1. DNS Server Configuration

Goal: Convert domain names (like www.xyz.com) into IP addresses.

Steps:

1. Place a **Server** → Click → **Config tab** → **DNS**.
2. Turn **DNS service ON**.
3. In "Name" → type your domain (e.g., www.xyz.com).
4. In "Address" → enter the web server's IP (e.g., 192.168.1.2).
5. Click **Add**.
6. On **Client PC** → Config → FastEthernet → set **Gateway & DNS Server IP**.
7. On PC → Desktop → Command Prompt → ping www.xyz.com.

✅ If reply is received → DNS works.

---

2. DHCP Server Configuration

Goal: Automatically assign IPs to devices.

Steps:

1. Add **Server** → Config tab → **DHCP**.
2. Turn **DHCP ON**.
3. Set:
    - **Pool Name:** LAN1
    - **Default Gateway:** Router Interface IP (e.g., 192.168.1.1)
    - **DNS Server:** DNS IP
    - **Start IP Address:** e.g., 192.168.1.10
    - **Subnet Mask:** e.g., 255.255.255.0
    - **Maximum Users:** e.g., 50
4. Click **Save**.
5. On PC → Config → FastEthernet → set to **DHCP**.
6. PC will automatically get an IP, Gateway, and DNS.

---

3. FTP Server Configuration

Goal: File Transfer between Client and Server.

Steps:

1. Server → Config tab → **FTP** → turn **ON**.

2. Add Username & Password (e.g., user1, pass123).
3. On PC → Desktop → Command Prompt:
4. ftp <server IP>
5. Username: user1
6. Password: pass123
7. Use commands like dir, get <file>, put <file>.

---

4. SMTP & POP3 (Mail Server)

Goal: Send and receive emails.

Steps:

1. Add **Server** → Config → **Email**.
2. Turn **SMTP & POP3 ON**.
3. Add users:
    - name: user1, domain: mail.com, password: pass123
4. On **Client PC** → Desktop → Email.
5. Configure:
    - **Display name:** User1
    - **Email address:** user1@mail.com
    - **Incoming Mail (POP3):** mail server IP
    - **Outgoing Mail (SMTP):** mail server IP
6. Test by sending emails between PCs.

---

5. Web Server Configuration (HTTP/HTTPS)

Goal: Host and access websites.

Steps:

1. Server → Config tab → **HTTP** → turn **ON**.
2. Optional: also enable **HTTPS**.
3. On PC → Desktop → Web Browser → type:
4. http://<web server IP>

   or if DNS configured:

   http://www.xyz.com

---

6. ACL (Access Control List) Configuration

Goal: Restrict or allow traffic.

Standard ACL (based on Source IP)

1. Go to Router → CLI.
2. Example:
3. R1(config)# access-list 1 deny 192.168.10.0 0.0.0.255
4. R1(config)# access-list 1 permit any
5. R1(config)# interface fa0/0
6. R1(config-if)# ip access-group 1 in

➞ Blocks 192.168.10.0 network from entering fa0/0.

● Extended ACL (based on Source, Destination, Protocol)

1. Example:
2. R1(config)# access-list 101 deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq www
3. R1(config)# access-list 101 permit ip any any
4. R1(config)# interface fa0/0
5. R1(config-if)# ip access-group 101 out

➞ Blocks HTTP traffic from students to teachers.

---

7. TELNET Configuration

Goal: Remote access to a router/switch.

Steps:

1. Router → CLI:
2. R1(config)# line vty 0 4
3. R1(config-line)# password cisco
4. R1(config-line)# login
5. R1(config)# enable password cisco
6. R1(config)# service password-encryption
7. On Client PC:
8. telnet <router IP>

✓ Router's command prompt will appear.

---

8. SSH Configuration

Goal: Secure remote access.

Steps:

1. Router → CLI:
2. R1(config)# hostname R1
3. R1(config)# ip domain-name cisco.com
4. R1(config)# crypto key generate rsa
5. (choose 1024 bits)
6. R1(config)# username admin password cisco
7. R1(config)# line vty 0 4
8. R1(config-line)# login local
9. R1(config-line)# transport input ssh
10. On PC:
11. ssh -l admin <router IP>

✅ SSH login successful if key generated and domain set.

