SESSION 1 & 2 – WINDOWS OPERATING SYSTEM

(PG Diploma in Computer Science – System & Server Administration)

---

1. Overview of Windows Operating System

1.1 Definition

The **Windows Operating System (OS)** is a **proprietary, graphical, multitasking operating system** developed by **Microsoft** that manages computer hardware, software resources, and provides services to applications and users.

1.2 Purpose of Windows OS

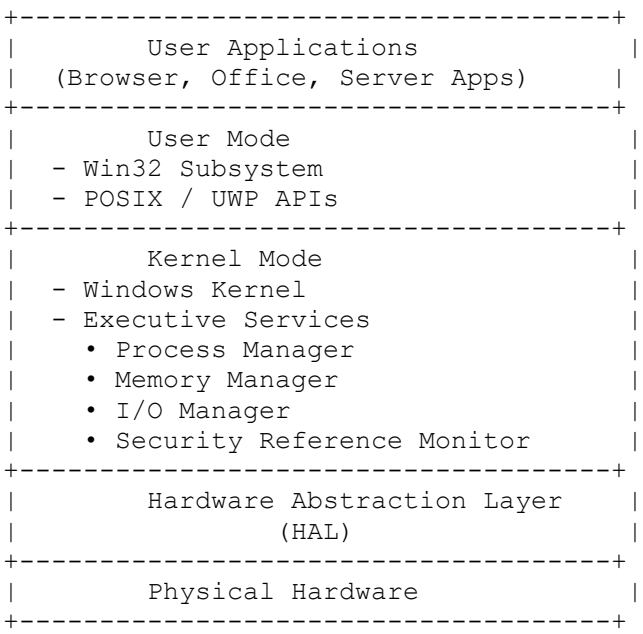
- Acts as an **interface between user and hardware**
- Manages **CPU, memory, storage, and I/O devices**
- Provides **security, networking, and application support**
- Supports **enterprise workloads** (AD, DNS, IIS, Hyper-V)
- Enables **client–server and cloud integration**

1.3 Key Features

- GUI-based (Explorer, Start Menu)
- Multi-user & multitasking
- NTFS/ReFS file systems
- Integrated networking
- Active Directory support
- Built-in security (Defender, BitLocker)
- Virtualization (Hyper-V)

1.4 Windows OS Architecture

High-Level Architecture



Kernel Components

Component	Function
Kernel	Low-level OS operations
HAL	Abstracts hardware differences
Device Drivers	Hardware communication
Executive	Resource management

1.5 Windows Editions & Versions

Client Editions

Edition	Use Case
Home	Personal use
Pro	Business users
Enterprise	Large organizations
Education	Academic institutions

Server Editions

Edition	Features
Standard	Physical/limited virtualization
Datacenter	Unlimited virtualization
Essentials	Small business
Azure Edition	Cloud-integrated workloads

Client vs Server

Feature	Client	Server
AD DS	❌	☑
Hyper-V	Limited	Full
IIS	Limited	Full
Users	Few	Thousands

---

2. Installation of Windows Operating System

2.1 Installation Types

Type	Description
Clean Install	Fresh OS, no data retained
Upgrade	Existing OS preserved
Migration	Move OS/data to new system

2.2 System Requirements (Example: Windows Server 2022)

- CPU: 64-bit, 1.4 GHz
- RAM: 2 GB minimum
- Disk: 32 GB+
- Firmware: UEFI + Secure Boot
- Network: Gigabit recommended

2.3 Step-by-Step Installation Workflow

```
Boot → Language Selection → Edition
→ Disk Partitioning → File Copy
```

```
→ Feature Installation → Updates
→ Reboot → Initial Configuration
```

Clean Installation Steps

1. Boot from USB/DVD (UEFI preferred)
2. Select language & edition
3. Choose **Custom Installation**
4. Create partitions
5. Install OS files
6. Complete OOBE (Admin, region, updates)

Upgrade Installation Steps

1. Run `setup.exe` from media
2. Choose **Upgrade**
3. Compatibility check
4. Install while retaining apps/data

---

3. Install, Upgrade, and Migrate Servers and Workloads

3.1 Server Installation Methods

Method	Description
Manual	GUI-based
Unattended	Answer files
WDS	Network boot
MDT	Enterprise deployment
SCCM	Large-scale management

3.2 Migration Concepts

Migration = Moving:

- OS
- Roles & Features

- Data
- Applications
- User profiles

Migration Tools

Tool	Purpose
Windows Server Migration Tools	Roles & data
Robocopy	File migration
USMT	User profiles
Azure Migrate	Cloud migration

Upgrade vs Migration

Upgrade	Migration
Same hardware	New hardware
Faster	Safer
Risky	Clean

Enterprise Scenario

Migrating **Windows Server 2012 R2 AD + File Server** to **Server 2022** using:

- New VM
- Server Migration Tools
- DNS & AD replication

---

4. Create, Manage, and Maintain Images for Deployment

4.1 Imaging Definition

OS Imaging is the process of capturing and deploying a standardized Windows installation across multiple systems.

4.2 Imaging Components

Component	Purpose
WIM	Windows Image file
DISM	Image servicing
Sysprep	Generalization
MDT/WDS	Deployment

4.3 Windows Image Format (WIM)

- File-based image
- Single-instance storage
- Multiple editions in one image

4.4 DISM (Deployment Image Servicing and Management)

Common Commands

```
dism /get-wiminfo /wimfile:install.wim
dism /mount-image /imagefile:install.wim /index:1 /mountdir:C:\Mount
dism /image:C:\Mount /add-driver /driver:C:\Drivers
dism /unmount-image /commit
```

4.5 Sysprep

Purpose

- Removes SID
- Generalizes OS
- Prepares for cloning

```
sysprep /generalize /oobe /shutdown
```

4.6 Image Deployment Workflow

```
Reference System
→ Install OS & Apps
→ Sysprep
→ Capture WIM
→ Store Image
→ Deploy via MDT/WDS
```

4.7 Real-World Enterprise Scenario

Deploying Windows 11 to **500 lab systems** using:

- MDT
- Custom WIM
- Unattended.xml
- Domain join automation

---

5. Troubleshooting Common Installation Issues

Issue	Cause	Fix
No disk found	Missing driver	Load storage driver
Boot loop	Legacy/UEFI mismatch	Fix firmware mode
Setup stuck	Corrupt media	Recreate USB
Upgrade fails	Incompatible app	Remove app

---

6. Best Practices

- Use **UEFI + GPT**
- Keep **golden image minimal**
- Separate OS & data disks
- Test images before rollout
- Automate with MDT/SCCM
- Always backup before upgrade

---

7. Exam-Oriented Key Points

- HAL abstracts hardware
- WIM supports multiple editions
- Sysprep removes SID
- Migration preferred over upgrade
- DISM replaces ImageX
- Datacenter = unlimited VMs

---

8. Interview Questions & Answers

Q1: Difference between upgrade and migration?

Answer: Upgrade keeps OS on same hardware; migration moves to new system.

Q2: Why Sysprep is required?

Answer: To remove SID and prepare system for cloning.

Q3: What is DISM used for?

Answer: To service Windows images offline/online.

Q4: Why WIM over Ghost?

Answer: File-based, hardware-independent, multi-image support.

Q5: What is a golden image?

Answer: A standardized, tested OS image for mass deployment.

---

9. One-Line Summary (For Viva)

Windows OS provides a secure, scalable platform for enterprise computing, and imaging tools like WIM, DISM, and Sysprep enable efficient large-scale deployment.

SESSION 3 – Windows Server Backup (WSB)

Role Focus: Backup & Disaster Recovery Specialist
Applies To: Windows Server 2012 / 2016 / 2019 / 2022

1. Concept of Windows Server Backup (WSB)

1.1 Definition

Windows Server Backup (WSB) is a **built-in backup and recovery feature** in Microsoft Windows Server that allows administrators to **protect critical data, system state, applications, and entire servers** against failures, corruption, ransomware, and disasters.

1.2 Purpose of Windows Server Backup

WSB is used to:

- Protect **server data and OS**
- Enable **fast recovery** after failures
- Support **business continuity**
- Minimize **downtime and data loss**
- Provide **disaster recovery (DR)** capability

1.3 Why Backup Is Critical in Enterprises

Risk	Impact
Hardware failure	Data loss
Ransomware	Encrypted systems
Human error	Accidental deletion
OS corruption	Server crash
Natural disasters	Complete site loss

➡ **Backup + DR = Business Survival**

1.4 Backup Terminology (Core Concepts)

1. Full Backup

- Backs up **entire selected data**
- Largest size
- Longest backup time
- Baseline backup

2. Incremental Backup

- Backs up **only changed data** since last backup
- Faster
- Smaller storage usage
- Depends on previous backups

3. System State Backup

Includes:

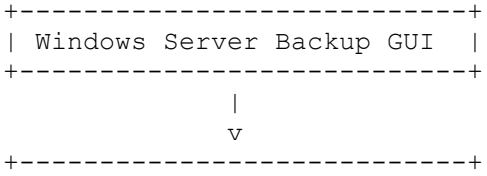
- Registry
- Boot files
- COM+ Class Registration
- Active Directory (on DC)
- SYSVOL
- Certificate Services

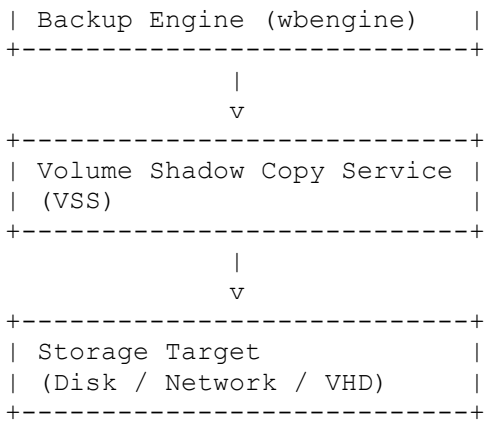
➡ **Mandatory for Domain Controllers**

1.5 Backup Types Supported by WSB

Backup Type	Description
Full Server	Entire server including OS
Bare Metal	OS + system files (no data)
System State	Critical OS components
Volume Backup	Selected drives
File/Folder	Specific files

1.6 Windows Server Backup Architecture





1.7 Key Components of WSB

1. Windows Server Backup Console

- GUI-based management tool

2. wbadmin.exe

- Command-line & PowerShell utility

3. Volume Shadow Copy Service (VSS)

- Creates consistent snapshots
- Ensures open files are backed up safely

4. Backup Storage Targets

- Local disk
- External USB
- Network share
- iSCSI / SAN (indirect)

---

2. Implement Windows Server Backup

2.1 Installing Windows Server Backup Feature

Using GUI

1. Open **Server Manager**
2. Add Roles and Features
3. Select **Windows Server Backup**
4. Install

Using PowerShell

```
Install-WindowsFeature Windows-Server-Backup
```

2.2 Backup Storage Options

Target	Recommended
Local Disk	❌ Not recommended
Dedicated Disk	☑ Best
USB External Disk	☑ Good
Network Share	⚠ Limited
Tape	❌ Not supported

2.3 Scheduling Backups (GUI)

Steps

1. Open **Windows Server Backup**
2. Click **Backup Schedule**
3. Choose:
    - Full Server / Custom
4. Select backup time
5. Select destination disk
6. Confirm

➡ WSB uses incremental backups after first full backup

2.4 One-Time Backup (GUI)

Used for:

- Emergency backup
- Pre-upgrade backup

- Manual protection

Steps

1. Select **Backup Once**
2. Choose backup configuration
3. Select destination
4. Start backup

2.5 Backup Using PowerShell (wbadmin)

Full Server Backup

```
wbadmin start backup -backupTarget:E: -allCritical -quiet
```

System State Backup

```
wbadmin start systemstatebackup -backupTarget:E: -quiet
```

