AWS Cloud Computing Practical Guide

Complete Step-by-Step Solutions for All 13 Labs

Course: Cloud Computing AWS
Type: Practical Lab Guide - Complete Solutions
Total Labs: 13
Format: Step-by-step instructions with commands and screenshots guidance

---

Lab 1: Install and Configure ESXi

What is ESXi?

VMware ESXi is a bare-metal hypervisor that installs directly on physical servers to create and run virtual machines.

Prerequisites

- Physical server with virtualization support (Intel VT-x or AMD-V)
- Minimum 4GB RAM (8GB+ recommended)
- 32GB storage minimum
- Network adapter
- ESXi ISO file downloaded from VMware

Part A: Install ESXi

Step 1: Create Bootable Media

1. Download ESXi ISO from VMware website
2. Use Rufus or similar tool to create bootable USB
3. Boot server from USB

Step 2: Installation Process

1. Press Enter at ESXi boot screen
2. Accept EULA (F11)
3. Select installation disk

4. Select keyboard layout (US Default)
5. Set root password (minimum 8 characters)
6. Press F11 to confirm installation
7. Reboot after completion

Step 3: Initial Configuration

1. After reboot, press F2 at ESXi screen
2. Login with root credentials
3. Navigate to "Configure Management Network"
4. Configure network settings:
    - Set IPv4 Configuration (static or DHCP)
    - Example: IP: 192.168.1.100, Subnet: 255.255.255.0, Gateway: 192.168.1.1
    - Set DNS servers
5. Press ESC to save and exit
6. Restart management network (Y)

Part B: Access ESXi Web Interface

1. From another computer, open browser
2. Navigate to: `https://[ESXi-IP-Address]`
3. Login with root credentials
4. You can now create and manage VMs

Part C: Create Your First VM

1. Click "Virtual Machines" → "Create/Register VM"
2. Select "Create a new virtual machine"
3. Configure:
    - Name: Test-VM
    - Guest OS: Select appropriate OS
    - Storage: Select datastore
    - CPU: 2 cores
    - Memory: 4GB

- Hard disk: 40GB
- Network: VM Network

4. Mount ISO file for OS installation
5. Power on VM and complete OS installation

Lab 2: Configure CDP, NAT-PAT in SOHO and Enterprise

A. Cisco Discovery Protocol (CDP)

What is CDP? CDP is a Cisco proprietary protocol that discovers information about directly connected Cisco devices.

Configuration Steps (Cisco Router/Switch):

```
! Enable CDP globally (usually enabled by default)
Router> enable
Router# configure terminal
Router(config)# cdp run

! Enable CDP on specific interface
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# cdp enable
Router(config-if)# exit

! Verify CDP
Router# show cdp neighbors
Router# show cdp neighbors detail

! Configure CDP timers
Router(config)# cdp timer 60        ! Send CDP packets every 60 seconds
Router(config)# cdp holdtime 180    ! Hold information for 180 seconds

! Disable CDP (security consideration)
Router(config)# no cdp run          ! Globally
Router(config-if)# no cdp enable    ! Per interface
```

B. NAT Configuration (Network Address Translation)

Static NAT (One-to-One Mapping):

```
! Configure inside and outside interfaces
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip address 203.0.113.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

! Create static NAT mapping
Router(config)# ip nat inside source static 192.168.1.10 203.0.113.10

! Verify
Router# show ip nat translations
Router# show ip nat statistics
```

Dynamic NAT (Pool-Based):

```
! Define inside network
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

! Define NAT pool
Router(config)# ip nat pool PUBLIC_POOL 203.0.113.10 203.0.113.20 netmask 255.255.255.0

! Map ACL to pool
Router(config)# ip nat inside source list 1 pool PUBLIC_POOL

! Configure interfaces
Router(config)# interface g0/0
Router(config-if)# ip nat inside
Router(config)# interface g0/1
Router(config-if)# ip nat outside
```

C. PAT Configuration (Port Address Translation / NAT Overload)

PAT with Interface Overload (SOHO Setup):

```
! Define inside network
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

! Configure PAT using interface
Router(config)# ip nat inside source list 1 interface gigabitEthernet 0/1 overload

! Configure inside interface
Router(config)# interface g0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit

! Configure outside interface
Router(config)# interface g0/1
Router(config-if)# ip address dhcp
Router(config-if)# ip nat outside
Router(config-if)# exit

! Verify
Router# show ip nat translations
Router# debug ip nat
```

PAT with Pool (Enterprise Setup):

```
! Define ACL
Router(config)# access-list 10 permit 10.0.0.0 0.255.255.255

! Create NAT pool
Router(config)# ip nat pool ENTERPRISE_PAT 203.0.113.1 203.0.113.5 netmask 255.255.255.248

! Enable PAT
Router(config)# ip nat inside source list 10 pool ENTERPRISE_PAT overload

! Configure interfaces
Router(config)# interface range g0/0-2
Router(config-if-range)# ip nat inside
Router(config)# interface g0/3
Router(config-if)# ip nat outside
```

Lab 3: AWS Managerial Tools & Disaster Management Policies

A. AWS CloudWatch (Monitoring)

Step 1: Access CloudWatch

1. Login to AWS Console
2. Navigate to CloudWatch service

Step 2: Create Dashboard

1. Click "Dashboards" → "Create dashboard"
2. Name: Production-Monitoring
3. Add widgets:
    - Line graph for EC2 CPU utilization
    - Number widget for billing
    - Log widget for application logs

Step 3: Set Up Alarms

1. Click "Alarms" → "Create alarm"
2. Select metric (e.g., EC2 > Per-Instance Metrics > CPUUtilization)
3. Conditions: Greater than 80%
4. Period: 5 minutes
5. Actions: Send notification to SNS topic
6. Create SNS topic: High-CPU-Alert
7. Add email subscription
8. Name alarm: High-CPU-Usage

Step 4: Create Billing Alarm

1. Region: Switch to US East (N. Virginia)
2. CloudWatch → Billing → Total Estimated Charge
3. Threshold: > $50
4. Action: Email notification

B. AWS CloudTrail (Auditing)

Configuration Steps:

Step 1: Create Trail

1. Services → CloudTrail
2. Trails → Create trail
3. Trail name: Organization-Audit-Trail
4. Storage location: Create new S3 bucket
5. Bucket name: company-cloudtrail-logs-2024
6. Log file validation: Enabled
7. SNS notification: Optional
8. CloudWatch Logs: Enable
9. Tags: Environment: Production

Step 2: Configure Events

1. Management events: Read/Write
2. Data events: S3, Lambda (optional)
3. Insights events: Enable

Step 3: View Events

1. Event history → Filter by:
    - Event name
    - User name
    - Resource type
    - Time range
2. Example: Find all DeleteBucket API calls

C. AWS Backup (Disaster Recovery)

Step 1: Create Backup Vault

1. AWS Backup → Backup vaults → Create vault
2. Name: Production-Backup-Vault

3. Encryption: Use AWS managed key or custom KMS key
4. Add tags

Step 2: Create Backup Plan

1. Backup plans → Create plan
2. Start with template: Daily-Monthly-1yr-Retention
3. Plan name: Production-Backup-Plan

Backup rule configuration:

- Rule name: Daily-Backups
- Frequency: Daily
- Backup window: 1:00 AM - 3:00 AM
- Retention: 35 days
- Vault: Production-Backup-Vault
- Copy to region: Yes (different region for DR)
- Lifecycle to cold storage: After 7 days

Step 3: Assign Resources

1. Resource assignment → Assign resources
2. Assignment name: Production-Resources
3. IAM role: Default or create new
4. Resource selection:
    - By tags: Environment=Production
    - Or specific resources: Select EC2, RDS, EFS

Step 4: Test Restore

1. Backup vaults → Select vault
2. Recovery points → Choose backup
3. Restore → Configure:
    - Instance type

- Subnet
- Security groups

4. Start restore job
5. Verify restored resource

D. Disaster Recovery Plan

Multi-Region DR Setup:

1. Cross-Region Replication

```
Primary Region: us-east-1
DR Region: us-west-2

S3 Replication:
- Source bucket: Create in us-east-1
- Enable versioning
- Create replication rule:
  • Destination: New bucket in us-west-2
  • IAM role: Auto-create
  • Objects: All
  • Storage class: Same as source

RDS Cross-Region:
- RDS → Select database
- Actions → Create read replica
- Destination region: us-west-2
- Instance specifications: Match production
```

2. Route 53 Failover

1. Route 53 → Hosted zones
2. Create record:
   - Name: www.example.com
   - Type: A record
   - Routing policy: Failover
   - Primary record: us-east-1 load balancer
   - Secondary record: us-west-2 load balancer
   - Health check: Create for primary