BONUS – Checking Connections

Task	Command	Description
Check Interface IP	show ip interface brief	Displays assigned IPs
Routing Table	show ip route	Shows learned routes
Test Connectivity	ping <IP>	Verifies connection
View ACLs	show access-lists	Displays ACL rules
Telnet Users	show users	Shows active Telnet sessions

Excellent question 💪 — this is one of the *most asked* topics in CN labs and exams.
Let's break it down clearly:

Below are **all types of Extended ACL configurations** you need to know, with examples, explanations, and where to apply them 👇

🔰 1. Basic Extended ACL Syntax

access-list <number> permit|deny <protocol> <source> <wildcard> <destination> <wildcard> [eq <port>]

✅ **Range for extended ACLs:** 100–199 and 2000–2699
✅ Extended ACLs filter on **source + destination + protocol + port number**

⚙️ 2. Example Configurations

(a) Deny HTTP (Port 80) from one network to another

```
R1(config)# access-list 100 deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 80
R1(config)# access-list 100 permit ip any any
R1(config)# interface fa0/0
R1(config-if)# ip access-group 100 in
```

- Blocks all HTTP traffic from Students LAN (192.168.1.0) to Teachers LAN (192.168.2.0).
- Other traffic is allowed (because of the `permit ip any any` at end).

(b) Allow only ICMP (ping) between two networks

```
R1(config)# access-list 101 permit icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)# access-list 101 deny ip any any
R1(config)# interface fa0/1
R1(config-if)# ip access-group 101 out
```

- Only allows ping between two networks, denies everything else.

(c) Deny FTP access to a specific server

```
R1(config)# access-list 102 deny tcp any host 192.168.3.10 eq 21
R1(config)# access-list 102 permit ip any any
R1(config)# interface g0/0
R1(config-if)# ip access-group 102 in
```

- Denies FTP (port 21) traffic **to** 192.168.3.10 (the FTP server).
- All other protocols are still allowed.

(d) Allow only Web traffic (HTTP + HTTPS) to server

```
R1(config)# access-list 103 permit tcp any host 192.168.3.20 eq 80
R1(config)# access-list 103 permit tcp any host 192.168.3.20 eq 443
R1(config)# access-list 103 deny ip any any
R1(config)# interface g0/1
R1(config-if)# ip access-group 103 out
```

- Allows only HTTP/HTTPS access to web server (192.168.3.20).

(e) Block one specific PC from accessing entire network

```
R1(config)# access-list 104 deny ip host 192.168.1.10 192.168.2.0 0.0.0.255
R1(config)# access-list 104 permit ip any any
R1(config)# interface g0/0
R1(config-if)# ip access-group 104 in
```

🔹 Blocks one PC's IP (192.168.1.10) from accessing network 192.168.2.0.

(f) Deny Telnet traffic (Port 23)

```
R1(config)# access-list 105 deny tcp any any eq 23
R1(config)# access-list 105 permit ip any any
R1(config)# interface fa0/0
R1(config-if)# ip access-group 105 in
```

🔹 Denies all Telnet connections between networks.

(g) Deny SMTP (Mail) traffic

```
R1(config)# access-list 106 deny tcp any any eq 25
R1(config)# access-list 106 permit ip any any
R1(config)# interface fa0/1
R1(config-if)# ip access-group 106 out
```

🔹 Blocks SMTP (email sending) on port 25.

(h) Allow only a specific PC to access a Web Server

```
R1(config)# access-list 107 permit tcp host 192.168.1.10 host 192.168.2.20 eq 80
R1(config)# access-list 107 deny ip any any
R1(config)# interface fa0/0
R1(config-if)# ip access-group 107 in
```

🔹 Only PC 192.168.1.10 can access web server 192.168.2.20.

💡 3. Important Notes

Rule	Meaning
tcp	For web, ftp, telnet, ssh traffic
udp	For DNS, DHCP, TFTP
icmp	For ping
eq <port>	Filters specific service
any	Represents all IPs

Rule	Meaning
host <IP>	Represents a single host
in / out	Direction of ACL on interface

⚡ 4. Apply ACLs at Correct Place

ACL Type	Placement
Standard ACL	Near the **destination**
Extended ACL	Near the **source** (to filter early and save bandwidth)

Tip

Always end your ACL with:

```
permit ip any any
```

Otherwise, by default, *everything else* is denied (implicit deny rule).