Volume Backup

```
wbadmin start backup -include:C: -backupTarget:E: -quiet
```

2.6 Backup Scheduling via PowerShell

```
wbadmin enable backup -addtarget:E: -schedule:21:00 -allCritical -quiet
```

---

3. Restore Scenarios in Windows Server Backup

3.1 File & Folder Restore

GUI Steps

1. Open Windows Server Backup
2. Select **Recover**
3. Choose backup date
4. Select files/folders
5. Restore to:

    - Original location
    - Alternate location

3.2 System State Restore

Used for:

- AD recovery
- Registry corruption
- Boot failure

Steps

```
wbadmin start systemstaterecovery
```

➡ Requires **Directory Services Restore Mode (DSRM)** for DCs

---

3.3 Bare Metal Recovery (BMR)

Purpose

- Recover entire server from scratch

Requirements

- Same or similar hardware
- Windows installation media
- Backup disk/network access

Process

1. Boot from Windows Server ISO
2. Choose **Repair your computer**
3. Select **System Image Recovery**
4. Select backup
5. Restore

---

4. Disaster Recovery – Real-World Scenarios

Scenario 1: Ransomware Attack

- Server encrypted
- Solution:
    - Disconnect network
    - Boot recovery environment
    - Perform **Bare Metal Restore**

Scenario 2: Domain Controller Failure

- AD corruption
- Solution:
    - Boot into DSRM
    - Restore **System State**
    - Restart DC

Scenario 3: Accidental File Deletion

- Restore individual files from backup

Scenario 4: Disk Failure

- Replace disk
- Restore volume backup

---

5. Common Backup Failures & Troubleshooting

Issue 1: Backup Failed – Not Enough Space

- Cause: Destination disk full
- Fix:
    - Expand disk
    - Delete old backups

Issue 2: VSS Errors

- Cause: Corrupt shadow copy
- Fix:

```
vssadmin list writers
vssadmin delete shadows /all
```

Issue 3: Network Backup Failure

- Cause:
  - Credentials issue
  - Network drop
- Fix:
  - Use dedicated service account
  - Verify permissions

Issue 4: Backup Not Running as Scheduled

- Check:
  - Task Scheduler
  - Backup service status
  - Event Viewer

---

6. Best Practices & Security Considerations

Best Practices

- ✔ Use **dedicated backup disk**
- ✔ Follow **3-2-1 rule** (3 copies, 2 media, 1 offsite)
- ✔ Test restores regularly
- ✔ Encrypt backup storage
- ✔ Maintain backup logs
- ✔ Use **offsite or cloud DR**

Security Considerations

- Restrict backup access
- Protect backup disks from ransomware
- Use BitLocker on backup disks
- Store credentials securely
- Monitor backup logs

---

7. Exam-Oriented Key Points

- WSB uses **VSS**
- Incremental after first full backup
- Bare Metal includes OS + boot
- System State is critical for DC
- WSB does **NOT support tape**
- Network backup limited to one version

---

8. Interview Questions & Answers

Q1. What is Windows Server Backup?

A: Built-in Windows feature for data, system, and full server backup & recovery.

Q2. Difference between Full and Bare Metal backup?

A: Full includes data + OS; Bare Metal includes OS + system files only.

Q3. Why is System State backup important?

A: It protects critical OS components like AD, registry, and boot files.

Q4. What is VSS?

A: Volume Shadow Copy Service ensures consistent backups of open files.

Q5. Can WSB back up to tape?

A: No, tape is not supported.

Q6. How do you recover a crashed Domain Controller?

A: Boot into DSRM and restore System State.

Q7. Command for full server backup?

```
wbadmin start backup -allCritical
```

---

9. Mini Case Study

Company: Mid-size enterprise
Problem: Ransomware attack encrypted file server
Solution:

- Offline backup disk used
- Bare Metal Recovery performed
- Server restored within 2 hours
  Result: Zero data loss, minimal downtime

SESSION 4 & 5 – ACTIVE DIRECTORY INFRASTRUCTURE

(PG Diploma in Computer Science – Windows Server & Identity Management)

---

1. Planning, Implementation, and Maintenance of Active Directory Infrastructure

---

1.1 Definition of Active Directory (AD)

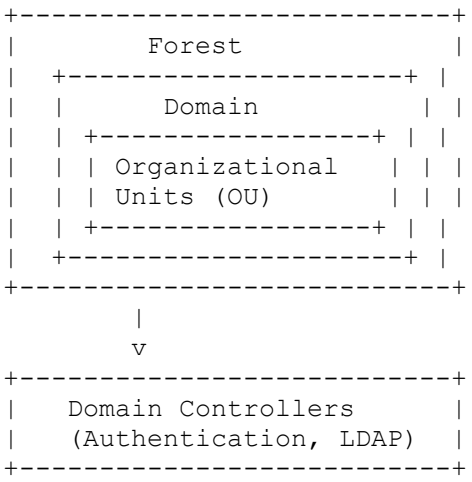
Active Directory (AD) is Microsoft's **centralized directory service** used to manage **users, computers, groups, applications, and security policies** in a Windows domain environment.

1.2 Purpose of Active Directory

- Centralized **identity and access management**
- Authentication & authorization
- Policy enforcement using **Group Policy**
- Resource management (files, printers, apps)
- Scalability for **enterprise networks**

1.3 Active Directory Architecture Overview

High-Level AD Architecture



1.4 AD Logical Components

Component	Description
Forest	Security boundary
Domain	Administrative boundary
Tree	Collection of domains
OU	Logical container

Component	Description
Object	User, group, computer
Schema	Blueprint of AD

1.5 AD Physical Components

Component	Description
Domain Controller	Hosts AD DS
Sites	Physical network locations
Subnets	IP ranges mapped to sites
Replication	Data synchronization

1.6 Forest, Domain & OU Design

Forest Design

- One forest = one **security boundary**
- Avoid multiple forests unless:
  - Legal separation
  - Different schema requirements

Domain Design

- Single domain preferred
- Multiple domains only if:
  - Password policies differ (pre-2016)
  - Legal boundaries

OU Design (Best Practice)

```
Domain
│
├── OU=Servers
├── OU=Workstations
├── OU=Users
│    ├── OU=HR
│    ├── OU=IT
│    └── OU=Finance
```

OU benefits:

- Delegation
- GPO targeting
- Administrative control

---

2. Implementing and Administering Active Directory

2.1 AD DS (Active Directory Domain Services)

Definition

AD DS stores directory data and manages communication between users and domains.

Core AD DS Services

- LDAP
- Kerberos authentication
- DNS integration
- Replication

2.2 Installing Active Directory Domain Services

Prerequisites

- Windows Server
- Static IP
- Proper DNS
- NTFS volume

Installation Workflow

```
Install Windows Server
→ Add AD DS Role
→ Promote to Domain Controller
```

```
→ Create New Forest / Join Domain
→ Reboot
```

Promotion to Domain Controller

```
Install-WindowsFeature AD-Domain-Services
Install-ADDSForest -DomainName corp.local
```

---

3. User Accounts and Groups in Active Directory

3.1 User Accounts

Types of User Accounts

Type	Description
Domain User	Centralized authentication
Built-in	Administrator, Guest
Service Account	Application services
gMSA	Managed service accounts

User Creation Tools

- ADUC (GUI)
- PowerShell

```
New-ADUser -Name "Ravi Kumar" -SamAccountName rkumar
```

3.2 Groups in Active Directory

Group Types

Type	Purpose
Security	Access control
Distribution	Email only

Group Scopes

Scope	Usage
Domain Local	Resource permissions
Global	Users within domain
Universal	Multi-domain

AGDLP Model (Best Practice)

```
Accounts → Global → Domain Local → Permission
```

---

4. Active Directory Domain Services (AD DS)

4.1 AD DS Components

Component	Role
NTDS.DIT	AD database
SYSVOL	GPO storage
Schema	Object definitions
GC	Forest-wide searches

4.2 Authentication & Authorization Workflow

Kerberos Authentication Flow

```
User Login
→ AS Request (KDC)
→ TGT Issued
→ Service Ticket
→ Access Granted
```

Authorization

- Group membership
- ACL evaluation
- Least privilege principle

---

5. Domain Controller (DC)

5.1 Domain Controller Definition

A **Domain Controller** is a server that hosts **AD DS** and authenticates users and computers.

5.2 FSMO Roles

FSMO Role	Function
Schema Master	Schema updates
Domain Naming Master	Domain creation
RID Master	SID allocation
PDC Emulator	Time, passwords
Infrastructure Master	Object references

5.3 DC Best Practices

- Dedicated server
- Regular backups
- Antivirus exclusions
- Secure physical access

---

6. Additional Domain Controller (ADC)

6.1 Definition

An **Additional Domain Controller** is an extra DC added for:

- Redundancy
- Load balancing
- Site resilience

6.2 Replication Process

```
Change on DC1
→ Replication via RPC
→ ADC updated
```

6.3 Global Catalog (GC)

- Stores partial forest data
- Required for logon
- Recommended on all DCs

---

7. Client (Windows 10/11)

7.1 Domain-Joined Client

Definition

A client system authenticated using **domain credentials**.

Join Domain Process

```
Client → DNS Query
→ Locate DC
→ Computer Account Created
→ Trust Established
```

Benefits

- Centralized login
- Group Policy
- Single Sign-On (SSO)

---

8. Member Server (MS)

8.1 Definition

A **Member Server** is a server joined to a domain but **not a DC**.

8.2 Roles of Member Server

- File server
- Application server
- IIS server
- Database server

8.3 Difference: DC vs Member Server

DC	Member Server
Hosts AD DS	Does not
Authenticates users	Uses DC
Stores AD database	No

---

9. Enterprise Real-World AD Scenarios

Scenario 1: Corporate AD Design

- Single forest
- Single domain
- Multiple OUs
- Two DCs per site

Scenario 2: High Availability

- 2 DCs + 1 ADC
- GC enabled
- DFS-R SYSVOL

Scenario 3: Branch Office

- RODC
- Cached credentials
- Limited admin access

---

10. Common AD Failures & Troubleshooting

Issue	Cause	Fix
Login failure	DNS issue	Fix DNS
Replication error	Time skew	Sync NTP
GPO not applied	SYSVOL issue	DFSR check
Slow login	GC missing	Enable GC

Tools

- `dcdiag`
- `repadmin`
- Event Viewer
- ADUC

---

11. AD Security Best Practices

- Least privilege
- Secure admin accounts
- Separate admin & user accounts
- Enable auditing
- Protect FSMO roles
- Regular AD backups

---

12. Exam-Oriented Key Points

- Forest = security boundary
- Domain = administrative boundary
- OU = delegation & GPO
- Kerberos = default auth
- ADC improves availability
- GC required for login

---

13. Interview Questions & Answers

Q1: Difference between forest and domain?

Answer: Forest is a security boundary; domain is an administrative boundary.

Q2: Why multiple domain controllers?

Answer: Fault tolerance, load balancing, redundancy.

Q3: What happens if PDC Emulator fails?

Answer: Password changes and time sync affected.

Q4: What is SYSVOL?

Answer: Shared folder storing GPOs and scripts.

Q5: Why DNS is critical for AD?

Answer: AD relies on DNS for locating domain controllers.

---

14. One-Line Viva Summary

Active Directory provides centralized identity, authentication, authorization, and policy management for enterprise Windows environments.

SESSION 6 & 7 – DNS, DHCP & IPAM

(PG Diploma in Computer Science – Windows Server Network Services)

---

1. Domain Name System (DNS)

1.1 Definition

DNS (Domain Name System) is a **hierarchical, distributed name resolution service** that translates **hostnames into IP addresses** and vice versa.