- Protocol: HTTPS
- Port: 443
- Path: /health

Lab 4: AWS Storage Management, Basic Security & Create VPC with Database Management

A. S3 Storage Management

Step 1: Create and Configure S3 Bucket

1. Navigate to S3 console
2. Create bucket:
    - Name: my-company-data-2024 (globally unique)
    - Region: us-east-1
    - Block all public access: Enabled
    - Versioning: Enable
    - Tags: Project=DataStorage
    - Encryption: Enable (SSE-S3)
3. Configure lifecycle rules:
    - Management → Lifecycle rules → Create rule
    - Rule name: Archival-Policy
    - Scope: All objects
    - Actions:
        - Transition to S3 Standard-IA after 30 days
        - Transition to Glacier after 90 days
        - Delete after 365 days

Step 2: S3 Security Configuration Bucket Policy Example:

```
json
```

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AllowAppAccess",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/AppRole"
   },
   "Action": [
    "s3:GetObject",
    "s3:PutObject"
   ],
   "Resource": "arn:aws:s3:::my-company-data-2024/*"
  }
 ]
}
```

Apply policy:

- Bucket → Permissions → Bucket policy
- Paste JSON → Save

B. EBS Management

Create and Attach EBS Volume:

1. EC2 → Elastic Block Store → Volumes
2. Create volume:
    - Type: gp3 (General Purpose SSD)
    - Size: 100 GiB
    - IOPS: 3000
    - Throughput: 125 MB/s
    - Availability Zone: Same as EC2 instance
    - Encryption: Enable
    - Snapshot: None (or select existing)
3. Attach to instance:
    - Select volume → Actions → Attach volume

- Instance: Select target EC2
- Device: /dev/sdf

4. On EC2 instance (Linux):

```
bash

sudo lsblk                    # List block devices
sudo mkfs -t ext4 /dev/xvdf   # Format volume
sudo mkdir /data              # Create mount point
sudo mount /dev/xvdf /data    # Mount volume

# Make permanent:
sudo blkid /dev/xvdf          # Get UUID
sudo nano /etc/fstab
# Add: UUID=xxx /data ext4 defaults 0 2
```

C. Create VPC with Database

Complete VPC Setup:

Step 1: Create VPC

1. VPC Dashboard → Your VPCs → Create VPC
    - Name: Production-VPC
    - IPv4 CIDR: 10.0.0.0/16
    - IPv6: No IPv6 CIDR block
    - Tenancy: Default
    - Tags: Environment=Production

Step 2: Create Subnets Create 4 subnets (2 public, 2 private in different AZs):

Public Subnet 1:

- VPC: Production-VPC
- Name: Public-Subnet-1A
- AZ: us-east-1a
- CIDR: 10.0.1.0/24

Public Subnet 2:

- Name: Public-Subnet-1B
- AZ: us-east-1b
- CIDR: 10.0.2.0/24

Private Subnet 1:

- Name: Private-Subnet-1A
- AZ: us-east-1a
- CIDR: 10.0.11.0/24

Private Subnet 2:

- Name: Private-Subnet-1B
- AZ: us-east-1b
- CIDR: 10.0.12.0/24

Step 3: Internet Gateway

1. Internet Gateways → Create IGW
    - Name: Production-IGW
2. Actions → Attach to VPC → Select Production-VPC

Step 4: NAT Gateway

1. NAT Gateways → Create NAT gateway
    - Name: Production-NAT
    - Subnet: Public-Subnet-1A
    - Elastic IP: Allocate new

Step 5: Route Tables

Public Route Table:

1. Create route table:
    - Name: Public-RT
    - VPC: Production-VPC
2. Add routes:

- Destination: 0.0.0.0/0
- Target: Production-IGW

3. Associate subnets:
    - Public-Subnet-1A
    - Public-Subnet-1B

Private Route Table:

1. Create route table:
    - Name: Private-RT
2. Add routes:
    - Destination: 0.0.0.0/0
    - Target: Production-NAT
3. Associate subnets:
    - Private-Subnet-1A
    - Private-Subnet-1B

Step 6: Security Groups

Web Server Security Group:

- Name: WebServer-SG
- Inbound rules:
    - HTTP (80) from 0.0.0.0/0
    - HTTPS (443) from 0.0.0.0/0
    - SSH (22) from Your-IP/32
- Outbound: All traffic

Database Security Group:

- Name: Database-SG
- Inbound rules:
    - MySQL (3306) from WebServer-SG
    - PostgreSQL (5432) from WebServer-SG

- Outbound: None needed

Step 7: Deploy RDS Database

1. RDS → Create database
2. Configuration:
    - Engine: MySQL / PostgreSQL
    - Version: Latest
    - Template: Production
    - DB identifier: production-db
    - Master username: admin
    - Password: [Strong password]
    - Instance class: db.t3.medium
    - Storage: 100 GB gp3
    - VPC: Production-VPC
    - Subnet group: Create new
        - Name: db-subnet-group
        - Subnets: Private-Subnet-1A, Private-Subnet-1B
    - Public access: No
    - Security group: Database-SG
    - Initial database: myapp
    - Backup retention: 7 days
    - Encryption: Enable
    - Monitoring: Enhanced monitoring

Step 8: Launch EC2 in Public Subnet

1. EC2 → Launch instance
    - AMI: Amazon Linux 2
    - Instance type: t2.micro
    - Network: Production-VPC
    - Subnet: Public-Subnet-1A
    - Auto-assign public IP: Enable

- Security group: WebServer-SG
- Key pair: Create/select key

2. User data (install web server):

```bash
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Web Server in Production VPC</h1>" > /var/www/html/index.html
```

Step 9: Test Connectivity

1. SSH to EC2:

```bash
ssh -i keypair.pem ec2-user@[public-ip]
```

2. Test database connection:

```bash
mysql -h [rds-endpoint] -u admin -p
```

3. Test internet from private subnet (should work through NAT Gateway)

Lab 5: Plan and Design File Server and Distribution File Server

Windows Server File Server Setup

Step 1: Install File Server Role

1. Server Manager → Add Roles and Features
2. Installation Type: Role-based
3. Server: Select local server

4. Server Roles: Check "File and Storage Services"
    - Expand and select:
        - File Server
        - File Server Resource Manager
        - DFS Namespaces
        - DFS Replication
5. Complete installation

Step 2: Create Shared Folders

1. Server Manager → File and Storage Services → Shares
2. New Share Wizard:
    - Profile: SMB Share - Quick
    - Location: C:\Shares
    - Share name: CompanyDocs
    - Settings:
        - Enable access-based enumeration
        - Enable continuous availability (optional)
    - Permissions:
        - Administrators: Full Control
        - Domain Users: Read/Write
        - Everyone: Remove
3. Create share

Step 3: Configure NTFS Permissions

1. Navigate to C:\Shares\CompanyDocs
2. Right-click → Properties → Security
3. Configure permissions:
    - Administrators: Full Control
    - Accounting_Group: Modify
    - HR_Group: Read & Execute

- Remove inheritance if needed

4. Advanced → Disable inheritance → Convert

Step 4: DFS Setup (Distributed File System)

1. Server Manager → Tools → DFS Management
2. New Namespace:
    - Namespace server: YourServer
    - Name: CompanyFiles
    - Type: Domain-based
    - Path: \domain.com\CompanyFiles
3. Add folders:
    - New Folder → Name: Documents
    - Add folder target: \Server1\CompanyDocs
    - Add folder target: \Server2\CompanyDocs (for replication)
4. Configure replication:
    - Right-click folder → Replicate Folder
    - Replication group: CompanyDocs-RG
    - Members: Server1, Server2
    - Topology: Full mesh
    - Schedule: Continuously

Step 5: File Server Resource Manager

1. Server Manager → Tools → File Server Resource Manager
2. Create quota:
    - Quota Templates → Create Quota
    - Path: C:\Shares\CompanyDocs\Users
    - Template: 200 GB Limit
    - Auto apply: Yes
3. Create file screen:
    - File Screening → Create File Screen
    - Path: C:\Shares\CompanyDocs

- Template: Block Audio and Video Files
- Active screening (blocks saves)

4. Storage reports:
    - Storage Reports Management → Schedule New Report
    - Reports: Large Files, Quota Usage
    - Schedule: Weekly
    - Delivery: Email to admin

Lab 6: Perform LAN LAB

Complete LAN Setup (Two PCs)

Physical Setup: Equipment needed:

- 2 PCs (PC-A and PC-B)
- 1 Switch or crossover cable
- 2 Ethernet cables (if using switch)

Part A: Configure IP Addresses

PC-A Configuration (Windows):

1. Control Panel → Network and Sharing Center
2. Change adapter settings
3. Right-click Ethernet → Properties
4. Select Internet Protocol Version 4 (TCP/IPv4)
5. Configure:
    - IP address: 192.168.1.10
    - Subnet mask: 255.255.255.0
    - Default gateway: (leave blank for direct connection)
    - Preferred DNS: (leave blank)
6. Click OK

PC-B Configuration: Same steps but:

- IP address: 192.168.1.20
- Subnet mask: 255.255.255.0

Linux Configuration (if using Linux):

