220041125

# Network Lab Mid Guide

## Phase 1: IP Addressing & Physical Connectivity

**Goal:** Configure hostnames and IP addresses on all router interfaces to establish physical links.

### Bridge Router (Central Gateway)

enable  
configure terminal  
hostname Bridge  
  
! 1. WAN Link to ISP (Outside)  
interface gigabitEthernet 0/0  
 description Link to ISP  
 ip address 203.0.113.5 255.255.255.252  
 no shutdown  
 exit  
  
! 2. Link to HQ Router (Inside)  
interface gigabitEthernet 0/1  
 description Link to HQ  
 ip address 172.16.0.229 255.255.255.252  
 no shutdown  
 exit  
  
! 3. Link to DS Branch Router (Inside)  
interface gigabitEthernet 0/2  
 description Link to DS Branch  
 ip address 172.16.0.1 255.255.255.128  
 no shutdown  
 exit

### ISP Router (Simulating the Internet)

enable

configure terminal  
hostname ISP  
  
! 1. Link to Bridge Router  
interface gigabitEthernet 0/0  
 ip address 203.0.113.6 255.255.255.252  
 no shutdown  
 exit  
  
! 2. Link to Public Server (8.8.8.8)  
interface gigabitEthernet 0/1  
 ip address 8.8.8.1 255.255.255.0  
 no shutdown  
 exit

*> Important Note: Do NOT add static routes to the 172.16.x.x network on the ISP router.*

### HQ Router

enable  
configure terminal  
hostname HQ  
  
! Link to Bridge  
interface gigabitEthernet 0/1  
 ip address 172.16.0.230 255.255.255.252  
 no shutdown  
 exit  
  
! Link to Internal LAN (Staff/Mgmt)  
interface gigabitEthernet 0/0  
 ip address 172.16.0.129 255.255.255.192  
 no shutdown  
 exit

### DS Branch Router

enable  
configure terminal  
hostname DS  
  
! Link to Bridge  
interface gigabitEthernet 0/2  
 ip address 172.16.0.2 255.255.255.128  
 no shutdown  
 exit

## Phase 2: VLANs & Switching

**Goal:** Configure the Switch to assign ports to the correct VLAN for Staff.

### Switch 1 (HQ Switch)

enable  
configure terminal  
hostname Switch-HQ  
  
! 1. Create the VLAN  
vlan 10  
 name STAFF  
 exit  
  
! 2. Configure Access Ports for PCs (e.g., Ports 2-10)  
interface range fastEthernet 0/2 - 10  
 switchport mode access  
 switchport access vlan 10  
 no shutdown  
 exit  
  
! 3. Configure Uplink Port to Router (e.g., Port 1)  
interface fastEthernet 0/1  
 switchport mode access  
 switchport access vlan 10  
 no shutdown  
 exit

## Phase 3: Routing Protocols (OSPF, RIP & Redistribution)

**Goal:** Configure OSPF for HQ, RIP for DS, and make the Bridge router translate between them.

### HQ Router (OSPF Configuration)

enable  
configure terminal  
  
! 1. Enable OSPF Process 1  
router ospf 1  
 ! Advertise internal networks to Area 0  
 network 172.16.0.128 0.0.0.63 area 0 ! Staff LAN  
 network 172.16.0.228 0.0.0.3 area 0 ! Link to Bridge  
 exit  
  
! 2. Static Default Route (Gateway of Last Resort)  
ip route 0.0.0.0 0.0.0.0 172.16.0.229

### DS Branch Router (RIPv2 Configuration)

enable  
configure terminal  
  
! 1. Enable RIP Version 2  
router rip  
 version 2  
 no auto-summary  
 ! Advertise networks  
 network 172.16.0.0  
 exit  
  
! 2. Static Default Route  
ip route 0.0.0.0 0.0.0.0 172.16.0.1

### Bridge Router (The "Translator")

enable  
configure terminal  
  
! 1. Configure Static Route to Internet  
ip route 0.0.0.0 0.0.0.0 203.0.113.6  
  
! 2. Configure OSPF (Talking to HQ)  
router ospf 1  
 network 172.16.0.228 0.0.0.3 area 0  
 ! Redistribute RIP routes into OSPF so HQ can reach DS  
 redistribute rip subnets  
 ! Advertise the Default Route (Internet) to HQ  
 default-information originate  
 exit  
  
! 3. Configure RIP (Talking to DS)  
router rip  
 version 2  
 no auto-summary  
 network 172.16.0.0  
 ! Redistribute OSPF routes into RIP so DS can reach HQ  
 redistribute ospf 1 metric 5  
 ! Advertise the Default Route (Internet) to DS  
 default-information originate  
 exit

## Phase 4: NAT & Internet Security (Detailed)

**Goal:** Configure Network Address Translation (NAT) with Overload to allow Staff to access the internet while blocking Management.

### Bridge Router (NAT Configuration)

Step 1: Define the "Inside" and "Outside" Interfaces

Tell the router which interfaces are trusted (internal) and which is untrusted (internet).

! The ISP Interface  
interface gigabitEthernet 0/0  
 ip nat outside  
 exit  
  
! The HQ Interface  
interface gigabitEthernet 0/1  
 ip nat inside  
 exit  
  
! The DS Branch Interface  
interface gigabitEthernet 0/2  
 ip nat inside  
 exit

Step 2: Create the Access Control List (ACL)

Define EXACTLY who is allowed to be translated. Any IP not on this list is implicitly denied.