Example:
`www.microsoft.com → 20.112.x.x`

1.2 Purpose of DNS

- Name resolution
- Service discovery
- Active Directory dependency
- Load balancing
- Application connectivity

⚠ **Active Directory cannot function without DNS**

1.3 DNS Architecture

DNS Hierarchy

```
Root (.)
 |
 +-- .com
 |    |
 |    +-- microsoft.com
 |         |
 |         +-- www
 |
 +-- .org
 +-- .edu
```

DNS Components

Component	Description
DNS Server	Stores zone data
DNS Zone	Database of records
Resolver	Client querying DNS
Resource Records	DNS entries

1.4 DNS in Active Directory Environment

```
Client
  |
  v
DNS Query (_ldap._tcp.dc._msdcs.domain)
  |
  v
Domain Controller
```

AD Uses DNS For:

- Locating DCs
- Kerberos authentication
- Replication
- Group Policy processing

1.5 DNS Zones

Zone Types

Zone	Description
Primary	Read/write
Secondary	Read-only copy
Stub	Only NS records
AD-Integrated	Stored in AD

Zone Replication Scope

- Domain-wide
- Forest-wide
- Custom application partition

1.6 DNS Records

Record	Purpose
A	Hostname → IPv4
AAAA	Hostname → IPv6
CNAME	Alias
MX	Mail server
NS	Name server
SRV	Service locator (AD)
PTR	Reverse lookup

1.7 Installing & Configuring DNS Server

Installation

```
Install-WindowsFeature DNS -IncludeManagementTools
```

DNS Configuration Steps

1. Create Forward Lookup Zone
2. Create Reverse Lookup Zone
3. Enable secure dynamic updates
4. Configure scavenging
5. Test name resolution

1.8 DNS Troubleshooting

Issue	Cause	Fix
Clients can’t login	DNS misconfig	Fix SRV records
Slow logins	No reverse zone	Create PTR
DC not found	Wrong DNS IP	Use DC IP

Tools

- `nslookup`
- `dnscmd`
- Event Viewer
- `dcdiag /test:dns`

1.9 DNS Best Practices

- Use **AD-integrated zones**
- Enable **DNS scavenging**
- No external DNS on DC
- One DNS per DC
- Secure dynamic updates only

---

2. Dynamic Host Configuration Protocol (DHCP)

2.1 Definition

DHCP automatically assigns **IP address configuration** to network clients.

2.2 Purpose

- Eliminates manual IP configuration
- Prevents IP conflicts
- Centralized network management

2.3 DHCP Architecture

```
Client → Discover
Server → Offer
Client → Request
Server → Acknowledge
(DORA)
```

2.4 DHCP Components

Component	Description
Scope	IP range
Lease	Time-bound IP
Reservation	Fixed IP
Exclusion	Blocked IP
Options	Network parameters

2.5 DHCP Scope Configuration

Scope Elements

- Start IP
- End IP
- Subnet mask
- Lease duration

Common DHCP Options

Option	Purpose
003	Default Gateway
006	DNS Server
015	DNS Suffix
066/067	PXE Boot

2.6 DHCP Installation & Authorization

```
Install-WindowsFeature DHCP -IncludeManagementTools
Add-DhcpServerInDC
```

⚠ DHCP must be **authorized in AD**

2.7 DHCP Failover

Modes

Mode	Description
Load Balance	50/50
Hot Standby	Active/Passive

2.8 DHCP Troubleshooting

Issue	Cause	Fix
No IP assigned	Scope exhausted	Extend scope
Wrong gateway	Option missing	Configure option
Unauthorized DHCP	Rogue server	Deauthorize

Tools

- `ipconfig /all`
- `ipconfig /release`
- `ipconfig /renew`

2.9 DHCP Best Practices

- Use DHCP failover
- Short leases for Wi-Fi
- Reservations for servers
- Separate scopes per subnet

---

3. IP Address Management (IPAM)

3.1 Definition

IPAM is a **centralized framework** to manage **IP addresses, DHCP, DNS, and auditing**.

3.2 Purpose

- Prevent IP conflicts

- Track IP utilization
- Centralized visibility
- Compliance & auditing

3.3 IPAM Architecture

```
IPAM Server
  |
  +-- DNS Servers
  +-- DHCP Servers
  +-- Domain Controllers
```

3.4 IPAM Components

Component	Function
IPAM Server	Central console
Access Scopes	Permission control
GPOs	Managed server access
Database	IP tracking

3.5 IPAM Deployment Workflow

```
Install IPAM
→ Provision GPOs
→ Discover Servers
→ Manage DNS/DHCP
```

Installation

```
Install-WindowsFeature IPAM -IncludeManagementTools
```

3.6 IPAM Management Capabilities

- IP address tracking
- DHCP scope monitoring
- DNS zone visibility
- Event auditing

3.7 IPAM Limitations

- No multi-forest support
- No non-Microsoft DHCP
- Not real-time scanning

---

4. Enterprise Real-World Scenarios

Scenario 1: AD-Based DNS

- DNS installed on DCs
- AD-integrated zones
- Secure updates enabled

Scenario 2: Large Enterprise DHCP

- Central DHCP servers
- Failover enabled
- VLAN-based scopes

Scenario 3: Enterprise IPAM

- IP utilization tracking
- Compliance auditing
- Automated IP lifecycle

---

5. Common Failures & Troubleshooting

Service	Failure	Resolution
DNS	DC not located	Fix SRV records
DHCP	No IP	Check authorization
IPAM	Server unreachable	GPO provisioning

---

6. Security Best Practices

- Secure DNS dynamic updates
- Block rogue DHCP servers
- Audit IP changes
- Restrict IPAM access
- Separate infra services

---

7. Exam-Oriented Key Points

- DNS is mandatory for AD
- DHCP must be authorized
- SRV records locate DCs
- DHCP uses DORA
- IPAM centralizes management

---

8. Interview Questions & Answers

Q1: Why DNS is critical for Active Directory?

Answer: AD uses DNS to locate domain controllers and services.

Q2: Difference between DHCP reservation and static IP?

Answer: Reservation is DHCP-managed; static IP is manual.

Q3: What is DHCP failover?

Answer: High availability mechanism for DHCP servers.

Q4: What does IPAM manage?

Answer: DNS, DHCP, and IP address lifecycle.

Q5: What record type does AD use heavily?

Answer: SRV records.

---

9. One-Line Viva Summary

DNS resolves names, DHCP assigns IPs, and IPAM centrally manages enterprise network addressing.

SESSION 8 – LOCAL POLICIES & GROUP POLICY (GPO)

(PG Diploma in Computer Science – Windows Server Administration & Security)

---

1. Introduction to Policies in Windows

1.1 What is a Policy?

A **policy** is a **rule or configuration setting** enforced by the operating system to control:

- User behavior
- System security
- Application execution
- Network access

1.2 Purpose of Policies

- Centralized administration
- Security enforcement
- Standardization of systems
- Compliance and auditing
- Reduced manual configuration

1.3 Types of Policies in Windows

Type	Scope
Local Policies	Single computer
Group Policy (GPO)	Domain-wide
Security Policies	Authentication & authorization
Administrative Templates	OS & app behavior

---

2. Local Security Policies

2.1 Definition

Local Policies are policies applied **only to a standalone computer** or **before domain GPOs**.

2.2 Local Policy Components

```
Local Computer
 ├── Account Policies
 ├── Local Policies
 ├── User Rights Assignment
 └── Security Options
```

2.3 Account Policies

Policy	Purpose
Password Policy	Complexity, age
Account Lockout	Brute-force prevention
Kerberos Policy	Ticket lifetime

Common Password Settings

- Minimum length
- Complexity
- History
- Maximum age

2.4 Local Policies

Audit Policy

- Logon events
- Object access
- Policy changes

User Rights Assignment

Right	Example
Log on locally	Desktop access
Shut down system	Power control
Backup files	Backup operators

2.5 Security Options

- Disable guest account
- Rename Administrator account
- SMB signing
- UAC configuration

2.6 Managing Local Policies

- `secpol.msc`
- `gpedit.msc`

Limitations of Local Policies

- No central management
- Manual configuration
- Not scalable
- Overridden by domain GPOs

---

3. Group Policy (GPO)

3.1 Definition

Group Policy is a **centralized management framework** that applies configuration settings to **users and computers** in an Active Directory domain.

3.2 Why Group Policy is Important

- Centralized control
- Security enforcement
- Reduced admin effort
- Compliance management
- Automation

3.3 Group Policy Architecture

```
GPO
 ├── Group Policy Container (AD)
 └── Group Policy Template (SYSVOL)
```

3.4 Group Policy Processing Order (LSDOU)

```
Local
 → Site
   → Domain
     → OU
```

🔑 **Later policies override earlier ones**

3.5 GPO Types

Type	Scope
Local GPO	Single machine

Type	Scope
Domain GPO	Entire domain
OU-linked GPO	Targeted users/computers

---

4. Group Policy Components

4.1 Computer Configuration

Applies during **system startup**

- Security settings
- Firewall
- Software installation

4.2 User Configuration

Applies during **user logon**

- Desktop restrictions
- Control panel settings
- Folder redirection

4.3 Administrative Templates

- Registry-based policies
- `.admx` & `.adml` files
- OS and application behavior

---

5. Implementing Group Policy

5.1 Creating a GPO

1. Open **Group Policy Management Console (GPMC)**
2. Create new GPO
3. Edit settings
4. Link to OU

5.2 Linking & Inheritance

- GPOs are linked to:
  - Sites
  - Domains
  - OUs
- Child OUs inherit parent policies

5.3 Enforced & Block Inheritance

Feature	Effect
Enforced	Cannot be overridden
Block Inheritance	Stops parent GPOs

5.4 Security Filtering

Apply GPO to **specific users or groups**

5.5 WMI Filtering

Apply GPO based on:

- OS version
- RAM
- Architecture

Example:

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.%"
```

6. Group Policy Processing & Refresh

6.1 Refresh Intervals

System	Interval
Workstations	90 min
Domain Controllers	5 min

6.2 Force Update

```
gpupdate /force
```

6.3 Troubleshooting GPO

Tools:

- `gpresult /r`
- `rsop.msc`
- Event Viewer
- GPMC reports

7. Enterprise Real-World Scenarios

Scenario 1: Corporate Desktop Lockdown

- Disable Control Panel
- Enforce password policy
- Block USB storage

Scenario 2: Server Hardening

- Firewall rules
- Disable SMBv1
- Audit policies enabled

Scenario 3: Software Deployment

- MSI deployment via GPO
- Automatic install on startup

---

8. Common GPO Failures & Fixes

Issue	Cause	Fix
GPO not applied	Wrong OU	Relink GPO
Slow login	Large GPO	Optimize
Access denied	Security filtering	Fix permissions
SYSVOL error	Replication issue	DFSR check

---

9. Security Best Practices

- Least privilege
- Separate user & computer GPOs
- Avoid linking GPOs to root domain
- Test GPOs before production
- Use naming standards

---

10. Exam-Oriented Key Points

- LSDOU order
- GPO stored in AD + SYSVOL
- User vs Computer configuration
- Enforced overrides Block
- WMI filtering is evaluated client-side

---

11. Interview Questions & Answers

Q1: What is LSDOU?

Answer: Local, Site, Domain, OU – GPO processing order.

Q2: Difference between enforced and block inheritance?

Answer: Enforced forces GPO; block inheritance blocks parent GPOs.

Q3: How to check applied GPOs?

Answer: `gpresult /r`

Q4: Where are GPOs stored?

Answer: AD database and SYSVOL.

Q5: What is WMI filtering?

Answer: Conditional GPO application based on system properties.

---

12. One-Line Viva Summary

Group Policy enables centralized, secure, and automated configuration management across an Active Directory domain.

SESSION 9 – NETWORK CONNECTIVITY & REMOTE ACCESS SOLUTIONS

(PG Diploma in Computer Science – Windows Server Networking & Secure Access)

---

1. Introduction to Network Connectivity in Windows Server

1.1 Definition

Network connectivity refers to the ability of systems to **communicate securely and reliably** over local and wide area networks using standardized protocols and services.

1.2 Purpose

- Enable client–server communication
- Provide secure remote access
- Support enterprise applications
- Ensure high availability and performance
- Enable hybrid & cloud connectivity

1.3 Types of Network Connectivity

Type	Description
LAN	Local area communication
WAN	Inter-site connectivity
VPN	Secure remote access
DirectAccess	Always-on connectivity

---

2. Network Connectivity Solutions

2.1 Network Components in Windows

Component	Function
NIC	Physical/virtual network interface
TCP/IP Stack	Core communication
DNS	Name resolution
Routing	Packet forwarding
Firewall	Traffic control

2.2 IPv4 & IPv6 Overview (Conceptual)

IPv4	IPv6
32-bit address	128-bit address
Dotted decimal	Hexadecimal
NAT required	No NAT

2.3 Network Profiles

Profile	Usage
Public	Untrusted networks
Private	Internal networks
Domain	AD-based networks

2.4 Windows Firewall with Advanced Security

- Inbound rules
- Outbound rules
- Connection security rules (IPsec)

---

3. Remote Access Solutions

3.1 Definition

Remote Access allows users to **connect to enterprise networks securely** from remote locations.

3.2 Remote Access Services (RRAS)

RRAS Capabilities

- VPN server
- Routing
- NAT
- Dial-up (legacy)

Installing RRAS

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

---

4. Virtual Private Network (VPN)

4.1 VPN Definition

A **VPN** creates a **secure encrypted tunnel** over an untrusted network (Internet).

4.2 VPN Protocols

Protocol	Features
PPTP	Legacy, insecure
L2TP/IPsec	Secure, complex
SSTP	SSL-based
IKEv2	Fast, secure
OpenVPN	Third-party

☑ **Recommended:** IKEv2 / SSTP

4.3 VPN Authentication Methods

- Username/password
- Certificates
- Smart cards
- MFA (NPS + Azure MFA)

4.4 VPN Workflow