```
bash

PC-A:
sudo ip addr add 192.168.1.10/24 dev eth0
sudo ip link set eth0 up

PC-B:
sudo ip addr add 192.168.1.20/24 dev eth0
sudo ip link set eth0 up
```

Part B: Create Shared Folder

On PC-A (Windows):

1. Create folder: C:\SharedFolder
2. Right-click → Properties → Sharing tab
3. Advanced Sharing:
    - Check "Share this folder"
    - Share name: SharedData
    - Permissions:
        - Everyone: Full Control (for lab only)
        - In production: Specific users/groups only
4. Click OK
5. Security tab:
    - Edit permissions
    - Add: Everyone (for lab)
    - Allow: Full Control
    - Apply

On PC-B (Create shared folder too):

1. Create folder: C:\SharedFolder
2. Share with same settings
3. Share name: PC-B-Share

Part C: Test Connectivity

From PC-A:

1. Open Command Prompt
2. Ping PC-B:

```
ping 192.168.1.20

Expected output:
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
```

3. Access shared folder:
    - Open File Explorer
    - Address bar: \192.168.1.20\PC-B-Share
    - Or: \PC-B\PC-B-Share (if name resolution works)
4. Map network drive:
    - Right-click "This PC" → Map network drive
    - Drive: Z:
    - Folder: \192.168.1.20\PC-B-Share
    - Check: Reconnect at sign-in
    - Finish

From PC-B:

1. Ping PC-A:

```bash
ping 192.168.1.10
```

2. Access PC-A's shared folder:

```
\\192.168.1.10\SharedData
```

3. Test file operations:
    - Create a text file in shared folder
    - Verify it appears on host computer

Part D: Troubleshooting

If ping fails:

1. Check firewall: Windows Defender Firewall → Advanced Settings
    - Inbound Rules → Enable:
        - File and Printer Sharing (Echo Request - ICMPv4-In)
2. Verify IP configuration:

```
bash

ipconfig /all
```

3. Check cable connection:
    - LED lights on network ports should be on
4. Verify subnet:
    - Both PCs must be on same subnet (192.168.1.0/24)

If shared folder not accessible:

1. Enable network discovery: Control Panel → Network and Sharing Center → Advanced sharing settings
    - Turn on network discovery
    - Turn on file and printer sharing
2. Check services: services.msc
    - Function Discovery Provider Host: Running
    - Function Discovery Resource Publication: Running

- Server: Running

3. Temporarily disable firewall to test:
    - If it works, create firewall exception

Lab 7: Plan, Design and Configure Domain Controller & Additional Domain Controller

Active Directory Domain Services Setup

Prerequisites:

- Windows Server 2019/2022
- Static IP address: 192.168.1.10
- Server name: DC01
- Minimum 2GB RAM, 40GB disk

Part A: Install Domain Controller

Step 1: Configure Static IP

1. Server Manager → Local Server
2. Click on IPv4 address assigned by DHCP
3. Configure:
    - IP: 192.168.1.10
    - Subnet: 255.255.255.0
    - Gateway: 192.168.1.1
    - DNS: 127.0.0.1 (itself after DC role)

Step 2: Install AD DS Role

1. Server Manager → Add Roles and Features
2. Installation Type: Role-based
3. Server: Select DC01
4. Server Roles: Active Directory Domain Services
5. Add Features (include management tools)

6. Install (don't check restart automatically yet)
7. Wait for installation to complete

Step 3: Promote to Domain Controller

1. Server Manager → Flag icon → Promote this server to domain controller
2. Deployment Configuration:
    - Select: Add a new forest
    - Root domain name: company.local
    - Click Next
3. Domain Controller Options:
    - Forest/Domain functional level: Windows Server 2016
    - Check: Domain Name System (DNS) server
    - Check: Global Catalog (GC)
    - Directory Services Restore Mode (DSRM) password: [Strong password]
    - Click Next
4. DNS Options:
    - Warning about delegation: Click Next (ignore)
5. Additional Options:
    - NetBIOS name: COMPANY (auto-filled)
6. Paths (use defaults):
    - Database: C:\Windows\NTDS
    - Log files: C:\Windows\NTDS
    - SYSVOL: C:\Windows\SYSVOL
7. Review Options → Install
8. Server will automatically restart

Step 4: Post-Installation Verification

1. Login: COMPANY\Administrator
2. Server Manager → Tools → Active Directory Users and Computers
3. Expand company.local

4. Verify default containers:
    - Computers
    - Users
    - Domain Controllers
5. Verify DNS:
    - Tools → DNS
    - Expand DC01 → Forward Lookup Zones → company.local
    - Should see DC01 A record
6. Command line verification:

```bash
dcdiag                  # Domain controller diagnostic
repadmin /showrepl      # Replication status
netdom query fsmo       # Show FSMO role holders
nslookup company.local  # DNS resolution test
```

Part B: Create Organizational Units (OUs)

1. Active Directory Users and Computers
2. Right-click company.local → New → Organizational Unit
3. Create structure:

```
company.local
├── Departments
│   ├── IT
│   ├── HR
│   ├── Finance
│   └── Sales
├── Servers
└── Workstations
```

4. For each OU:
    - Right-click company.local → New → OU
    - Name: IT (uncheck "Protect from deletion" for lab)
    - OK

Part C: Create Users and Groups

Create Users:

1. Navigate to IT OU
2. Right-click IT → New → User
3. User details:
    - First name: John
    - Last name: Smith
    - User logon name: jsmith
    - Click Next
    - Password: P@ssw0rd123
    - Uncheck: User must change password
    - Check: Password never expires (lab only)
    - Click Next → Finish
4. Create additional users:
    - In HR OU: jdoe (Jane Doe)
    - In Finance OU: bwilson (Bob Wilson)
    - In Sales OU: alee (Alice Lee)

Create Security Groups:

1. Right-click IT OU → New → Group
2. Group details:
    - Group name: IT_Admins
    - Group scope: Global
    - Group type: Security
    - OK
3. Add members:
    - Right-click IT_Admins → Properties
    - Members tab → Add
    - Enter: jsmith

- Check Names → OK

4. Create additional groups:
    - HR_Users (in HR OU)
    - Finance_Users (in Finance OU)
    - Sales_Users (in Sales OU)

Part D: Additional Domain Controller (ADC)

Install Second DC:

1. Prepare second server:
    - Windows Server 2019/2022
    - Name: DC02
    - Static IP: 192.168.1.11
    - DNS: 192.168.1.10 (point to first DC)
2. Install AD DS role (same as Part A)
3. Promote to Domain Controller:
    - Deployment: Add domain controller to existing domain
    - Domain: company.local
    - Credentials: COMPANY\Administrator
    - Domain Controller Options:
        - DNS server: Checked
        - Global Catalog: Checked
        - Read-only: Unchecked
    - Install
4. Verify replication:

```
bash

On DC01 or DC02:
repadmin /replsummary
repadmin /showrepl

Should show successful replication between DC01 and DC02
```

Lab 8: Plan and Configure Group Policy Object (GPO)

Complete GPO Configuration Guide

Part A: Create Basic GPO

Step 1: Open Group Policy Management

1. Server Manager → Tools → Group Policy Management
2. Expand Forest → Domains → company.local
3. View existing GPOs under Group Policy Objects

Step 2: Create New GPO

1. Right-click Group Policy Objects → New
2. Name: Desktop Security Policy
3. Source Starter GPO: (none)
4. OK

Part B: Configure Common Policies

Password Policy:

1. Right-click "Desktop Security Policy" → Edit
2. Navigate to: Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy
3. Configure:
    - Minimum password length: 8 characters (Enabled)
    - Password must meet complexity: Enabled
    - Maximum password age: 90 days
    - Minimum password age: 1 day
    - Enforce password history: 5 passwords
    - Store passwords using reversible encryption: Disabled
4. Account Lockout Policy: → Account Policies → Account Lockout Policy
    - Account lockout threshold: 5 invalid attempts

- Account lockout duration: 30 minutes
- Reset account lockout counter after: 30 minutes

Desktop Restrictions: Navigate to: User Configuration → Policies → Administrative Templates → Control Panel

Configure:

- Prohibit access to Control Panel: Enabled
- Settings Page Visibility: hide:display;network;personalization

→ System

- Prevent access to command prompt: Enabled
- Prevent access to registry editing tools: Enabled
- Remove Task Manager: Enabled (use carefully)

→ Desktop

- Remove Recycle Bin icon: Enabled (optional)
- Prohibit user from changing desktop background: Enabled

Software Installation:

1. Download MSI package (e.g., 7-Zip)
2. Place in shared folder: \DC01\Software
3. GPO Editor: Computer Configuration → Policies → Software Settings → Software Installation
4. Right-click → New → Package
5. Path: \DC01\Software\7z1900-x64.msi
6. Deployment method: Assigned
7. OK

Software will install automatically on computer startup

Mapped Drives: User Configuration → Preferences → Windows Settings → Drive Maps

1. Right-click → New → Mapped Drive
2. General tab:

- Action: Create
- Location: \DC01\SharedData
- Label as: Company Data
- Drive letter: Z:
- Reconnect: Checked

3. Common tab:
    - Run in logged-on user's security context: Checked
4. Apply → OK

Folder Redirection: User Configuration → Policies → Windows Settings → Folder Redirection

1. Right-click Documents → Properties
2. Setting: Basic
3. Target folder location: Create folder for each user
4. Root Path: \DC01\UserData%USERNAME%\Documents
5. Settings tab:
    - Grant exclusive rights: Checked
    - Move contents: Checked
6. Apply → OK

Repeat for:

- Desktop
- Pictures
- Music

Part C: Link GPO to OU

Link to Specific OU:

1. Group Policy Management console
2. Navigate to desired OU (e.g., IT)
3. Right-click IT OU → Link an Existing GPO
4. Select "Desktop Security Policy"

5. OK

GPO order (processed bottom to top):

- Default Domain Policy
- Desktop Security Policy

Link to Entire Domain:

1. Right-click company.local → Link an Existing GPO
2. Select desired GPO
3. This applies to all users/computers in domain

Part D: Security Filtering

Apply GPO to Specific Group:

1. Group Policy Management → Select GPO
2. Scope tab → Security Filtering section
3. Remove: Authenticated Users
4. Add → Enter: IT_Admins
5. OK

Now GPO only applies to IT_Admins group members

Part E: Test and Troubleshoot GPO

Force GPO Update:

```
bash

On client computer:
gpupdate /force              # Apply all policies
gpupdate /target:computer    # Computer policies only
gpupdate /target:user        # User policies only

Note: Some policies require logoff/restart
```

View Applied Policies:

```
bash
```

```
gpresult /r                  # Summary report
gpresult /h report.html      # Detailed HTML report
gpresult /scope:computer /v  # Computer policies verbose
gpresult /scope:user /v      # User policies verbose

Review in Group Policy Management:
- Right-click OU → Group Policy Results
- Run wizard to see what applied to specific user/computer
```

Common Troubleshooting:

1. Check GPO link is enabled:
    - Link should not have X icon
    - Right-click link → Link Enabled (checked)
2. Check enforcement:
    - Right-click link → Enforced
    - Enforced GPOs cannot be blocked
3. Verify permissions:
    - GPO → Delegation tab
    - Group must have Read and Apply permissions
4. Check WMI filtering:
    - Scope tab → WMI Filtering
    - (none) means applies to all
5. Event Viewer logs:
    - Applications and Services Logs
    - Microsoft → Windows → GroupPolicy → Operational

Lab 9: Install and Configure Packet Tracer, GNS3 & VMware Environment

A. Install Packet Tracer

System Requirements:

- OS: Windows 10/11, Linux, macOS

- RAM: 4GB minimum (8GB recommended)
- Disk: 2GB free space
- Display: 1024x768 minimum

Installation Steps (Windows):

1. Download:
    - Go to netacad.com
    - Login/create Cisco Networking Academy account
    - Download Packet Tracer (latest version)
2. Install:
    - Run PacketTracer_xxx_windows_64bit.exe
    - Accept license agreement
    - Choose installation directory
    - Create desktop shortcut: Yes
    - Install
3. First Launch:
    - Open Packet Tracer
    - Login with Cisco NetAcad credentials
    - Accept multi-user setup (optional)
4. Basic Interface:
    - Bottom left: Device types (Routers, Switches, End Devices)
    - Bottom right: Connections (copper, fiber, wireless)
    - Workspace: Drag and drop devices

Quick Test:

1. Add devices:
    - 2 PCs from End Devices
    - 1 Switch from Network Devices
2. Connect:
    - Select copper straight-through cable

- Click PC → FastEthernet0
- Click Switch → FastEthernet0/1
- Repeat for second PC to FastEthernet0/2

3. Configure:
    - Click PC0 → Desktop → IP Configuration
    - IP: 192.168.1.10
    - Subnet: 255.255.255.0
    - Repeat for PC1: 192.168.1.11
4. Test:
    - PC0 → Desktop → Command Prompt
    - Type: ping 192.168.1.11
    - Should see replies

B. Install GNS3

System Requirements:

- OS: Windows 10/11, Linux, macOS
- RAM: 8GB minimum (16GB+ recommended)
- CPU: Virtualization support (VT-x/AMD-V)
- Disk: 1GB for GNS3 + space for images

Installation (Windows):

1. Download:
    - Visit gns3.com
    - Download GNS3 all-in-one installer
2. Run installer:
    - Accept license
    - Components to install: ☑ GNS3 ☑ GNS3 VM (VirtualBox recommended) ☑ Wireshark ☑ Npcap (for packet capture) ☐ Solar-PuTTY (optional)
    - Choose installation path
    - Install

3. First Launch Setup:
    - Open GNS3
    - Setup Wizard:
        - Server: Run appliances in virtual machine (GNS3 VM)
        - Path to GNS3 VM: Auto-detected
        - Local server path: Default
    - Finish
4. Start GNS3 VM:
    - GNS3 will start VirtualBox
    - GNS3 VM will boot automatically
    - Wait for "Server ready" message

Add Router IOS Image: LEGAL NOTE: You must own legitimate Cisco hardware or have proper licensing to use IOS images.

1. GNS3 → Edit → Preferences → IOS Routers
2. New:
    - Name: Cisco 2691
    - Platform: c2691
    - Image file: Browse to IOS image (.bin)
    - RAM: 256 MB
    - Network adapters: 2 Fast Ethernet
    - WIC Modules: 2x WIC-2T (serial)
3. Finish

Template will appear in router list

Quick Test Lab:

1. Drag router template to canvas
2. Drag another router
3. Add connection:
    - Select link tool
    - Click R1 → Select interface

- Click R2 → Select interface

4. Start devices:
    - Right-click routers → Start
    - Right-click → Console (opens terminal)
5. Basic config:

```
R1:
enable
configure terminal
interface fastEthernet 0/0
ip address 10.1.1.1 255.255.255.0
no shutdown
exit

R2:
enable
configure terminal
interface fastEthernet 0/0
ip address 10.1.1.2 255.255.255.0
no shutdown
exit
```

6. Test:

```
R1# ping 10.1.1.2
Should see !!!!! (success)
```

C. Install VMware Workstation/ESXi

VMware Workstation Pro:

1. Download:
    - VMware.com → Products → Workstation Pro
    - Download for Windows/Linux
2. Install (Windows):
    - Run installer
    - Accept license

- Installation directory: Default
- Enhanced Keyboard Driver: Yes
- Check for updates: Yes
- Shortcuts: Both
- Install

3. License:
    - Launch VMware
    - Enter license key or use trial
4. Create First VM:
    - File → New Virtual Machine
    - Typical configuration
    - Installer disc: Browse to ISO
    - Guest OS: Linux/Windows
    - Name: TestVM
    - Disk: 40GB, single file
    - Customize:
        - Memory: 4GB
        - Processors: 2
        - Network: NAT
    - Finish
    - Power on VM

VMware ESXi (Already covered in Lab 1)

Lab 10: Plan, Design and Configure DHCP and DNS LABs

A. Windows DHCP Server

Step 1: Install DHCP Role

1. Server Manager → Add Roles
2. Select: DHCP Server

3. Add Features → Install
4. Complete installation

Step 2: Authorize DHCP Server

1. Server Manager → Tools → DHCP
2. Right-click server name → Authorize
3. Right-click → Refresh
4. IPv4 icon should have green checkmark

Step 3: Create DHCP Scope

1. DHCP console → Expand server → IPv4
2. Right-click IPv4 → New Scope
3. Scope Wizard:
    - Name: Office-Network
    - Description: Main office DHCP scope
    - Start IP: 192.168.1.100
    - End IP: 192.168.1.200
    - Length: 24
    - Subnet mask: 255.255.255.0
    - Exclusions:
        - 192.168.1.1-192.168.1.10 (servers)
        - 192.168.1.254 (gateway)
    - Lease duration: 8 days (default)
    - Configure options: Yes
    - Router: 192.168.1.254
    - Domain name: company.local
    - DNS servers: 192.168.1.10 (DC IP)
    - WINS: Skip
    - Activate: Yes
    - Finish
4. Verify:

- Scope should show green arrow (active)

Step 4: Configure DHCP Options

Server Options (Apply to all scopes):

1. Right-click Server Options → Configure Options
2. Common options:
    - 003 Router: 192.168.1.254
    - 006 DNS Servers: 192.168.1.10
    - 015 DNS Domain Name: company.local
    - 042 NTP Servers: 192.168.1.10
    - 046 WINS/NBT Node Type: 0x8 (H-node)

Scope Options (Specific to scope):

1. Right-click Scope Options → Configure Options
2. Override server options if needed

Step 5: Create Reservation

1. Expand scope → Reservations
2. Right-click → New Reservation
3. Details:
    - Reservation name: PrintServer
    - IP address: 192.168.1.50
    - MAC address: 00-15-5D-00-01-0A
    - Description: HP Printer Floor 1
    - Supported types: Both DHCP and BOOTP
4. Add

Benefits: Device always gets same IP

Step 6: Test DHCP

On client computer:

1. Network adapter → Properties

2. TCP/IPv4 → Obtain automatically
3. OK

Command line:

```bash
ipconfig /release       # Release current IP
ipconfig /renew         # Request new IP
ipconfig /all           # Verify DHCP server

Should show:
- IP from DHCP range (100-200)
- DHCP Server: 192.168.1.10
- Default Gateway: 192.168.1.254
- DNS Servers: 192.168.1.10
```

B. Windows DNS Server

Step 1: Install DNS Role

1. Server Manager → Add Roles
2. Select: DNS Server
3. Install (usually installed with AD DS)

Step 2: Configure Forward Lookup Zone

1. Server Manager → Tools → DNS
2. Expand server → Forward Lookup Zones
3. Right-click → New Zone
4. Zone Wizard:
    - Zone type: Primary
    - AD integrated: Yes (if AD installed)
    - Replication scope: All DNS servers in domain
    - Zone name: company.local
    - Dynamic updates: Secure only
    - Finish

Step 3: Create DNS Records

A Records (Host):

1. Expand Forward Lookup Zone → company.local
2. Right-click → New Host (A or AAAA)
3. Details:
    - Name: webserver
    - IP: 192.168.1.100
    - Create PTR record: Checked
4. Add Host

Create additional records:

- mailserver → 192.168.1.101
- fileserver → 192.168.1.102
- dbserver → 192.168.1.103

CNAME Records (Alias):

1. Right-click zone → New Alias (CNAME)
2. Alias name: www
3. FQDN: webserver.company.local
4. OK

Now www.company.local points to webserver

MX Records (Mail):

1. Right-click zone → New Mail Exchanger (MX)
2. Host: (leave blank for @ / zone)
3. Mail server: mailserver.company.local
4. Priority: 10
5. OK

Step 4: Configure Reverse Lookup Zone

1. Right-click Reverse Lookup Zones → New Zone
2. Zone type: Primary, AD integrated
3. Replication: All DNS servers
4. IPv4 Reverse Lookup Zone
5. Network ID: 192.168.1 (Will create 1.168.192.in-addr.arpa)
6. Dynamic updates: Secure only
7. Finish

Verify PTR records:

- Should see PTR records for A records created earlier
- If not, recreate A records with PTR checked

Step 5: Configure Forwarders

1. Right-click server name → Properties
2. Forwarders tab → Edit
3. Add forwarder IPs:
    - 8.8.8.8 (Google DNS)
    - 8.8.4.4 (Google DNS alternate)
    - Or ISP DNS servers
4. OK

Purpose: Forward queries for external domains

Step 6: Test DNS

Command Prompt:

```bash
```

```
nslookup webserver.company.local
# Should return: 192.168.1.100

nslookup 192.168.1.100
# Should return: webserver.company.local

nslookup www.google.com
# Should resolve (via forwarders)
```

Test from client:

bash

```
ping webserver.company.local
ping webserver
# Both should work
```

DNS troubleshooting:

bash

```
ipconfig /displaydns       # Show DNS cache
ipconfig /flushdns         # Clear DNS cache
nslookup -debug domain.com # Detailed query
```

Lab 11: Configure BGP in Enterprise

Basic BGP Configuration (Enterprise)

Network Topology:

```
ISP Router (AS 65001)
    |
    | (203.0.113.1/30)
    |
Company Router (AS 65100)
    |
Internal: 10.0.0.0/8
```

Step 1: ISP Router Configuration

```
ISP-Router> enable
ISP-Router# configure terminal
ISP-Router(config)# hostname ISP-R1
ISP-R1(config)#

! Configure interface to customer
ISP-R1(config)# interface gigabitEthernet 0/0
ISP-R1(config-if)# description Link to Company Router
ISP-R1(config-if)# ip address 203.0.113.1 255.255.255.252
ISP-R1(config-if)# no shutdown
ISP-R1(config-if)# exit

! Configure BGP
ISP-R1(config)# router bgp 65001
ISP-R1(config-router)# bgp router-id 1.1.1.1
ISP-R1(config-router)# neighbor 203.0.113.2 remote-as 65100
ISP-R1(config-router)# neighbor 203.0.113.2 description Company Router
ISP-R1(config-router)#
ISP-R1(config-router)# network 0.0.0.0 mask 0.0.0.0
ISP-R1(config-router)# exit

! Save
ISP-R1# write memory
```

Step 2: Company Router Configuration

```
Company-Router> enable
Company-Router# configure terminal
Company-Router(config)# hostname COMPANY-R1

! WAN interface to ISP
COMPANY-R1(config)# interface gigabitEthernet 0/1
COMPANY-R1(config-if)# description WAN Link to ISP
COMPANY-R1(config-if)# ip address 203.0.113.2 255.255.255.252
COMPANY-R1(config-if)# no shutdown
COMPANY-R1(config-if)# exit

! LAN interface
COMPANY-R1(config)# interface gigabitEthernet 0/0
COMPANY-R1(config-if)# description Internal Network
COMPANY-R1(config-if)# ip address 10.0.0.1 255.255.255.0
COMPANY-R1(config-if)# no shutdown
COMPANY-R1(config-if)# exit

! Configure BGP
COMPANY-R1(config)# router bgp 65100
COMPANY-R1(config-router)# bgp router-id 2.2.2.2
COMPANY-R1(config-router)# neighbor 203.0.113.1 remote-as 65001
COMPANY-R1(config-router)# neighbor 203.0.113.1 description ISP Router
COMPANY-R1(config-router)#
! Advertise internal network
COMPANY-R1(config-router)# network 10.0.0.0 mask 255.255.255.0
COMPANY-R1(config-router)# exit

! Save configuration
COMPANY-R1# write memory
```

Step 3: Verify BGP

bash

```
! Check BGP neighbor status
COMPANY-R1# show ip bgp summary

Expected output:
BGP router identifier 2.2.2.2, local AS number 65100
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
203.0.113.1     4 65001     xxx     xxx        x    0    0 00:xx:xx        1

! View BGP routes
COMPANY-R1# show ip bgp

! Check routing table
COMPANY-R1# show ip route bgp
B    0.0.0.0/0 [20/0] via 203.0.113.1, 00:15:23

! Detailed neighbor info
COMPANY-R1# show ip bgp neighbors 203.0.113.1
```

Step 4: BGP Route Filtering (Optional)

```
! Create prefix list to control advertisements
COMPANY-R1(config)# ip prefix-list ALLOW_INTERNAL permit 10.0.0.0/8
COMPANY-R1(config)#
COMPANY-R1(config)# router bgp 65100
COMPANY-R1(config-router)# neighbor 203.0.113.1 prefix-list ALLOW_INTERNAL out
COMPANY-R1(config-router)# exit

! Apply route-map for additional control
COMPANY-R1(config)# route-map SET_ATTRIBUTES permit 10
COMPANY-R1(config-route-map)# set metric 100
COMPANY-R1(config-route-map)# exit
COMPANY-R1(config)#
COMPANY-R1(config)# router bgp 65100
COMPANY-R1(config-router)# neighbor 203.0.113.1 route-map SET_ATTRIBUTES out
```

Troubleshooting BGP:

```
Common issues:
1. Neighbor not establishing:
   - Check connectivity: ping 203.0.113.1
   - Verify AS numbers match configuration
   - Check firewall (TCP port 179)

2. No routes received:
   - show ip bgp neighbors 203.0.113.1 advertised-routes
   - show ip bgp neighbors 203.0.113.1 routes

3. Routes not in routing table:
   - Check administrative distance (eBGP = 20)
   - Verify next-hop reachability

Debug commands:
debug ip bgp                # BGP processes
debug ip bgp updates        # Route updates
undebug all                 # Turn off debugging
```

Lab 12: Perform IOS Backup and Restore, then Configure OSPF for Enterprise Network

A. IOS Backup and Restore

Step 1: Backup IOS to TFTP Server

```bash
```

```
# Setup TFTP server on PC (use Tftpd64 software)
# Configure PC with IP: 192.168.1.100
# Start TFTP server, note directory location

Router> enable
Router# show flash:
# Note IOS filename (e.g., c2900-universalk9-mz.SPA.151-4.M4.bin)

# Verify connectivity to TFTP server
Router# ping 192.168.1.100

# Copy IOS to TFTP server
Router# copy flash:c2900-universalk9-mz.SPA.151-4.M4.bin tftp:
Address or name of remote host []? 192.168.1.100
Destination filename [c2900-universalk9-mz.SPA.151-4.M4.bin]? [Enter]
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - xxxx bytes copied in xx.xxx secs]

# Backup running configuration
Router# copy running-config tftp:
Address or name of remote host []? 192.168.1.100
Destination filename [router-confg]? router1-backup.cfg
!!
[OK]

# Backup startup configuration
Router# copy startup-config tftp:
```

Step 2: Restore IOS from TFTP

bash

```
# Verify current flash contents
Router# show flash:

# Delete old IOS (if needed for space)
Router# delete flash:old-ios.bin
Delete filename [old-ios.bin]? [Enter]
Delete flash:old-ios.bin? [confirm] [Enter]

# Copy new IOS from TFTP
Router# copy tftp: flash:
Address or name of remote host []? 192.168.1.100
Source filename []? c2900-universalk9-mz.SPA.151-4.M4.bin
Destination filename [c2900-universalk9-mz.SPA.151-4.M4.bin]? [Enter]
Accessing tftp://192.168.1.100/c2900...
Loading from 192.168.1.100: !!!!!!!!!!!!!!!!
[OK - copied xxxxx bytes in xx.xx secs]

# Verify IOS in flash
Router# show flash:

# Set boot variable
Router# configure terminal
Router(config)# boot system flash:c2900-universalk9-mz.SPA.151-4.M4.bin
Router(config)# exit
Router# write memory

# Reload router
Router# reload
Proceed with reload? [confirm] [Enter]
```

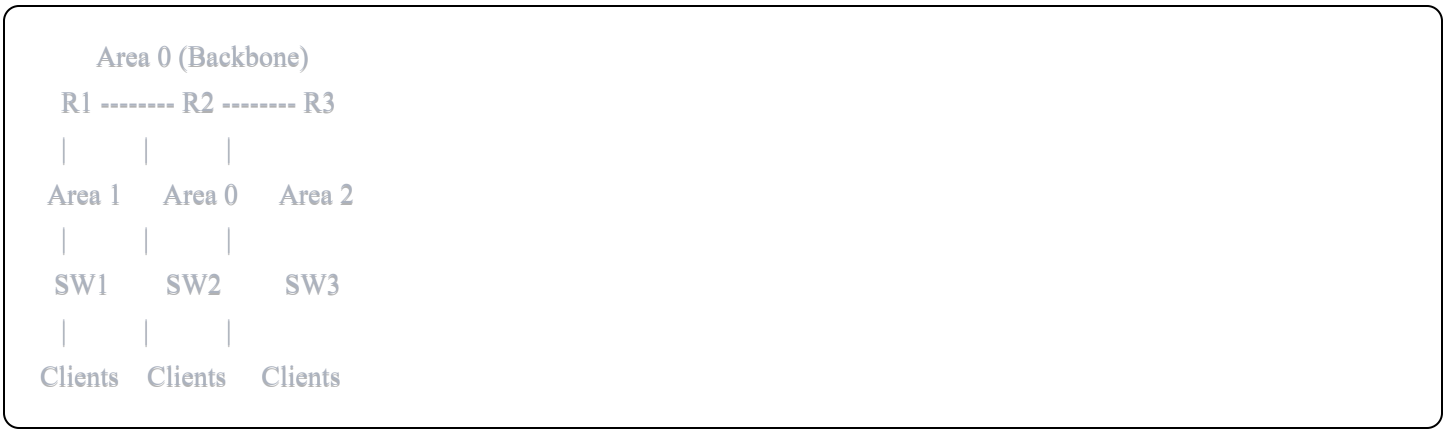
Step 3: Restore Configuration

```
bash
```

```
# After reload, restore configuration
Router> enable
Router# copy tftp: running-config
Address or name of remote host []? 192.168.1.100
Source filename []? router1-backup.cfg
Destination filename [running-config]? [Enter]
Accessing tftp://192.168.1.100/router1-backup.cfg...
Loading from 192.168.1.100: !
[OK - xxx bytes]

# Verify configuration loaded
Router# show running-config

# Save to startup-config
Router# copy running-config startup-config
```

B. Configure OSPF for Enterprise Network

Network Topology:



Step 1: Configure R1 (Area Border Router - ABR)

```
R1> enable
R1# configure terminal
R1(config)# hostname R1

! Configure interfaces
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 10.0.12.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# interface gigabitEthernet 0/1
R1(config-if)# description Area 1 Network
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit

! Configure OSPF
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.0.12.0 0.0.0.3 area 0
R1(config-router)# network 192.168.1.0 0.0.0.255 area 1
R1(config-router)# passive-interface gigabitEthernet 0/1
R1(config-router)# exit

! Save
R1# write memory
```

Step 2: Configure R2 (Core Router)

```
R2# configure terminal
R2(config)# hostname R2

! Interface to R1
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# description Link to R1
R2(config-if)# ip address 10.0.12.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit

! Interface to R3
R2(config)# interface gigabitEthernet 0/1
R2(config-if)# description Link to R3
R2(config-if)# ip address 10.0.23.1 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit

! Loopback for testing
R2(config)# interface loopback 0
R2(config-if)# ip address 2.2.2.2 255.255.255.255
R2(config-if)# exit

! Configure OSPF
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 10.0.12.0 0.0.0.3 area 0
R2(config-router)# network 10.0.23.0 0.0.0.3 area 0
R2(config-router)# network 2.2.2.2 0.0.0.0 area 0
R2(config-router)# exit

R2# write memory
```

Step 3: Configure R3 (ABR)

```
R3# configure terminal
R3(config)# hostname R3

! Interface to R2
R3(config)# interface gigabitEthernet 0/0
R3(config-if)# description Link to R2
R3(config-if)# ip address 10.0.23.2 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit

! Interface to Area 2
R3(config)# interface gigabitEthernet 0/1
R3(config-if)# description Area 2 Network
R3(config-if)# ip address 192.168.2.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit

! Configure OSPF
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 10.0.23.0 0.0.0.3 area 0
R3(config-router)# network 192.168.2.0 0.0.0.255 area 2
R3(config-router)# passive-interface gigabitEthernet 0/1
R3(config-router)# exit

R3# write memory
```

Step 4: Verify OSPF

bash

```
! Check OSPF neighbors
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:35    10.0.12.2       GigabitEthernet0/0

! View OSPF database
R1# show ip ospf database

! Check routing table
R1# show ip route ospf
O IA  192.168.2.0/24 [110/3] via 10.0.12.2, 00:05:23, GigabitEthernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/2] via 10.0.12.2, 00:10:15, GigabitEthernet0/0

! Test connectivity
R1# ping 192.168.2.1
!!!!!
Success rate is 100 percent (5/5)

! Detailed OSPF interface info
R1# show ip ospf interface brief
Interface    PID   Area   IP Address/Mask    Cost  State Nbrs F/C
Gi0/0        1     0      10.0.12.1/30       1     DR    1/1
Gi0/1        1     1      192.168.1.1/24     1     DR    0/0
```

Step 5: Advanced OSPF Configuration

bash

```
! Configure OSPF cost manually
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip ospf cost 50
R1(config-if)# exit

! Configure OSPF authentication (area level)
R1(config)# router ospf 1
R1(config-router)# area 0 authentication message-digest
R1(config-router)# exit
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 MySecretKey123
R1(config-if)# exit

