP addresses to resolve domain names.

Example: Using public DNS servers such as Google DNS (8.8.8.8, 8.8.4.4) or company internal DNS servers.

2. DHCP vs Static IP Addressing

Aspect	DHCP (Dynamic IP)	Static IP
IP Address Assignment	Automatically assigned from a pool	Manually assigned and fixed
Configuration Effort	Minimal manual work required	Manual setup needed on each device

Use Cases	Client devices like laptops, mobile phones, and guest devices	Servers, network printers, devices requiring constant IP for accessibility
IP Address Consistency	Can change over time (lease expiration)	Fixed and stable
IP Address Conflicts	DHCP reduces conflicts by centralized management	Requires careful planning to avoid conflicts

2.1 Lease Period Concept in DHCP

3. Advanced Server Management

3.1 Server Monitoring and Optimization

Effective server management requires continuous monitoring and optimization to maintain performance and availability.

Performance Tools

i. **CPU, Memory, Disk Usage:** Tools like Task Manager (Windows), top/htop (Linux), or performance monitors show resource utilization.
ii. **Network Monitoring:** Tools such as Wireshark, netstat, or SNMP-based monitors track traffic and detect bottlenecks.
iii. **Process and Service Monitoring:** Ensures critical services are running and responsive.

Log Analysis

i. System logs record events, errors, and warnings useful for troubleshooting.
ii. Application and security logs track user activity and detect anomalies.
Examples of log tools: Windows Event Viewer, Linux syslog, Splunk, ELK stack.

3.2 Backup and Disaster Recovery Strategies

Building robust backup and recovery plans is essential to protect data against loss or corruption.

Backup Types

i. Full Backup: A complete copy of all data at a specific time.
ii. Incremental Backup: Only backs up data changed since the last backup (saving space and time).
iii. Differential Backup: Backs up data changed since the last full backup (not incremental but cumulative).

Restoration Planning

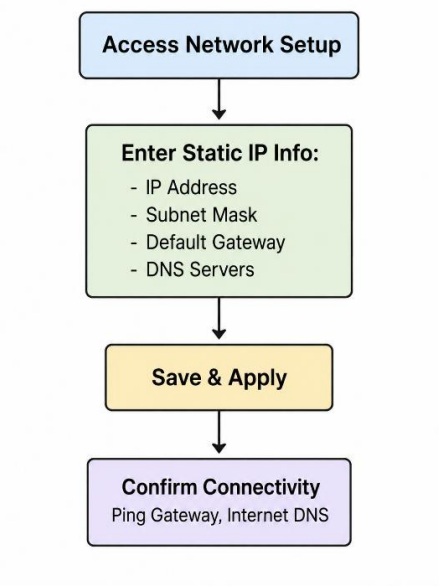
i. Test recovery process regularly to ensure backups are valid and restorable.
ii. Maintain offsite or cloud backups to protect against site-wide disasters.
iii. Document backup schedules, storage locations, and responsible personnel.

3.3 Example Backup Schedule

Day	Backup Type	Description
Sunday	Full	Complete copy of all server data
Monday - Saturday	Incremental	Backup of only changed data since last backup

4. Diagrams

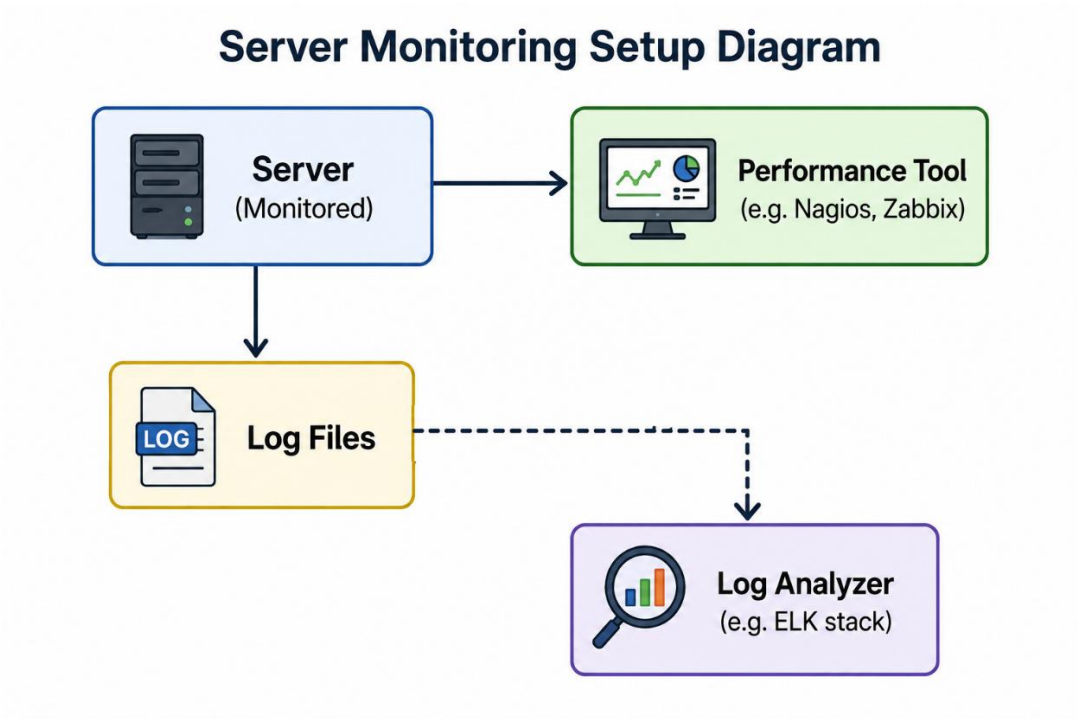
4.1 Static configuration flow



4.2 Lease Process in DHCP

Step	Message	Direction	Description
1	DHCP Discover	Client → Broadcast	Client searches for DHCP servers
2	DHCP Offer	Server → Client (Broadcast)	Server offers IP address and config
3	DHCP Request	Client → Server	Client requests offered IP
4	DHCP Acknowledgment	Server → Client	Server confirms assignment and lease

4.3 Server Monitoring Setup Diagram



4.4 Backup and Disaster Recovery Plan Flow