```
Client
 → Authentication
 → Tunnel Creation
 → Encryption
 → Network Access
```

4.5 VPN Deployment Scenario

- Work-from-home users
- Secure access to file servers
- Encrypted communication over Internet

---

5. DirectAccess

5.1 Definition

DirectAccess provides **always-on, seamless remote access** without user-initiated VPN connections.

5.2 Key Characteristics

- Automatic connection
- Uses IPv6
- Bi-directional connectivity
- No manual login

5.3 DirectAccess Architecture

```
Client
 → Internet
 → DirectAccess Server
 → Internal Network
```

5.4 Requirements

- Windows Server
- Windows Enterprise client
- IPv6 or transition technologies
- Certificates
- AD infrastructure

5.5 DirectAccess vs VPN

Feature	VPN	DirectAccess
User action	Manual	Automatic
Connectivity	On-demand	Always-on
Complexity	Low	High
Support	Modern	Deprecated

⚠ DirectAccess is being replaced by **Always On VPN**

---

6. Network Policy Server (NPS)

6.1 Definition

NPS is Microsoft's implementation of **RADIUS**.

6.2 Purpose

- Centralized authentication

- Authorization
- Accounting (AAA)

6.3 NPS Components

- Connection request policies
- Network policies
- RADIUS clients

---

7. Authentication & Authorization Workflow

VPN Authentication Flow

```
Client
 → VPN Server
 → NPS
 → Active Directory
 → Access Granted/Denied
```

---

8. Enterprise Real-World Scenarios

Scenario 1: Corporate VPN

- RRAS + IKEv2
- NPS with MFA
- Split tunneling disabled

Scenario 2: Branch Office Connectivity

- Site-to-site VPN
- Centralized authentication
- Encrypted inter-site traffic

Scenario 3: Secure Admin Access

- IPsec rules
- Restricted RDP access
- Firewall hardened

---

9. Common Failures & Troubleshooting

Issue	Cause	Fix
VPN fails	Certificate issue	Renew cert
Authentication denied	NPS misconfig	Fix policy
No internal access	Routing issue	Enable routes
Slow VPN	MTU issue	Adjust MTU

Tools

- Event Viewer
- `rasdial`
- `netsh`
- NPS logs

---

10. Security Best Practices

- Use strong encryption
- Enable MFA
- Restrict admin access
- Monitor logs
- Disable weak protocols

---

11. Exam-Oriented Key Points

- RRAS enables VPN & routing
- IKEv2 is most secure
- NPS provides AAA
- DirectAccess is always-on
- Firewall profiles matter

---

12. Interview Questions & Answers

Q1: Difference between VPN and DirectAccess?

Answer: VPN is user-initiated; DirectAccess is automatic.

Q2: What is RRAS used for?

Answer: VPN, routing, and remote access services.

Q3: Why use NPS?

Answer: Centralized authentication and authorization.

Q4: Which VPN protocol is recommended?

Answer: IKEv2 or SSTP.

Q5: What replaces DirectAccess?

Answer: Always On VPN.

---

13. One-Line Viva Summary

Remote access solutions like VPN and DirectAccess enable secure enterprise connectivity over untrusted networks.

SESSION 10 – INTERNET INFORMATION SERVICES (IIS) WEB SERVER

(PG Diploma in Computer Science – Windows Server Web Infrastructure)

---

1. Introduction to IIS Web Server

1.1 Definition

Internet Information Services (IIS) is Microsoft's **enterprise-grade web server platform** used to host **websites, web applications, APIs, and services** on Windows Server.

1.2 Purpose of IIS

- Host web applications (ASP.NET, PHP, static sites)
- Provide HTTP/HTTPS services
- Integrate with Active Directory
- Support enterprise authentication
- Enable scalable, secure web hosting

1.3 Key Features of IIS

- Modular architecture
- Application pools
- Integrated security
- High performance
- Native Windows integration
- GUI & PowerShell management

---

2. IIS Architecture

2.1 IIS Logical Architecture

```
Client Browser
     |
     v
HTTP.sys (Kernel Mode)
     |
     v
Worker Process (w3wp.exe)
```

```
     |
     v
Web Application
```

2.2 IIS Components

Component	Description
HTTP.sys	Kernel-mode listener
WAS	Windows Process Activation
Worker Process	Handles requests
Application Pool	Isolation boundary
Site	Website container

2.3 Request Processing Flow

```
Client Request
 → HTTP.sys
 → Application Pool
 → w3wp.exe
 → Application Code
 → Response
```

---

3. Installing IIS Web Server

3.1 Installation Methods

GUI Method

- Server Manager → Add Roles
- Select **Web Server (IIS)**

PowerShell Method

```
Install-WindowsFeature Web-Server -IncludeManagementTools
```

3.2 IIS Role Services

Category	Examples
Common HTTP Features	Static content
Application Development	ASP.NET, CGI
Security	SSL, Auth
Performance	Compression
Management	IIS Manager

---

4. IIS Websites & Application Pools

4.1 Website Components

- Site name
- Physical path
- Binding (IP, Port, Hostname)
- Application pool

4.2 Application Pools

Definition

An **application pool** isolates applications using separate **worker processes**.

Benefits

- Fault isolation
- Security isolation
- Performance tuning

App Pool Settings

Setting	Purpose
.NET CLR	Runtime
Identity	Security context

Setting	Purpose
Recycling	Memory management

---

5. IIS Security

5.1 Authentication Methods

Method	Use Case
Anonymous	Public sites
Basic	Legacy
Windows Auth	Intranet
Digest	Domain
Client Certificates	High security

5.2 Authorization

- NTFS permissions
- IIS authorization rules

5.3 SSL/TLS Configuration

```
Client
 → HTTPS
 → SSL Certificate
 → Secure Connection
```

Steps:

1. Obtain certificate
2. Bind HTTPS
3. Enforce SSL

---

6. Managing IIS

6.1 Management Tools

- IIS Manager (GUI)
- PowerShell
- AppCmd
- Web Deploy

PowerShell Examples

```
Get-Website
New-WebSite -Name "CorpSite" -Port 80 -PhysicalPath C:\Web
```

---

7. Logging & Monitoring

7.1 IIS Logs

- Request details
- Status codes
- Client IP
- URL accessed

7.2 Log Location

```
C:\inetpub\logs\LogFiles
```

7.3 Monitoring Tools

- Event Viewer
- Performance Monitor
- Failed Request Tracing

---

8. Performance & Scalability

8.1 Performance Features

- Output caching
- Compression
- Load balancing (ARR)
- Web farms

8.2 Scaling IIS

- Vertical scaling (resources)
- Horizontal scaling (multiple servers)
- Load balancers (NLB, Azure LB)

---

9. Enterprise Real-World Scenarios

Scenario 1: Corporate Intranet

- IIS + Windows Authentication
- AD-integrated access
- HTTPS enforced

Scenario 2: Public Website Hosting

- Anonymous access
- SSL enabled
- Reverse proxy

Scenario 3: Application Hosting

- ASP.NET apps
- Separate app pools
- Load-balanced IIS farm

---

10. Common IIS Failures & Troubleshooting

Issue	Cause	Fix
403 Error	Permission issue	Fix NTFS
404 Error	Wrong path	Verify site
503 Error	App pool stopped	Start pool
SSL error	Cert mismatch	Rebind cert

Tools

- Event Viewer
- IIS logs
- App Pool status

---

11. IIS Security Best Practices

- Use HTTPS only
- Separate app pools
- Least privilege identities
- Disable unused modules
- Regular patching

---

12. Exam-Oriented Key Points

- HTTP.sys works in kernel mode
- Application pools isolate apps
- w3wp.exe handles requests
- IIS integrates with AD
- SSL binds to site bindings

---

13. Interview Questions & Answers

Q1: What is an application pool?

Answer: A container that isolates IIS applications.

Q2: What causes HTTP 503 error?

Answer: Application pool stopped or crashed.

Q3: Difference between IIS and Apache?

Answer: IIS is Windows-native; Apache is cross-platform.

Q4: Where are IIS logs stored?

Answer: `C:\inetpub\logs\LogFiles`

Q5: What is HTTP.sys?

Answer: Kernel-mode driver that handles HTTP requests.

---

14. One-Line Viva Summary

IIS is a secure, scalable Windows-based web server platform for hosting enterprise web applications.

SESSION 11 – CORE & DISTRIBUTED NETWORK SOLUTIONS

IPv4 & IPv6 Addressing and Implementation

(PG Diploma in Computer Science – Enterprise Networking & Windows Server)

---

1. Introduction to Core & Distributed Network Solutions

1.1 Definition

Core and distributed network solutions define how **IP addressing, routing, and communication** are designed and implemented across **enterprise, data center, and distributed environments**.

1.2 Purpose

- Efficient IP address management
- Scalable network design
- Support for cloud and hybrid environments
- High availability and fault tolerance
- Secure data communication

1.3 Network Types

Type	Description
Core Network	Central backbone
Distribution Network	Aggregation layer
Access Network	End-user connectivity

1.4 Three-Tier Network Model

```
      Core Layer
(High-speed routing)
         |
  Distribution Layer
 (Policy & routing)
         |
     Access Layer
 (Clients & servers)
```

---

2. IPv4 Addressing

2.1 IPv4 Definition

IPv4 (Internet Protocol version 4) uses **32-bit addresses** to uniquely identify network interfaces.

Example:
`192.168.10.25`

2.2 IPv4 Address Structure

```
Network Portion | Host Portion
192.168.10.0    | 25
```

2.3 IPv4 Address Classes (Legacy)

Class	Range	Default Mask
A	1.0.0.0 – 126.0.0.0	/8
B	128.0.0.0 – 191.255.0.0	/16
C	192.0.0.0 – 223.255.255.0	/24

⚠ Classful addressing is **obsolete**, replaced by CIDR.

2.4 CIDR (Classless Inter-Domain Routing)

- Uses **prefix length**
- Efficient address utilization
- Supports subnetting & VLSM

Example:

`192.168.1.0/26`

2.5 Private IPv4 Address Ranges

Range	Use
10.0.0.0/8	Large enterprises
172.16.0.0/12	Medium
192.168.0.0/16	Small

2.6 Subnetting Concept

Subnetting divides a network into **smaller logical networks**.

Benefits

- Reduced broadcast traffic
- Improved security
- Efficient IP usage

---

3. IPv6 Addressing

3.1 IPv6 Definition

IPv6 is the next-generation IP protocol using **128-bit addresses**.

Example:

```
2001:db8:acad::1
```

3.2 IPv6 Address Structure

```
| Global Prefix | Subnet ID | Interface ID |
```

3.3 IPv6 Address Types

Type	Purpose
Unicast	One-to-one
Multicast	One-to-many
Anycast	Nearest node

3.4 IPv6 Special Addresses

Address	Meaning
::1	Loopback

Address	Meaning
::	Unspecified
fe80::/10	Link-local

3.5 IPv6 Prefixes

- Typical subnet: `/64`
- Global unicast: `2000::/3`

---

4. IPv4 vs IPv6 Comparison

Feature	IPv4	IPv6
Address size	32-bit	128-bit
NAT	Required	Not required
Broadcast	Supported	Not supported
Security	Optional	Built-in IPsec

---

5. IPv6 Transition Technologies

5.1 Dual Stack

- IPv4 and IPv6 run together
- Preferred method

5.2 Tunneling

- 6to4
- ISATAP
- Teredo

5.3 Translation

- NAT64
- DNS64

---

6. Implementing IPv4 & IPv6 in Windows Server

6.1 Configuring IPv4

```
New-NetIPAddress -InterfaceAlias "Ethernet" `
 -IPAddress 192.168.1.10 -PrefixLength 24 -DefaultGateway 192.168.1.1
```

6.2 Configuring IPv6

```
New-NetIPAddress -InterfaceAlias "Ethernet" `
 -IPAddress 2001:db8::10 -PrefixLength 64
```

6.3 Verifying Configuration

```
ipconfig /all
ping
tracert
```

---

7. Distributed Network Scenarios

Scenario 1: Enterprise Campus

- IPv4 private addressing
- DHCP for clients
- Static IP for servers

Scenario 2: Data Center

- IPv6-enabled infrastructure
- Dual-stack deployment
- Load-balanced services

Scenario 3: Cloud & Hybrid

- IPv6-ready design
- NAT-free connectivity
- Secure routing

---

8. Common Network Issues & Troubleshooting

Issue	Cause	Fix
No connectivity	Wrong IP	Reconfigure
Duplicate IP	Static conflict	DHCP reservation
IPv6 unreachable	Missing route	Check gateway
DNS issues	Wrong IP version	Fix DNS

---

9. Security Best Practices

- Use subnet isolation
- Disable unused protocols
- Secure routing paths
- Monitor IP usage
- Implement firewall rules

---

10. Exam-Oriented Key Points

- IPv4 uses 32-bit addressing
- IPv6 uses 128-bit addressing
- /64 is standard IPv6 subnet
- Dual stack preferred
- No broadcast in IPv6

---

11. Interview Questions & Answers

Q1: Why IPv6 is required?

Answer: IPv4 address exhaustion and better scalability.

Q2: What is Dual Stack?

Answer: Running IPv4 and IPv6 simultaneously.

Q3: What replaces broadcast in IPv6?

Answer: Multicast.

Q4: Is NAT required in IPv6?

Answer: No.

Q5: What is link-local address?

Answer: IPv6 address used within local network only.

---

12. One-Line Viva Summary

IPv4 and IPv6 provide scalable and structured IP addressing for core and distributed enterprise networks.

SESSION 12 – WINDOWS DEPLOYMENT SERVICES (WDS)

(PG Diploma in Computer Science – Windows Server Deployment & Automation)

---

1. Concept of Windows Deployment Services (WDS)

1.1 Definition

Windows Deployment Services (WDS) is a **Microsoft server role** that enables **network-based (PXE) deployment** of Windows operating systems to client computers **without physical media**.

1.2 Purpose of WDS

- Centralized OS deployment
- Rapid mass installation
- Consistent OS configuration
- Reduced manual effort
- Supports enterprise-scale rollout

1.3 Where WDS is Used

- Corporate IT departments
- Educational labs
- Call centers
- Data centers
- Manufacturing floors

1.4 Benefits of WDS

- No USB/DVD required
- Faster deployment
- Standardized images
- Easy OS recovery
- Integrated with Active Directory

---

2. WDS Architecture

2.1 High-Level WDS Architecture

```
PXE Client
   |
   | (DHCP Request)
   v
DHCP Server
   |
   | (IP + Boot Info)
   v
WDS Server
   |
   | (Boot Image)
   v
Windows Setup
   |
   | (Install Image)
   v
Client OS Installed
```

2.2 Core WDS Components

Component	Description
WDS Server	Hosts images
PXE Client	Target machine
DHCP	Assigns IP
Boot Image	Starts installation
Install Image	OS image
AD DS	Authorization & management
TFTP	Transfers boot files

2.3 WDS Server Modes

Mode	Description
Standalone	No AD required
Integrated	AD-based authorization

☑ **Enterprise standard:** AD-integrated WDS

---

3. PXE Boot Process

3.1 What is PXE?

PXE (Preboot Execution Environment) allows a client system to **boot from the network** before any OS is installed.

3.2 PXE Boot Workflow

```
1. Client powers on
2. PXE firmware sends DHCPDISCOVER
3. DHCP assigns IP address
4. WDS responds with boot server info
5. Client downloads boot image (TFTP)
6. Windows Setup starts
```

3.3 DHCP & PXE Interaction

Option	Purpose
60	PXEClient
66	Boot Server Name
67	Boot File Name

⚠ Required only when DHCP & WDS are on **different servers**

---

4. Image Types in WDS

4.1 Boot Images

- Used to **start Windows Setup**
- Based on **WinPE**
- Example: `boot.wim`

4.2 Install Images

- Actual OS image

- Can be **standard or custom**
- Example: `install.wim`

4.3 Image Groups

Logical containers used to:

- Organize images
- Assign permissions
- Simplify management

4.4 Image Types Summary

Image Type	Purpose
Boot Image	Launch setup
Install Image	Install OS
Capture Image	Create custom image
Discover Image	Non-PXE clients

---

5. Deploying Windows 10/11 Using WDS

5.1 Prerequisites

- Windows Server with WDS role
- DHCP server
- DNS configured
- NTFS partition for image storage
- Windows 10/11 ISO

5.2 Installing WDS Role

```
Install-WindowsFeature WDS -IncludeManagementTools
```

5.3 Configuring WDS Server

Configuration Steps

1. Open **WDS Console**
2. Initialize WDS
3. Choose RemoteInstall folder
4. Configure PXE response
5. Authorize WDS in DHCP

5.4 Adding Boot Image

1. Mount Windows ISO
2. Navigate to `sources\boot.wim`
3. Add to **Boot Images**

5.5 Adding Install Image

1. Select `install.wim`
2. Create image group
3. Add OS editions

5.6 Deployment Flow

```
Client PXE Boot
→ Select Boot Image
→ Windows Setup
→ Choose Install Image
→ Disk Partition
→ OS Installation
→ Reboot
```

---

6. Real-World Mass Deployment Scenarios

Scenario 1: College Computer Lab

- 100 PCs
- Single standard Windows 11 image
- PXE boot enabled
- Deployment in 1–2 hours

Scenario 2: Corporate Laptop Rollout

- Windows 10 Enterprise
- Domain join during setup
- Standard apps preinstalled
- Minimal technician involvement

Scenario 3: OS Recovery

- Bare-metal recovery
- Reimage failed systems
- Consistent configuration

---

7. Troubleshooting PXE & WDS Errors

7.1 Common PXE Errors

Error	Cause	Fix
PXE-E51	No DHCP response	Check DHCP
PXE-E53	Boot filename missing	Set option 67
PXE-E32	TFTP timeout	Firewall issue
WDS not responding	Service stopped	Restart WDS

7.2 Troubleshooting Tools

- Event Viewer
- `wdsutil`
- DHCP logs
- Network packet capture

---

8. Security Considerations

- Approve known clients
- Restrict PXE access
- Secure WDS server
- Use separate VLAN for deployment
- Monitor deployment logs

---

9. Best Practices

- Keep boot images updated
- Separate image storage disk
- Use AD-integrated WDS
- Combine WDS with MDT for automation
- Test images before mass deployment

---

10. Exam-Oriented Key Points

- WDS uses PXE & TFTP
- Boot image starts installation
- Install image installs OS
- DHCP required for PXE
- Image groups organize OS images

---

11. Interview Questions & Answers

Q1: What is WDS used for?

Answer: Network-based deployment of Windows OS.

Q2: Difference between boot image and install image?

Answer: Boot image starts setup; install image installs OS.

Q3: What protocol does PXE use?

Answer: DHCP and TFTP.

Q4: Can WDS work without AD?

Answer: Yes, in standalone mode (limited features).

Q5: How to deploy to non-PXE clients?

Answer: Use Discover Image.

---

12. One-Line Viva Summary

Windows Deployment Services enables fast, centralized, network-based deployment of Windows operating systems using PXE.

SESSION 13 & 14 – HYPER-V & SERVER STORAGE

(PG Diploma in Computer Science – Virtualization & Storage Technologies)

---

1. Hyper-V

1.1 Definition

Hyper-V is Microsoft's **Type-1 (bare-metal) hypervisor** that enables **server virtualization**, allowing multiple virtual machines (VMs) to run on a single physical server.

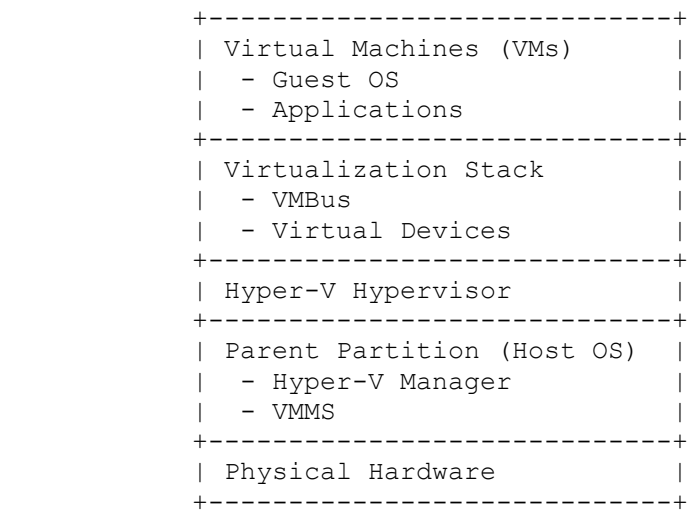
1.2 Purpose of Hyper-V

- Server consolidation
- Resource optimization
- Cost reduction
- High availability & disaster recovery
- Test & development environments
- Cloud & hybrid readiness

1.3 Type-1 vs Type-2 Hypervisor

Feature	Type-1 (Hyper-V)	Type-2
Runs on	Bare metal	Host OS
Performance	High	Lower
Security	Strong	Weaker
Example	Hyper-V, ESXi	VirtualBox

1.4 Hyper-V Architecture



1.5 Key Hyper-V Components

Component	Function
Hypervisor	CPU & memory isolation

Component	Function
Parent Partition	Manages VMs
Child Partition	Guest OS
VMBus	High-speed VM communication
VMMS	VM management service

---

2. Install and Configure Hyper-V

2.1 Hardware Requirements

- 64-bit CPU
- Hardware virtualization (Intel VT-x / AMD-V)
- SLAT support
- Minimum 8 GB RAM (recommended)
- BIOS virtualization enabled

2.2 Installing Hyper-V

GUI Method

- Server Manager → Add Roles
- Select **Hyper-V**

PowerShell Method

```
Install-WindowsFeature Hyper-V -IncludeManagementTools -Restart
```

2.3 Post-Installation Configuration

- Create virtual switches
- Configure default VM paths
- Set resource limits
- Enable Hyper-V Replica (optional)

3. Virtual Networking in Hyper-V

3.1 Virtual Switch Types

Switch	Connectivity
External	VM ↔ LAN
Internal	VM ↔ Host
Private	VM ↔ VM only

3.2 Virtual Networking Architecture