! Remove old list if it exists  
no access-list 1  
  
! Permit DS Branch Network (172.16.0.0 /25)  
access-list 1 permit 172.16.0.0 0.0.0.127  
  
! Permit HQ Staff Network (172.16.0.128 /26)  
access-list 1 permit 172.16.0.128 0.0.0.63  
  
! Note: Management (172.16.0.192) is NOT added, so it is BLOCKED.

Step 3: Apply NAT Overload (PAT)

Link the ACL to the Outside interface so multiple private IPs can share one public IP.

ip nat inside source list 1 interface gigabitEthernet 0/0 overload

## Phase 5: Verification & Troubleshooting

**Goal:** Use "Show" commands to prove the network meets all requirements.

### 1. Verify IP Addresses & Interfaces

**Command:** show ip interface brief

* **Check:** All used interfaces should say "YES", Status "up", Protocol "up".
* **Troubleshoot:** If "administratively down", go to interface and type no shutdown.

### 2. Verify Routing Table

**Command:** show ip route

* **On HQ:** Look for O E2 (External routes from Bridge) or the static default route S\*.
* **On DS:** Look for R (Routes from HQ/Bridge).
* **On Bridge:** Look for S\* 0.0.0.0/0 pointing to the ISP.

### 3. Verify NAT (Crucial Step)

**Command:** show ip nat translations

* **Scenario A: Staff PC Pings 8.8.8.8** -> **Result:** SUCCESS.
  + *Check:* The table should show an entry mapping 172.16.0.130 (Inside Local) to 203.0.113.5 (Inside Global).
* **Scenario B: Mgmt PC Pings 8.8.8.8** -> **Result:** FAIL.
  + *Check:* The table should NOT show any entry for the Management IP.

### 4. Verify NAT Statistics & ACL

**Command:** show ip nat statistics

* **Check:** Look for "Total active translations".
* **Check:** Ensure "Outside interface: GigabitEthernet0/0".

**Command:** show access-lists

* **Check:** Look for the "matches" count next to the permit lines. If matches are 0 after pinging, check your IP addressing.

### 5. Real-Time Debugging (If things fail)

**Command:** debug ip nat

* **Action:** Turn this on, then ping from a PC.
* **Output:** You will see the router saying "s=172.16.x.x -> 203.0.113.5" if it works.
* **Stop:** Type undebug all when finished.

Here are the specific **DHCP** and **Appendix** sections you requested for your Lab Midterm preparation document.

# Phase: DHCP Configuration

**Goal:** Configure the Router to either act as the DHCP Server itself or relay requests to a central server.

### Scenario A: Router as DHCP Server

*Use this when the router assigns IPs to PCs directly.*

Bash

enable

configure terminal

! 1. Exclude IPs for Gateway/Servers (Optional but Recommended)

! Format: ip dhcp excluded-address <Start\_IP> <End\_IP>

ip dhcp excluded-address 192.168.1.1 192.168.1.5

! 2. Create the DHCP Pool

ip dhcp pool STAFF\_POOL

! Define the network and subnet mask

network 192.168.1.0 255.255.255.0

! Define the Default Gateway (This router's interface IP)

default-router 192.168.1.1

! Define DNS Server (Usually 8.8.8.8 or the ISP)

dns-server 8.8.8.8

exit

### Scenario B: DHCP Relay (Helper Address)

*Use this on the Router interface connected to the PCs if the DHCP Server is on a DIFFERENT network.*

Bash

enable

configure terminal

! Enter the interface connected to the Client PCs

interface gigabitEthernet 0/1

! Point to the IP address of the Remote DHCP Server

ip helper-address 192.168.2.100

exit

# Appendix: Comprehensive "Show" & Troubleshooting Commands

**Use these commands during the Verification Phase to prove your configuration works.**

### 1. Interface & Connectivity

| **Command** | **Description** |
| --- | --- |
| show ip interface brief | Quick check of IP addresses and Interface Status (Up/Up). |
| show interfaces serial 0/0/0 | Detailed check for Serial links (Look for DCE/DTE clock rate). |
| ping <Destination\_IP> | Test basic connectivity (e.g., ping 8.8.8.8). |

### 2. Routing Protocols (OSPF, RIP, Static)

| **Command** | **Description** |
| --- | --- |
| show ip route | View the routing table. Look for codes: **S** (Static), **R** (RIP), **O** (OSPF), **C** (Connected). |
| show ip protocols | Check which networks you are advertising and protocol timers. |
| show ip ospf neighbor | Verify OSPF neighbor adjacencies (State should be FULL). |
| show ip rip database | View the RIP network database. |

### 3. NAT & Security (Crucial for Midterm)

| **Command** | **Description** |
| --- | --- |
| show ip nat translations | View active connections. **Empty** = No traffic or Broken NAT. **Entries** = Working NAT. |
| show ip nat statistics | Check total translations and if the "Outside" interface is correctly set. |
| show access-lists | View ACLs. Look for the "matches" counter increasing on permit lines. |
| debug ip nat | View real-time translation logs. (Turn off with undebug all). |

### 4. DHCP Verification

| **Command** | **Description** |
| --- | --- |
| show ip dhcp binding | See which PCs have successfully received an IP address from the pool. |
| show ip dhcp pool | View pool usage statistics (how many IPs are leased vs. free). |

### 5. Switching & VLANs

| **Command** | **Description** |
| --- | --- |
| show vlan brief | List all VLANs and ensure ports are assigned to the correct VLAN. |
| show interfaces trunk | Verify Trunk ports (Status should be trunking). |
| show mac address-table | See which MAC addresses the switch has learned and on which ports. |