! Configure default route propagation
R2(config)# router ospf 1
R2(config-router)# default-information originate
R2(config-router)# exit

! Tune OSPF timers
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
R1(config-if)# exit

! Route summarization at ABR
R1(config)# router ospf 1
R1(config-router)# area 1 range 192.168.0.0 255.255.252.0
R1(config-router)# exit
```

OSPF Troubleshooting:

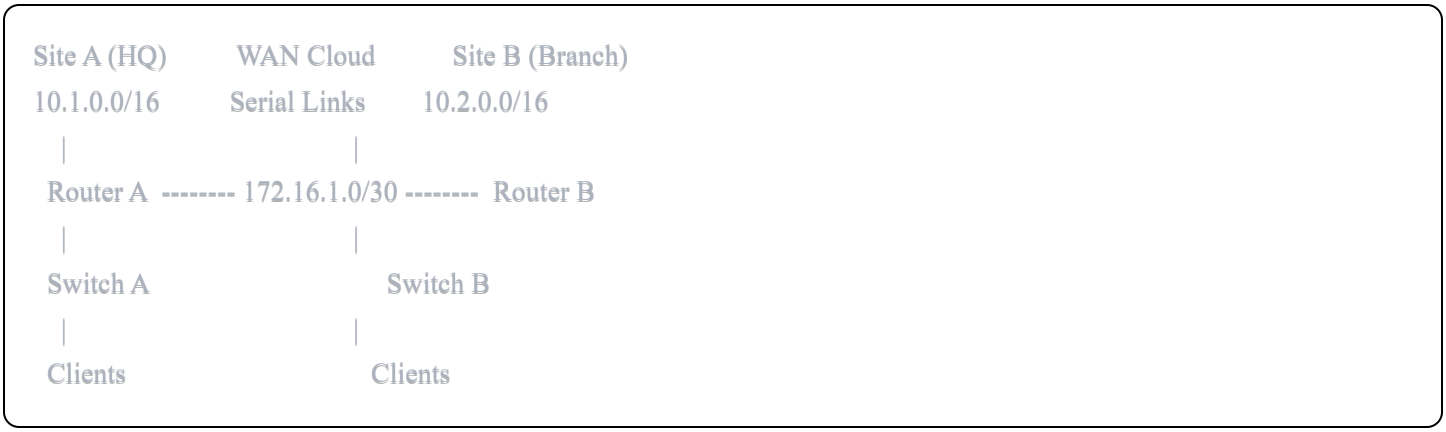
```
bash
```

```
! Verify OSPF is running
show ip protocols

! Check interface OSPF status
show ip ospf interface

! View OSPF process ID
show ip ospf

! Debug OSPF (use carefully)
debug ip ospf adj          # Adjacency formation
debug ip ospf events       # OSPF events
debug ip ospf packets      # OSPF packets

Common issues:
1. Neighbors not forming:
   - Check network connectivity (ping)
   - Verify area numbers match
   - Check authentication configuration
   - Verify hello/dead timers match
   - Check MTU settings

2. Routes not appearing:
   - Verify network statements
   - Check passive interfaces
   - Review area configuration

3. Slow convergence:
   - Tune hello/dead timers
   - Check for flapping links
   - Review network design
```

Lab 13: Design WAN LAB, Perform Static Routing & Configure Access-List

A. Design WAN Lab

Network Topology:



Equipment Required:

- 2 Routers with serial interfaces
- 2 Switches (Layer 2)
- 4 PCs (or more)
- Serial cables (DCE/DTE)
- Ethernet cables

Step 1: Configure Site A (HQ) Router

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# hostname SiteA-R1

! Configure LAN interface
SiteA-R1(config)# interface gigabitEthernet 0/0
SiteA-R1(config-if)# description LAN Interface Site A
SiteA-R1(config-if)# ip address 10.1.0.1 255.255.0.0
SiteA-R1(config-if)# no shutdown
SiteA-R1(config-if)# exit

! Configure WAN interface (DCE side - provides clock)
SiteA-R1(config)# interface serial 0/0/0
SiteA-R1(config-if)# description WAN Link to Site B
SiteA-R1(config-if)# ip address 172.16.1.1 255.255.255.252
SiteA-R1(config-if)# clock rate 128000
SiteA-R1(config-if)# bandwidth 128
SiteA-R1(config-if)# no shutdown
SiteA-R1(config-if)# exit

! Configure default gateway (or static route)
SiteA-R1(config)# ip route 10.2.0.0 255.255.0.0 172.16.1.2
SiteA-R1(config)# exit
SiteA-R1# write memory
```

Step 2: Configure Site B (Branch) Router

```
RouterB> enable
RouterB# configure terminal
RouterB(config)# hostname SiteB-R1

! Configure LAN interface
SiteB-R1(config)# interface gigabitEthernet 0/0
SiteB-R1(config-if)# description LAN Interface Site B
SiteB-R1(config-if)# ip address 10.2.0.1 255.255.0.0
SiteB-R1(config-if)# no shutdown
SiteB-R1(config-if)# exit

! Configure WAN interface (DTE side)
SiteB-R1(config)# interface serial 0/0/0
SiteB-R1(config-if)# description WAN Link to Site A
SiteB-R1(config-if)# ip address 172.16.1.2 255.255.255.252
SiteB-R1(config-if)# bandwidth 128
SiteB-R1(config-if)# no shutdown
SiteB-R1(config-if)# exit

! Configure static route
SiteB-R1(config)# ip route 10.1.0.0 255.255.0.0 172.16.1.1
SiteB-R1(config)# exit
SiteB-R1# write memory
```

Step 3: Configure Switches

bash

```
! Switch A (Site A)
SwitchA> enable
SwitchA# configure terminal
SwitchA(config)# hostname SiteA-SW1
SwitchA(config)# interface vlan 1
SwitchA(config-if)# ip address 10.1.0.10 255.255.0.0
SwitchA(config-if)# no shutdown
SwitchA(config-if)# exit
SwitchA(config)# ip default-gateway 10.1.0.1
SwitchA(config)# exit
SwitchA# write memory

! Switch B (Site B) - Similar configuration
SwitchB(config)# interface vlan 1
SwitchB(config-if)# ip address 10.2.0.10 255.255.0.0
SwitchB(config-if)# no shutdown
SwitchB(config)# ip default-gateway 10.2.0.1
```

Step 4: Configure End Devices

```
Site A PC1:
IP: 10.1.0.100
Subnet: 255.255.0.0
Gateway: 10.1.0.1
DNS: 8.8.8.8

Site A PC2:
IP: 10.1.0.101
Subnet: 255.255.0.0
Gateway: 10.1.0.1

Site B PC1:
IP: 10.2.0.100
Subnet: 255.255.0.0
Gateway: 10.2.0.1
DNS: 8.8.8.8

Site B PC2:
IP: 10.2.0.101
Subnet: 255.255.0.0
Gateway: 10.2.0.1
```

B. Static Routing Configuration

Basic Static Routes (Already configured above):

```
! Site A Router
ip route 10.2.0.0 255.255.0.0 172.16.1.2

! Site B Router
ip route 10.1.0.0 255.255.0.0 172.16.1.1
```

Advanced Static Routing Scenarios:

1. Default Static Route

```
! Send all unknown traffic to specific next-hop
SiteB-R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1

! Or to specific interface
SiteB-R1(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/0

! With administrative distance (for redundancy)
SiteB-R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1 10
SiteB-R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.1 20
! First route preferred (lower AD)
```

2. Floating Static Route (Backup)

```
! Primary route via OSPF (AD=110)
! Backup static route with higher AD
SiteA-R1(config)# ip route 10.2.0.0 255.255.0.0 172.16.1.2 150

! This route only activates if OSPF route fails
```

3. Static Route with Exit Interface

```
! Using next-hop IP
ip route 192.168.3.0 255.255.255.0 172.16.1.2

! Using exit interface
ip route 192.168.3.0 255.255.255.0 serial 0/0/0

! Using both (recommended for serial links)
ip route 192.168.3.0 255.255.255.0 serial 0/0/0 172.16.1.2
```

4. Multiple Path Static Routes (Load Balancing)

```
SiteA-R1(config)# ip route 10.3.0.0 255.255.0.0 172.16.1.2
SiteA-R1(config)# ip route 10.3.0.0 255.255.0.0 172.16.2.2

! Both routes have equal cost, traffic load-balanced
```

Verify Static Routes:

bash

```
! View routing table
show ip route
show ip route static

! Test connectivity
ping 10.2.0.100 source 10.1.0.100
traceroute 10.2.0.100

! Show route for specific destination
show ip route 10.2.0.100
```