```
VM
 ↓
Virtual NIC
 ↓
Virtual Switch
 ↓
Physical NIC
 ↓
Network
```

3.3 Advanced Networking

- NIC Teaming
- VLAN tagging
- SR-IOV
- QoS policies

4. VM Configuration

4.1 VM Generation Types

Generation	Features
Gen 1	BIOS, legacy support
Gen 2	UEFI, Secure Boot

4.2 VM Resource Configuration

CPU

- vCPU allocation
- Processor compatibility
- NUMA awareness

Memory

Type	Description
Static	Fixed memory
Dynamic	RAM adjusts dynamically

Storage

- Attach VHD/VHDX
- Controller selection (IDE/SCSI)

Networking

- Assign virtual switch
- Configure VLAN
- Enable MAC spoofing (if needed)

---

5. Disks and Volumes

5.1 Disk Types

Disk Type	Description
Basic	Simple volumes
Dynamic	Advanced volumes
GPT	Large disks
MBR	Legacy disks

5.2 Volume Types

Volume	Use Case
Simple	Single disk
Spanned	Capacity
Striped (RAID-0)	Performance
Mirrored (RAID-1)	Redundancy
RAID-5	Balance

5.3 File Systems

File System	Feature
NTFS	Standard
ReFS	Resilience
FAT32	Legacy

---

6. Server Storage

6.1 Server Storage Definition

Server storage refers to **local or network-attached storage systems** used to store OS, applications, and VM data.

6.2 Storage Types

Type	Description
DAS	Direct-attached
NAS	File-based
SAN	Block-based
Storage Spaces	Software-defined

6.3 Storage Spaces

```
Physical Disks
 ↓
Storage Pool
 ↓
Virtual Disk
 ↓
Volume
```

6.4 VHD & VHDX

Feature	VHD	VHDX
Max Size	2 TB	64 TB
Resilience	Low	High
Recommended	❌	☑

---

7. Data Deduplication

7.1 Definition

Data Deduplication reduces storage usage by eliminating **duplicate data blocks**.

7.2 How Deduplication Works

```
Duplicate Files
 → Chunking
 → Hashing
 → Single Instance Storage
```

7.3 Use Cases

- File servers
- VDI environments
- Backup repositories

7.4 Installing Deduplication

```
Install-WindowsFeature FS-Data-Deduplication
```

7.5 Best Practices

- Do not enable on active VM disks
- Schedule optimization jobs
- Monitor CPU usage

---

8. Real-World Virtualization Scenarios

Scenario 1: Server Consolidation

- 10 physical servers → 1 Hyper-V host
- Reduced power & cooling
- Centralized management

Scenario 2: Development Environment

- Multiple OS VMs
- Snapshot/checkpoints
- Isolated testing

Scenario 3: Disaster Recovery

- Hyper-V Replica

- Asynchronous replication
- Fast failover

---

9. Performance Tuning

9.1 CPU Optimization

- Avoid CPU over-commit
- Enable NUMA awareness

9.2 Memory Optimization

- Use Dynamic Memory carefully
- Reserve RAM for host

9.3 Storage Optimization

- Use VHDX
- Use fixed disks for performance
- Enable write-back cache

9.4 Networking Optimization

- NIC teaming
- SR-IOV for high throughput

---

10. Troubleshooting

10.1 Common Hyper-V Issues

Issue	Cause	Fix
VM won’t start	No memory	Increase RAM
Slow VM	Disk I/O	Use fixed VHDX
Network down	Switch misconfig	Reassign switch
Snapshot issues	Disk full	Merge checkpoints

10.2 Troubleshooting Tools

- Hyper-V Manager
- Event Viewer
- Performance Monitor
- PowerShell

---

11. Security Best Practices

- Secure Hyper-V host
- Separate management network
- Use Shielded VMs
- Patch host OS
- Limit admin access

---

12. Exam-Oriented Key Points

- Hyper-V is Type-1 hypervisor
- VHDX preferred over VHD
- External switch connects to LAN
- Gen-2 VMs support Secure Boot
- Deduplication saves disk space

---

13. Interview Questions & Answers

Q1: Difference between Gen-1 and Gen-2 VM?

Answer: Gen-2 supports UEFI, Secure Boot, and faster boot.

Q2: What is VMBus?

Answer: High-speed communication channel between host and VM.

Q3: When should deduplication not be used?

Answer: On active Hyper-V VM disks.

Q4: What is Hyper-V Replica?

Answer: Built-in VM replication for disaster recovery.

Q5: Fixed vs Dynamic VHDX?

Answer: Fixed offers better performance; dynamic saves space.

---

14. One-Line Viva Summary

Hyper-V combined with optimized server storage provides scalable, secure, and high-performance enterprise virtualization.

SESSION 15 – FILE SERVER RESOURCE MANAGER (FSRM)

(PG Diploma in Computer Science – Windows Server File Services & Storage Control)

---

1. Concept of File Server Resource Manager (FSRM)

1.1 Definition

File Server Resource Manager (FSRM) is a **Windows Server role service** that enables administrators to **manage, monitor, and control data stored on file servers**.

It allows control over:

- Disk usage
- File types
- Storage growth
- File server compliance

1.2 Purpose of FSRM

- Prevent disk space exhaustion
- Enforce storage policies
- Block unwanted file types
- Generate storage usage reports
- Improve file server governance

1.3 Why FSRM is Important in Enterprises

- Controls uncontrolled data growth
- Prevents users from storing media/software
- Helps meet compliance & audit requirements
- Improves server performance and availability

---

2. FSRM Architecture

2.1 FSRM Logical Architecture

```
Users / Applications
        |
        v
File Server
  |
  +-- FSRM Engine
       |
       +-- Quota Management
       +-- File Screening
       +-- Storage Reports
```

2.2 Core Components of FSRM

Component	Description
Quota Management	Limits disk usage
File Screening	Controls file types
Storage Reports	Usage analysis
File Management Tasks	Automated actions
Classification	Metadata tagging

---

3. Installing File Server Resource Manager

3.1 Prerequisites

- Windows Server
- NTFS volume
- File Server role installed
- Administrative privileges

3.2 Installation (GUI Method)

1. Open **Server Manager**
2. Add Roles and Features
3. Select **File and Storage Services**
4. Choose **File Server Resource Manager**

3.3 Installation (PowerShell)

```
Install-WindowsFeature FS-Resource-Manager -IncludeManagementTools
```

---

4. Quota Management

4.1 What is a Quota?

A **quota** limits the **amount of disk space** users or folders can consume.

4.2 Types of Quotas

Quota Type	Description
Hard Quota	Enforces limit strictly
Soft Quota	Warning only

4.3 Quota Templates

Predefined quota configurations for:

- Home folders
- Department shares
- Project folders

4.4 Creating a Quota (Step-by-Step)

1. Open **FSRM Console**
2. Quota Management → Quotas
3. Create Quota
4. Select folder path
5. Choose quota template
6. Configure notifications
7. Apply quota

4.5 Quota Notifications

- Email alerts
- Event logs
- Command execution
- Report generation

---

5. File Screening

5.1 What is File Screening?

File screening prevents users from saving **unwanted file types** on file servers.

5.2 File Screen Types

Type	Behavior
Active Screening	Blocks files
Passive Screening	Logs only

5.3 File Screen Templates

Common templates:

- Block Audio & Video
- Block Executables
- Block Archives

5.4 Implementing File Screening (Steps)

1. FSRM → File Screening Management
2. Create File Screen
3. Select path
4. Choose template

5. Configure notifications
6. Apply

---

6. Storage Reporting

6.1 Purpose of Storage Reports

Provides visibility into:

- Disk usage
- Large files
- Duplicate files
- File type distribution
- Old/stale data

6.2 Common Report Types

Report	Use
Duplicate Files	Identify redundancy
Large Files	Find storage hogs
Least Recently Used	Cleanup planning
File Types	Compliance

6.3 Scheduling Reports

- On demand
- Daily / weekly / monthly
- Email delivery

---

7. File Management Tasks

7.1 Definition

Automated tasks based on:

- File age
- Size
- Classification

7.2 Examples

- Move old files to archive
- Delete files older than 5 years
- Notify owners of large files

---

8. Real-World Storage Control Scenarios

Scenario 1: Home Folder Control

- 5 GB hard quota per user
- Email alert at 80%
- Prevent disk exhaustion

Scenario 2: Blocking Media Files

- Block `.mp3`, `.mp4`, `.avi`
- Prevent misuse of corporate storage

Scenario 3: Compliance Reporting

- Monthly file type report
- Identify prohibited file storage

Scenario 4: Archive Old Data

- Move files older than 3 years
- Reduce active storage load

---

9. Troubleshooting FSRM

9.1 Common Issues & Fixes

Issue	Cause	Resolution
Quota not enforced	Soft quota	Use hard quota
Files not blocked	Passive screening	Enable active
Reports missing	Scheduler issue	Check Task Scheduler
Emails not sent	SMTP config	Verify mail settings

9.2 Troubleshooting Tools

- Event Viewer
- FSRM logs
- Task Scheduler
- PowerShell

---

10. Security & Best Practices

- Use hard quotas for enforcement
- Apply quotas at root folders
- Test file screens in passive mode first
- Regularly review reports
- Combine FSRM with NTFS permissions

---

11. Exam-Oriented Key Points

- FSRM manages file server storage

- Hard quota blocks writes
- Active file screening blocks files
- Reports aid compliance
- Templates simplify management

---

12. Interview Questions & Answers

Q1: Difference between hard and soft quota?

Answer: Hard blocks storage; soft only warns.

Q2: Can FSRM block file extensions?

Answer: Yes, using active file screening.

Q3: Does FSRM work on ReFS?

Answer: Limited support; best on NTFS.

Q4: How are FSRM reports delivered?

Answer: On-demand or scheduled via email.

Q5: Can FSRM automate cleanup?

Answer: Yes, using File Management Tasks.

---

13. One-Line Viva Summary

FSRM enables administrators to control, monitor, and optimize file server storage using quotas, file screening, and reporting.

SESSION 16 – NETWORK POLICY SERVER (NPS)

(PG Diploma in Computer Science – Network Security & Authentication Services)

---

1. Concept of Network Policy Server (NPS)

1.1 Definition

Network Policy Server (NPS) is Microsoft's implementation of a **RADIUS (Remote Authentication Dial-In User Service) server** that provides **centralized authentication, authorization, and accounting (AAA)** for network access.

1.2 Purpose of NPS

- Centralized user authentication
- Policy-based authorization
- Secure network access control
- Logging and auditing of access attempts
- Integration with Active Directory, VPN, and Wi-Fi

1.3 Where NPS is Used

- VPN authentication
- Wi-Fi (802.1X) authentication
- Network device authentication (switches, routers)
- Remote access servers (RRAS)
- MFA integration (Azure MFA)

---

2. RADIUS Architecture

2.1 What is RADIUS?

RADIUS is a client/server protocol used to manage **remote user access** to networks using centralized authentication.

2.2 RADIUS Components

Component	Description
RADIUS Client	Device requesting authentication (VPN, AP, switch)
RADIUS Server	NPS server
User Database	Active Directory
Shared Secret	Security key between client & server

2.3 RADIUS Architecture Diagram

```
User / Device
     |
     v
RADIUS Client
(VPN / Wi-Fi AP)
     |
     | Access-Request
     v
NPS (RADIUS Server)
     |
     v
Active Directory
     |
     | Access-Accept / Reject
     v
RADIUS Client
```

2.4 RADIUS Ports

- **UDP 1812** – Authentication
- **UDP 1813** – Accounting

---

3. Authentication & Authorization Flow

3.1 Authentication

Verifies **who the user is**.

Methods:

- Username & password
- Certificates
- Smart cards
- EAP (Extensible Authentication Protocol)

3.2 Authorization

Determines **what the user is allowed to do**.

Based on:

- Group membership
- Time of access
- Device type
- Connection method

3.3 AAA Workflow (End-to-End)

```
User attempts access
 → RADIUS Client
 → NPS Authentication
 → AD Credential Validation
 → Policy Evaluation
 → Access Allowed / Denied
 → Accounting Logged
```

---

4. Installing and Implementing NPS

4.1 Prerequisites

- Windows Server
- Domain-joined system
- Static IP
- Proper DNS resolution
- Administrative privileges

4.2 Install NPS Role

