Network Configuration & ACL Implementation Guide

✅ Task 1: Investigate the Current Network Configuration

🔹 Step 1: View the running configuration

On all routers (R1, R2, R3, ISP), run:

show run
or
show ip interface brief

This helps confirm:

• Interfaces are up
• IP addresses match the plan
• Routing (EIGRP 100) is properly configured
• EIGRP neighbor relationships are established

🔹 Step 2: Confirm device connectivity

From each PC, try to ping:
• Default gateway (e.g., PC1 should ping 192.168.10.1)
• Web server: ping 209.165.201.30
• Another PC from a different subnet

From each router, ping other routers' serial interfaces and the web server.

✅ Task 2: Evaluate Policies and Plan ACL Implementation

🔹 Step 1: Policy for R1 LANs (192.168.10.0/24 and 192.168.11.0/24)
Let’s say the policy is:

PC1 and PC2 (R1 LANs) should not access the Web Server (209.165.201.30)
✅ They can access everything else.

🔹 Step 2: Plan ACL for R1 LANs

Use standard ACL (since we’re filtering by source IP). Place ACL closest to the destination — typically outbound on R1's serial interface S0/0/0

Access list example for R1:

access-list 10 deny 192.168.10.0 0.0.0.255
access-list 10 deny 192.168.11.0 0.0.0.255
access-list 10 permit any

interface S0/0/0
ip access-group 10 out

🔹 Step 3: Policy for R3 LAN (192.168.30.0/24)

Let’s assume:
❌ Only PC4 (192.168.30.128) is allowed to access the Web Server
❌ PC3 (192.168.30.10) should be blocked

🔹 Step 4: Plan ACL for R3

Apply a named standard ACL on R3 Fa0/0 (inbound):

ip access-list standard R3-LAN-ACL
 permit 192.168.30.128
 deny any
interface Fa0/0
ip access-group R3-LAN-ACL in

✅ Task 3: Configure Numbered Standard ACLs

🔹 Step 1: Wildcard Mask
For full subnet 192.168.10.0/24 → wildcard: 0.0.0.255
For a specific host (PC4): 0.0.0.0

🔹 Step 2: Determine Statements

For R1:
access-list 10 deny 192.168.10.0 0.0.0.255
access-list 10 deny 192.168.11.0 0.0.0.255
access-list 10 permit any

For R3:
access-list 15 permit 192.168.30.128
access-list 15 deny any

🔹 Step 3: Apply ACL to Interfaces

R1:
interface S0/0/0
ip access-group 10 out

R3:
interface Fa0/0
ip access-group 15 in

🔹 Step 4: Verify and Test ACLs

From each PC, try:
ping 209.165.201.30
tracert 209.165.201.30 (Windows)
Use show access-lists on routers to confirm hits.

🔹 Step 5: Check Results

PC1 & PC2 should be blocked from reaching Web Server
PC3 should be blocked; PC4 should succeed
Other communications (e.g., LAN to LAN) should work

✅ Task 4: Configure Named Standard ACL

Let's say for R3:

ip access-list standard ONLY_PC4
 permit 192.168.30.128
 deny any
interface Fa0/0
ip access-group ONLY_PC4 in

STEP 1: Confirm Basic Connectivity & Routing

1.1: Check IP Configuration

Ensure all PCs and servers have:

Correct IP addresses

Correct default gateways

For example:

Device	IP Address	Subnet Mask	Default Gateway
PC1	192.168.10.10	255.255.255.0	192.168.10.1

PC2 192.168.11.10 255.255.255.0 192.168.11.1

PC3 192.168.30.10 255.255.255.0 192.168.30.1

PC4 192.168.30.128 255.255.255.0 192.168.30.1

WebServer 209.165.201.30 255.255.255.224 209.165.201.1

OutsideHost 209.165.202.158 255.255.255.224 209.165.202.129

1.2: Ensure Interfaces Are Up

On all routers (R1, R2, R3, ISP), use:

show ip interface brief

Check that all relevant interfaces are:

"up" and "up"

Configured with the correct IPs

1.3: Check Routing (EIGRP 100)

On R1, R2, R3, confirm that routing is working:

show ip route

show ip protocols

Make sure:

Each router has routes to 209.165.201.0/27 and 209.165.202.128/27

EIGRP neighbors are up: *show ip eigrp neighbors*

Also verify that the ISP router has static routes pointing back to internal networks, like:

ip route 192.168.0.0 255.255.0.0 209.165.200.225

✅ STEP 2: Test Pings

From PC1, PC2, PC3 or PC4, try:

ping 209.165.202.158 (Outside Host)

ping 209.165.201.30 (Web Server)

✅ STEP 3: Fix Connectivity to Web Server

The ping to 209.165.201.30 replies with Destination host unreachable from 192.168.30.1

That means R3 (192.168.30.1) doesn't have a valid route to 209.165.201.30.

3.1: Add Static Route on R3 (if missing)

If EIGRP isn't covering this path (maybe ISP isn't participating in EIGRP), manually add a static route:

R3(config)# ip route 209.165.201.0 255.255.255.224 10.2.2.2

This tells R3 to forward traffic for the Web Server network via R2.

3.2: Add Reverse Static Routes on ISP

The ISP router needs a static route back to the internal LANs, if not present:

ISP(config)# ip route 192.168.0.0 255.255.0.0 209.165.200.225

✅ STEP 4: Verify Again

Now try again from a PC:

ping 209.165.201.30

ping 209.165.202.158

If the pings now succeed:

Routing is fixed.

You can now proceed to apply ACLs for traffic control.

Here is the complete configuration for the ISP router to ensure full connectivity between internal networks (e.g., 192.168.x.x) and external networks (like 209.165.201.30 and 209.165.202.158).

✅ ISP Router Configuration

Assuming:

You're not running EIGRP on the ISP router

You’re using static routes on the ISP router

Interface IPs (based on your setup):

S0/0/1 → 209.165.200.226/27 (connected to R2)

Fa0/0 → 209.165.201.1/27 (connected to Web Server)

Fa0/1 → 209.165.202.129/27 (connected to Outside Host)

Step 1: Interface Configuration

enable

configure terminal

interface Serial0/0/1

ip address 209.165.200.226 255.255.255.224

no shutdown

interface FastEthernet0/0

ip address 209.165.201.1 255.255.255.224

no shutdown

interface FastEthernet0/1

ip address 209.165.202.129 255.255.255.224

no shutdown

Step 2: Add Static Routes Back to Internal Networks

This tells the ISP router how to reach internal subnets via R2 (at 209.165.200.225):

ip route 192.168.10.0 255.255.255.0 209.165.200.225

ip route 192.168.11.0 255.255.255.0 209.165.200.225

ip route 192.168.20.0 255.255.255.0 209.165.200.225

ip route 192.168.30.0 255.255.255.0 209.165.200.225

These four static routes ensure that the ISP router knows how to forward replies back to PCs and routers in the LAN.

Step 3: (Optional) Default Route Toward Inside

If you want Web Server and Outside Host to access the LAN using a default route, and there's no NAT, you could add:

ip route 0.0.0.0 0.0.0.0 209.165.200.225

Step 4: Save Configuration

end

write memory

✅ **Final Check**

Run the following to confirm:

show ip route

show ip interface brief

ping 192.168.10.10 Test LAN connectivity

ping 209.165.201.30 ! Web Server

ping 209.165.202.158 ! Outside Host