C. Configure Access Control Lists (ACLs)

Standard ACL (Filters by Source IP only)

```
! Deny specific host, permit all others
SiteA-R1(config)# access-list 10 deny host 10.1.0.150
SiteA-R1(config)# access-list 10 permit any

! Apply to interface
SiteA-R1(config)# interface serial 0/0/0
SiteA-R1(config-if)# ip access-group 10 out
SiteA-R1(config-if)# exit

! Permit specific network only
SiteA-R1(config)# access-list 20 permit 10.1.0.0 0.0.255.255
SiteA-R1(config)# access-list 20 deny any
```

Extended ACL (Filters by Source, Destination, Protocol, Port)

```
! Block web traffic from Site B to specific server
SiteA-R1(config)# access-list 100 deny tcp 10.2.0.0 0.0.255.255 host 10.1.0.50 eq 80
SiteA-R1(config)# access-list 100 deny tcp 10.2.0.0 0.0.255.255 host 10.1.0.50 eq 443
SiteA-R1(config)# access-list 100 permit ip any any

! Apply inbound on interface
SiteA-R1(config)# interface serial 0/0/0
SiteA-R1(config-if)# ip access-group 100 in
SiteA-R1(config-if)# exit

! Allow SSH only from admin network
SiteA-R1(config)# access-list 110 permit tcp 10.1.1.0 0.0.0.255 any eq 22
SiteA-R1(config)# access-list 110 deny tcp any any eq 22
SiteA-R1(config)# access-list 110 permit ip any any

! Block ICMP (ping) from specific subnet
SiteA-R1(config)# access-list 120 deny icmp 10.2.100.0 0.0.0.255 any echo
SiteA-R1(config)# access-list 120 permit ip any any
```

Named ACLs (More flexible)

```
! Create named standard ACL
SiteA-R1(config)# ip access-list standard BLOCK_GUEST_VLAN
SiteA-R1(config-std-nacl)# deny 10.1.100.0 0.0.0.255
SiteA-R1(config-std-nacl)# permit any
SiteA-R1(config-std-nacl)# exit

! Create named extended ACL
SiteA-R1(config)# ip access-list extended FIREWALL_RULES
SiteA-R1(config-ext-nacl)# remark Allow established connections
SiteA-R1(config-ext-nacl)# permit tcp any any established
SiteA-R1(config-ext-nacl)# remark Block Telnet
SiteA-R1(config-ext-nacl)# deny tcp any any eq 23
SiteA-R1(config-ext-nacl)# remark Allow HTTPS
SiteA-R1(config-ext-nacl)# permit tcp any any eq 443
SiteA-R1(config-ext-nacl)# remark Allow DNS
SiteA-R1(config-ext-nacl)# permit udp any any eq 53
SiteA-R1(config-ext-nacl)# remark Deny all other traffic
SiteA-R1(config-ext-nacl)# deny ip any any log
SiteA-R1(config-ext-nacl)# exit

! Apply named ACL
SiteA-R1(config)# interface gigabitEthernet 0/0
SiteA-R1(config-if)# ip access-group FIREWALL_RULES in
```

Common ACL Examples:

1. Restrict VTY Access (Telnet/SSH to router)

```
SiteA-R1(config)# access-list 50 permit 10.1.1.0 0.0.0.255
SiteA-R1(config)# access-list 50 deny any
SiteA-R1(config)# line vty 0 4
SiteA-R1(config-line)# access-class 50 in
SiteA-R1(config-line)# exit
```

2. Allow Only Specific Services

```
! Allow only HTTP, HTTPS, DNS, and ICMP
SiteA-R1(config)# ip access-list extended INTERNET_ACCESS
SiteA-R1(config-ext-nacl)# permit tcp any any eq 80
SiteA-R1(config-ext-nacl)# permit tcp any any eq 443
SiteA-R1(config-ext-nacl)# permit udp any any eq 53
SiteA-R1(config-ext-nacl)# permit icmp any any echo
SiteA-R1(config-ext-nacl)# permit icmp any any echo-reply
SiteA-R1(config-ext-nacl)# deny ip any any
SiteA-R1(config-ext-nacl)# exit
```

3. Time-Based ACL

```
! Create time range
SiteA-R1(config)# time-range BUSINESS_HOURS
SiteA-R1(config-time-range)# periodic weekdays 9:00 to 17:00
SiteA-R1(config-time-range)# exit

! Apply to ACL
SiteA-R1(config)# ip access-list extended TIME_POLICY
SiteA-R1(config-ext-nacl)# permit tcp any any eq 80 time-range BUSINESS_HOURS
SiteA-R1(config-ext-nacl)# deny tcp any any eq 80
SiteA-R1(config-ext-nacl)# exit
```

Verify ACLs:

bash

```
! View all ACLs
show access-lists

! View specific ACL
show access-lists 100
show ip access-list FIREWALL_RULES

! View ACL statistics
show ip access-lists

! Show where ACLs are applied
show ip interface gigabitEthernet 0/0

! Clear ACL counters
clear access-list counters 100
```

ACL Best Practices:

1. Place standard ACLs close to destination
2. Place extended ACLs close to source
3. Always include implicit deny at end (automatic)
4. Process ACLs top-down, first match wins
5. Use named ACLs for better management
6. Add remarks for documentation
7. Be careful with deny any - can lock you out
8. Test before applying to production
9. One ACL per interface, per direction, per protocol
10. Remember: inbound = before routing, outbound = after routing

---

Summary & Exam Tips

All 13 Labs Covered:

1. ✅ ESXi Installation & Configuration
2. ✅ CDP, NAT-PAT Configuration
3. ✅ AWS Management Tools & Disaster Recovery
4. ✅ AWS Storage, Security & VPC with Database
5. ✅ File Server Design & DFS
6. ✅ LAN Lab (2 PC Setup)
7. ✅ Domain Controller & Additional DC
8. ✅ Group Policy Object (GPO)
9. ✅ Packet Tracer, GNS3, VMware Installation
10. ✅ DHCP & DNS Configuration
11. ✅ BGP Enterprise Configuration
12. ✅ IOS Backup/Restore & OSPF
13. ✅ WAN Lab, Static Routing & Access Lists

Practical Exam Tips:

Time Management (2 hours 30 minutes):

- Allocate 10-15 minutes per lab
- Quick labs (5-7 minutes): LAN, BGP, Static Routing
- Medium labs (10-15 minutes): DHCP, DNS, VPC
- Long labs (15-20 minutes): ESXi, Domain Controller, OSPF

Common Mistakes to Avoid:

1. **Not saving configurations**: Always `write memory` or `copy run start`
2. **Wrong subnet masks**: Double-check CIDR calculations
3. **Forgetting clock rate**: DCE side of serial connections needs clock rate
4. **Security group rules**: Remember inbound vs outbound
5. **DNS pointing**: Make sure DNS points to correct server
6. **OSPF area mismatches**: Verify area numbers on both sides
7. **ACL placement**: Standard near destination, extended near source
8. **NAT interfaces**: Inside vs outside configuration

Must-Know Commands:

Cisco IOS:

```
show running-config        # Current configuration
show ip interface brief    # IP addresses and status
show ip route              # Routing table
show ip protocols          # Routing protocols
ping [ip]                  # Test connectivity
traceroute [ip]            # Path to destination
write memory               # Save configuration
```

Windows Server:

```
ipconfig /all              # Network configuration
dcdiag                     # DC diagnostics
repadmin /showrepl         # AD replication
gpupdate /force            # Update GPO
nslookup [hostname]        # DNS lookup
```

AWS CLI (if needed):

```
aws ec2 describe-instances       # List EC2 instances
aws s3 ls                        # List S3 buckets
aws vpc describe-vpcs            # List VPCs
```

Troubleshooting Checklist:

- [ ] Physical connectivity (cables, lights)
- [ ] IP configuration (correct IP, subnet, gateway)
- [ ] Routing (show ip route)
- [ ] Firewall/Security Groups
- [ ] DNS resolution
- [ ] Services running (DHCP, DNS, HTTP)
- [ ] Logs (Event Viewer, CloudWatch)

Practice Strategy:

1. Do each lab 3 times minimum
2. Time yourself on third attempt
3. Practice without notes on final run
4. Create your own variations
5. Document common errors

End of Practical Solutions Document

To Convert to PDF:

1. Copy this entire document
2. Paste into Microsoft Word or Google Docs
3. Format as needed (adjust fonts, spacing)

4. File → Save As → PDF
5. Or use online Markdown to PDF converters like:
    - markdown-pdf.com
    - dillinger.io (export to PDF)
    - pandoc (command line tool)

Good luck with your practical exam! 🚀