```
Install-WindowsFeature NPAS -IncludeManagementTools
```

4.3 Register NPS in Active Directory

Required to read user account properties

```
netsh nps add registeredserver
```

---

5. Configuring NPS

5.1 RADIUS Clients Configuration

Defines devices that will use NPS.

Steps:

1. Open **NPS Console**
2. RADIUS Clients → New
3. Specify:
    - Name
    - IP address
    - Shared secret

5.2 Connection Request Policies

Determines **how requests are processed**.

Examples:

- Forward to another RADIUS
- Authenticate locally

5.3 Network Policies

Define **who is allowed access** and **under what conditions**.

Policy Conditions

- User groups
- Authentication method
- NAS port type
- Time restrictions

Policy Constraints

- EAP types
- Encryption strength
- Idle timeout

---

6. VPN Integration Scenario

Architecture

```
VPN Client
 → VPN Server (RRAS)
 → NPS
 → Active Directory
```

Use Case

- Remote employees
- Secure access to internal resources
- Centralized policy enforcement

Best Practice

- Use **EAP-MSCHAPv2** or **Certificate-based authentication**
- Integrate **Azure MFA** for strong security

---

7. Wi-Fi (802.1X) Integration Scenario

Architecture

```
Wireless Client
 → Access Point
 → NPS
 → Active Directory
```

Benefits

- User-based authentication
- No shared Wi-Fi passwords
- Dynamic VLAN assignment

Authentication Protocols

- PEAP
- EAP-TLS
- EAP-TTLS

---

8. Real-World Enterprise Scenarios

Scenario 1: Corporate VPN with MFA

- RRAS + NPS
- Azure MFA extension
- AD group-based access

Scenario 2: Secure Enterprise Wi-Fi

- 802.1X Wi-Fi
- NPS authentication
- Role-based access

Scenario 3: Network Device Authentication

- Switches authenticate admins via NPS
- Centralized access control

---

9. Troubleshooting NPS

9.1 Common Issues & Fixes

Issue	Cause	Resolution
Access denied	Policy mismatch	Review conditions
No response	Firewall blocked	Open UDP ports
Authentication failed	Wrong EAP	Fix auth method
Logs missing	Logging disabled	Enable accounting

9.2 Troubleshooting Tools

- Event Viewer (Security & NPS logs)
- NPS log files
- `netsh nps`
- Wireshark (RADIUS packets)

---

10. Security Best Practices

- Use strong shared secrets
- Enable logging & auditing

- Use certificate-based auth
- Apply least privilege
- Integrate MFA
- Secure NPS server

---

11. Exam-Oriented Key Points

- NPS = Microsoft RADIUS
- Provides AAA
- Integrates with AD
- Used for VPN & Wi-Fi
- Uses UDP 1812/1813

---

12. Interview Questions & Answers

Q1: What is NPS?

Answer: Microsoft’s RADIUS server for centralized authentication.

Q2: Difference between authentication and authorization?

Answer: Authentication verifies identity; authorization grants permissions.

Q3: What is RADIUS shared secret?

Answer: A key used to secure communication between client and server.

Q4: Can NPS work with Azure MFA?

Answer: Yes, using NPS extension.

Q5: Which port does RADIUS use?

Answer: UDP 1812 (auth), 1813 (accounting).

---

13. One-Line Viva Summary

Network Policy Server provides centralized, secure authentication and authorization for enterprise network access using RADIUS.

SESSION 17 – HIGH AVAILABILITY & WINDOWS SECURITY

(PG Diploma in Computer Science – Windows Security & HA Infrastructure)

PART A – NETWORK LOAD BALANCING (NLB)

---

1. Concept of Network Load Balancing (NLB)

1.1 Definition

Network Load Balancing (NLB) is a **Windows Server feature** that distributes **client traffic across multiple servers** to provide:

- High availability (HA)
- Scalability
- Fault tolerance

1.2 Purpose of NLB

- Eliminate single point of failure
- Improve application availability
- Distribute workload evenly
- Ensure business continuity

1.3 Typical Use Cases

- IIS web servers
- Application servers
- Remote Desktop Gateway
- VPN services
- Web APIs

---

2. NLB Architecture

2.1 NLB High-Level Architecture

```
Client Requests
       |
       v
Virtual IP (VIP)
       |
+------+------+
|             |
NLB Node 1   NLB Node 2
(Web/App)    (Web/App)
```

2.2 Key NLB Components

Component	Description
Cluster	Group of NLB nodes
Node	Individual server
Virtual IP (VIP)	Cluster IP
Dedicated IP	Node-specific IP
Port Rules	Traffic distribution rules

2.3 NLB Operation Modes

Mode	Description
Unicast	Default, simpler
Multicast	Better switch compatibility
IGMP Multicast	Reduces broadcast traffic

---

3. NLB Traffic Distribution

3.1 Load Distribution Methods

Method	Use Case
Single Host	One active node
Equal	Even traffic
Weighted	Based on node capacity

3.2 Port Rules

Define:

- Port range
- Protocol (TCP/UDP)
- Load distribution
- Affinity (None / Single / Network)

---

4. Implementing Network Load Balancing

4.1 Prerequisites

- Windows Server (Standard/Datacenter)
- Static IP addresses
- Same application installed on all nodes
- No dependency on shared state (unless external)

4.2 NLB Installation

```
Install-WindowsFeature NLB -IncludeManagementTools
```

4.3 NLB Configuration Steps

1. Open **NLB Manager**
2. Create new cluster
3. Add first host
4. Configure cluster IP
5. Configure port rules
6. Add additional nodes

4.4 Real-World NLB Scenario

Corporate IIS Farm

- 3 IIS servers
- NLB with VIP
- Equal load distribution
- HTTPS traffic on port 443

---

5. NLB Troubleshooting

5.1 Common NLB Issues

Issue	Cause	Resolution
Cluster not converging	NIC misconfig	Use single NIC
Traffic not balanced	Wrong port rules	Review rules
Node unreachable	Firewall blocked	Allow NLB traffic
MAC conflicts	Unicast issues	Use multicast

5.2 Troubleshooting Tools

- Event Viewer
- `nlb.exe`
- Network traces
- Ping & port testing

---

6. NLB Best Practices

- Use dedicated NIC
- Avoid mixing NLB with failover clustering
- Use external load balancers for large scale
- Monitor node health
- Secure NLB interfaces

PART B – WINDOWS 10 / 11 SECURITY

---

7. Windows 10/11 Security Architecture

7.1 Core Security Features

Feature	Purpose
Windows Defender	Anti-malware
Firewall	Network protection
BitLocker	Disk encryption
Secure Boot	Boot integrity
Credential Guard	Protect credentials
Device Guard	Application control

7.2 Authentication Security

- Strong passwords

- Windows Hello (biometrics)
- MFA (Azure AD integration)
- Smart cards

7.3 Attack Scenarios on Clients

- Malware infection
- Credential theft
- Ransomware
- Privilege escalation
- Phishing attacks

---

8. Hardening Windows 10/11

8.1 Client Hardening Techniques

- Disable unused services
- Enforce strong password policy
- Enable Defender & Firewall
- Apply security baselines
- Regular patching

8.2 Group Policy-Based Hardening

- Disable USB storage
- Block PowerShell for users
- Enforce BitLocker
- Restrict Control Panel access

PART C – ACTIVE DIRECTORY SECURITY ISSUES

---

9. Common AD Security Threats

9.1 AD Attack Scenarios

Attack	Description
Pass-the-Hash	Credential replay
Pass-the-Ticket	Kerberos abuse
Golden Ticket	Forged Kerberos TGT
Privilege Escalation	Abuse of rights
LDAP Injection	Directory attacks

9.2 AD Vulnerabilities

- Weak admin passwords
- Over-privileged users
- Unpatched DCs
- Insecure delegation
- Legacy protocols (NTLMv1)

---

10. Securing Active Directory

10.1 AD Hardening Techniques

- Tiered admin model
- Separate admin accounts
- Disable NTLM where possible
- Secure LDAP (LDAPS)
- Regular audits

10.2 Protecting Domain Controllers

- Physical security
- Firewall rules
- Patch management
- Antivirus exclusions
- Secure backups

PART D – SECURING WINDOWS SERVICES

---

11. Windows Services Security

11.1 Common Services to Secure

- SMB
- RDP
- IIS
- DNS
- DHCP
- WinRM

11.2 Service Hardening Techniques

Technique	Description
Least privilege	Minimal service rights
Service accounts	Use gMSA
Firewall rules	Restrict ports
Disable legacy services	SMBv1

11.3 RDP Security Best Practices

- Change default port
- Enable NLA

- Use MFA
- Restrict by IP
- Monitor logs

---

12. Security Monitoring & Auditing

- Enable advanced auditing
- Centralized log collection
- SIEM integration
- Regular security reviews

---

13. Real-World Enterprise Scenarios

Scenario 1: HA Web Application

- IIS + NLB
- HTTPS only
- Firewall hardened

Scenario 2: Secure AD Environment

- Two DCs per site
- Tiered admin model
- NTLM disabled

Scenario 3: Secure Endpoints

- BitLocker enforced
- Defender ATP enabled
- USB blocked

---

14. Exam-Oriented Key Points

- NLB provides HA & load distribution
- VIP is shared cluster IP
- Windows Defender is built-in
- AD is high-value attack target
- Least privilege is core security principle

---

15. Interview Questions & Answers

Q1: Difference between NLB and Failover Clustering?

Answer: NLB distributes traffic; failover clustering provides service failover.

Q2: What is a Golden Ticket attack?

Answer: Forging Kerberos TGT to gain unlimited AD access.

Q3: How to secure RDP?

Answer: Enable NLA, MFA, restrict access, monitor logs.

Q4: Why disable SMBv1?

Answer: It is insecure and vulnerable to attacks.

Q5: What is the Tiered Admin Model?

Answer: Separating admin roles to reduce lateral movement.

---

16. One-Line Viva Summary

High availability using NLB and strong Windows & AD security are critical for resilient and secure enterprise infrastructures.

SESSION 18 – MICROSOFT EXCHANGE SERVER

(PG Diploma in Computer Science – Enterprise Messaging & Collaboration)

---

1. Concept of Exchange Server

1.1 Definition

Microsoft Exchange Server is an **enterprise-class messaging and collaboration platform** used to provide:

- Email services
- Calendaring
- Contacts
- Tasks
- Collaboration & compliance

It works tightly with **Active Directory** and supports **Outlook, web, mobile, and API-based access**.

1.2 Purpose of Exchange Server

- Centralized email management
- Secure and reliable mail delivery
- Collaboration across users & teams
- Compliance, auditing, and eDiscovery
- High availability and disaster recovery

1.3 Why Exchange Server in Enterprises

- Control over data (on-premises)
- Integration with AD & Windows security
- Advanced transport rules
- Regulatory compliance
- Hybrid cloud capability (Exchange + Microsoft 365)

1.4 Exchange Deployment Models

Model	Description
On-Premises	Exchange hosted in data center
Hybrid	Exchange + Microsoft 365
Cloud	Exchange Online (M365)

🔑 **Exchange Server knowledge is mandatory even for cloud admins** due to hybrid deployments.

---

2. Exchange Server Architecture

2.1 Logical Architecture (Modern Exchange – 2016/2019)

```
Clients (Outlook / OWA / Mobile)
           |
           v
Client Access Services
(Protocol Handling)
           |
           v
Mailbox Server Role
  - Mailbox Database
  - Transport Services
  - Unified Messaging (legacy)
```

Since Exchange 2016, **only one server role exists: Mailbox Server**

2.2 Exchange Server Components

Component	Function
Client Access Services	Handles client connections
Mailbox Database	Stores mailboxes
Transport Service	Mail routing
Frontend Transport	Receives external mail
Edge Transport (optional)	Perimeter security
Active Directory	Authentication & config

2.3 Exchange & Active Directory Integration

```
Active Directory
 ├── Users
 ├── Groups
 ├── Configuration Partition
 └── Exchange Schema Extensions
```

Exchange depends on AD for:

- User authentication
- Configuration storage
- Permissions
- Recipient management

---

3. Exchange Mail Flow

3.1 What is Mail Flow?

Mail flow is the **path an email follows** from sender to recipient.

3.2 Internal Mail Flow

```
User A
 → Outlook
 → Exchange Transport
```

```
 → Mailbox Database
 → User B
```

3.3 External Mail Flow (Inbound)

```
Internet
 → DNS (MX Record)
 → Exchange Frontend Transport
 → Anti-spam checks
 → Mailbox Transport
 → Mailbox Database
```

3.4 External Mail Flow (Outbound)

```
User
 → Exchange Transport
 → Send Connector
 → Internet (SMTP)
```

3.5 Mail Flow Components

Component	Purpose
Receive Connector	Accepts incoming mail
Send Connector	Sends outgoing mail
Transport Rules	Control mail behavior
Accepted Domains	Email domains handled

---

4. Installing and Implementing Exchange Server

4.1 Pre-Requisites

Infrastructure Requirements

- Windows Server (2019/2022)
- Active Directory domain
- Static IP

- Proper DNS
- Supported .NET Framework
- Valid SSL certificate (recommended)

AD Preparation

Exchange extends AD schema.

```
Setup.exe /PrepareSchema
Setup.exe /PrepareAD
Setup.exe /PrepareDomain
```

4.2 Exchange Installation Steps

High-Level Workflow

```
Prepare Active Directory
 → Install Exchange Role
 → Configure Certificates
 → Configure Mail Flow
 → Create Mailboxes
 → Test Connectivity
```

Installing Exchange

```
Setup.exe /Mode:Install /Role:Mailbox
```

4.3 Post-Installation Configuration

- Configure URLs (OWA, ECP, EWS)
- Assign SSL certificate
- Create send/receive connectors
- Configure accepted domains
- Create mailbox databases

---

5. Exchange Client Access

5.1 Client Access Methods

Client	Protocol
Outlook	MAPI over HTTP
Web	OWA (HTTPS)
Mobile	ActiveSync
SMTP	Mail submission

5.2 Outlook Web App (OWA)

- Browser-based access
- Secure HTTPS
- Feature-rich UI

---

6. Exchange Security & Compliance

6.1 Exchange Security Architecture

Layer	Security
Network	Firewall, TLS
Transport	Anti-spam, anti-malware
Access	Authentication & authorization
Data	Encryption & auditing

6.2 Security Features

- TLS encryption
- Anti-spam filters
- Anti-malware protection
- Role-Based Access Control (RBAC)
- Secure authentication (Kerberos/NTLM)

6.3 Compliance & Governance

- Mailbox auditing
- Litigation hold
- eDiscovery
- Retention policies
- Journaling

---

7. High Availability in Exchange

7.1 Database Availability Group (DAG)

```
Mailbox Server 1
 ↔ Replication ↔
Mailbox Server 2
```

Benefits:

- Automatic failover
- Database replication
- No single point of failure

7.2 Load Balancing

- Client access load balancing
- DNS or hardware load balancers

---

8. Real-World Enterprise Scenarios

Scenario 1: Corporate Email System

- 2 Exchange servers
- DAG enabled
- Load-balanced OWA

- 5,000 users

Scenario 2: Hybrid Exchange

- On-prem Exchange
- Microsoft 365 mailboxes
- Hybrid mail flow
- Centralized identity

Scenario 3: Compliance-Driven Organization

- Retention policies
- Litigation hold
- Auditing enabled

---

9. Troubleshooting Exchange Server

9.1 Common Exchange Issues

Issue	Cause	Resolution
Mail not flowing	Connector issue	Check send/receive connectors
OWA not opening	Cert/URL issue	Fix IIS bindings
Database dismounted	Disk issue	Restore or reseed
Outlook disconnects	Autodiscover	Verify DNS

9.2 Troubleshooting Tools

- Exchange Admin Center (EAC)
- PowerShell (`Get-Mailbox`, `Test-Mailflow`)
- Event Viewer
- Queue Viewer
- Message Tracking Logs

---

10. Best Practices

- Use DAG for HA
- Regular backups
- Patch Exchange regularly
- Secure Exchange with TLS
- Monitor mail queues
- Separate Exchange roles logically

---

11. Exam-Oriented Key Points

- Exchange depends on AD
- Mailbox server role only (2016+)
- DAG provides high availability
- Connectors control mail flow
- RBAC controls admin access

---

12. Interview Questions & Answers

Q1: What is Exchange Server?

Answer: Enterprise messaging platform for email and collaboration.

Q2: What is DAG?

Answer: Database Availability Group for mailbox database replication and failover.

Q3: How does Exchange use Active Directory?

Answer: For authentication, configuration, and recipient management.

Q4: Difference between Send and Receive Connector?

Answer: Receive accepts mail; send delivers mail externally.

Q5: What is Autodiscover?

Answer: Service that automatically configures Outlook clients.

---

13. One-Line Viva Summary

Exchange Server is an enterprise messaging platform that provides secure, reliable, and highly available email services integrated with Active Directory.

SESSION 19 & 20 – WINDOWS POWERSHELL & AUTOMATION

(PG Diploma in Computer Science – Windows Automation & Scripting)

---

1. PowerShell Overview & Architecture

1.1 What is PowerShell?

Windows PowerShell is a **task-based command-line shell and scripting language** built on the **.NET framework**, designed for **system administration and automation**.

Unlike traditional shells, PowerShell works with **objects**, not plain text.

1.2 Purpose of PowerShell

- Automate administrative tasks
- Manage Windows servers & services

- Configure Active Directory, IIS, Hyper-V
- Perform bulk operations
- Enable consistent, repeatable administration

1.3 PowerShell Versions

Version	Description
Windows PowerShell 5.1	Windows-only
PowerShell 7+	Cross-platform (Core)

1.4 PowerShell Architecture

```
User / Script
     |
     v
PowerShell Engine
     |
     v
Cmdlets (C# / .NET)
     |
     v
.NET Framework / Core
     |
     v
Windows OS / APIs
```

1.5 Key Components

Component	Description
Cmdlet	Single-function command
Pipeline	Passes objects
Provider	Access data stores
Module	Collection of cmdlets
Script	Automated task
Function	Reusable code block

---

2. Cmdlets & Pipelines

2.1 Cmdlet Naming Convention

```
Verb-Noun
```

Examples:

```
Get-Service
Start-Process
New-ADUser
Restart-Computer
```

2.2 Common Cmdlet Verbs

Verb	Purpose
Get	Read
Set	Modify
New	Create
Remove	Delete
Start	Start service
Stop	Stop service

2.3 The PowerShell Pipeline

Pipeline (`|`) passes objects, not text

```
Get-Service | Where-Object {$_.Status -eq "Stopped"} | Start-Service
```

Pipeline Flow

```
Cmdlet → Object → Cmdlet → Object → Result
```

2.4 Object-Based Advantage

- No text parsing
- Strong typing
- Rich properties & methods

---

3. Error Handling & Debugging

3.1 Types of Errors

Type	Description
Syntax	Typing mistake
Runtime	Occurs during execution
Logical	Script runs but wrong result

3.2 Error Variables

```
$Error
$?
$LASTEXITCODE
```

3.3 Try / Catch / Finally

```
try {
    Get-Item C:\Data\File.txt -ErrorAction Stop
}
catch {
    Write-Host "Error occurred: $_"
}
finally {
    Write-Host "Execution completed"
}
```

3.4 ErrorAction Parameter

Value	Behavior
SilentlyContinue	Ignore
Continue	Show error
Stop	Terminate

3.5 Debugging Techniques

Breakpoints

```
Set-PSBreakpoint -Line 10 -Script script.ps1
```

Verbose Output

```
Write-Verbose "Processing user"
```

Tracing

```
Set-PSDebug -Trace 1
```

---

4. Windows Administration using PowerShell

4.1 Service Management

```
Get-Service
Start-Service Spooler
Stop-Service Spooler
```

4.2 Process Management

```
Get-Process
Stop-Process -Name notepad
```

4.3 Disk & File Management

```
Get-Volume
New-Item -ItemType Directory C:\Logs
Remove-Item C:\Temp\* -Recurse
```

4.4 User & AD Management

```
New-ADUser -Name "Amit Kumar" -Enabled $true
Get-ADUser -Filter *
Add-ADGroupMember IT_Admins Amit
```

4.5 System Information

```
Get-ComputerInfo
Get-WmiObject Win32_OperatingSystem
```

---

5. Background Jobs & Remote Administration

5.1 Background Jobs

Used for **long-running tasks**.

```
Start-Job -ScriptBlock { Get-EventLog System }
Get-Job
Receive-Job -Id 1
Remove-Job -Id 1
```

5.2 PowerShell Remoting (WinRM)

Enable Remoting

```
Enable-PSRemoting -Force
```

One-Time Remote Command

```
Invoke-Command -ComputerName Server01 -ScriptBlock { Get-Service }
```

Interactive Session

```
Enter-PSSession -ComputerName Server01
```

5.3 Multi-Server Administration

```
Invoke-Command -ComputerName Server01,Server02 -ScriptBlock {
    Restart-Service Spooler
}
```

5.4 Security Considerations

- Kerberos authentication

- HTTPS listeners
- Restricted endpoints
- Least privilege

---

6. Script Reuse & Functions

6.1 Why Use Functions?

- Code reuse
- Modular scripts
- Easier maintenance
- Better testing

6.2 Creating a Function

```
function Get-DiskUsage {
    Get-Volume | Select DriveLetter, SizeRemaining
}
```

6.3 Functions with Parameters

```
function Restart-AppService {
    param (
        [string]$ServiceName
    )
    Restart-Service $ServiceName
}
```

Usage:

```
Restart-AppService -ServiceName Spooler
```

6.4 Script Modules

```
MyModule.psm1
MyModule.psd1
Import-Module MyModule
```

---

7. Real-World Automation Scenarios

Scenario 1: Bulk User Creation

- Read CSV
- Create AD users
- Assign groups

```
Import-Csv users.csv | ForEach-Object {
    New-ADUser -Name $_.Name -SamAccountName $_.Username
}
```

Scenario 2: Server Health Monitoring

- Check disk, CPU, services
- Generate report
- Email admin

Scenario 3: Patch Automation

- Trigger updates
- Restart servers
- Log results

Scenario 4: Cleanup Automation

- Delete temp files
- Archive logs
- Schedule via Task Scheduler

---

8. Security Best Practices

- Use execution policies
- Digitally sign scripts
- Avoid hardcoded passwords
- Use SecureString

- Log script execution

Execution Policies

```
Set-ExecutionPolicy RemoteSigned
```

---

9. Troubleshooting PowerShell Scripts

Issue	Cause	Fix
Script blocked	Execution policy	Change policy
Cmdlet not found	Module missing	Import module
Access denied	Privilege issue	Run as admin
Remote fails	WinRM issue	Enable remoting

---

10. Exam-Oriented Key Points

- PowerShell is object-based
- Cmdlets follow Verb-Noun
- Pipeline passes objects
- Try/Catch handles errors
- Remoting uses WinRM
- Functions enable reuse

---

11. Interview Questions & Answers

Q1: Why PowerShell is better than CMD?

Answer: Object-based output, automation, .NET integration.

Q2: What is the pipeline in PowerShell?

Answer: Mechanism to pass objects between cmdlets.

Q3: Difference between Invoke-Command and Enter-PSSession?

Answer: Invoke runs commands remotely; Enter provides interactive session.

Q4: How do you handle errors in PowerShell?

Answer: Try/Catch, ErrorAction, logging.

Q5: What is a PowerShell module?

Answer: A reusable collection of functions and cmdlets.

---

12. One-Line Viva Summary

PowerShell is a powerful object-oriented automation platform for managing and securing Windows infrastructure at scale.