Table of Contents

Introduction

This project simulates a comprehensive enterprise network design using Cisco Packet Tracer (version 9.0.0). The objective is to design a secure, scalable, and multi-protocol network environment that integrates IPv4 and IPv6 addressing, advanced switching technologies, dynamic routing, and layered security mechanisms.
The network is divided into two major domains:

Left Side (IPv4-only Domain)

Implements IPv4 subnetting using the `10.11.12.0/24` address space. This domain provides:

- DHCP services.
- Dynamic routing using OSPF (IPv4).
- Centralized management and security services, including NTP, Syslog, and AAA.

This side represents the internal enterprise network with strict access control and monitoring.

Right Side (Dual-Stack IPv4 & IPv6 Domain)

Supports both IPv4 and IPv6 addressing, utilizing the `2000:12:34::/64` IPv6 prefix alongside IPv4 networks. IPv6 addressing is implemented using SLAAC. Routing within this domain relies on OSPFv2 for IPv4 only, with no OSPFv3 deployment, as IPv6 connectivity is achieved through IPv6 tunneling over an IPv4 infrastructure.
This domain hosts enterprise services, including:

- DNS Server for name resolution.
- Web Server for HTTP/HTTPS services.
- Mail Server for enterprise email communication (SMTP, POP3).
- FTP Server for file transfer.

These servers are reachable securely from the internal and external networks based on defined security policies.

Security and Connectivity Features

To ensure strong connectivity and defense, the design incorporates:

- VLAN segmentation and Layer 2 security mechanisms such as 802.1X authentication, port security, DHCP snooping, and Dynamic ARP Inspection (DAI).
- Zone-Based Policy Firewall (ZPF) policies, Access Control Lists (ACLs), and Intrusion Prevention System (IPS) rules to enforce traffic control and protect against malicious activity.
- AAA authentication using TACACS+, RADIUS, and local authentication fallback, implementing role-based access control and customized privilege levels.

- Integration of a Cisco ASA firewall to provide DMZ protection, alongside wireless security controls for secure end-user access.
- A Site-to-Site IPSec VPN tunnel over IPv4, enabling secure communication between the two network domains.
- IPv6 tunneling across IPv4 hops, allowing end-to-end IPv6 communication through an IPv4-only routed backbone.

Objectives

Establish a Dual-Stack Network Environment

- Deploy IPv4 addressing (`10.11.12.0/24`) on the left-side network, right-side network and across inter-router links.
- Implement IPv6 addressing (`2000:12:34::/64`) on the right-side routers (R5–R8) and their LAN segments.
- Configure DHCP for IPv4 host address assignment.
- Configure IPv6 addressing using SLAAC.
- Enable IPv6 tunneling over IPv4, allowing IPv6 communication across IPv4-only routed hops.

Implement Secure Layer 2 Switching

- Configure VLANs for user traffic, management, and trunk links.
- Apply Layer 2 security features including:
  - 802.1X authentication.
  - Port security.
  - DHCP snooping.
  - Dynamic ARP Inspection (DAI).
  - Spanning Tree Protocol (STP) security mechanisms, including PortFast, BPDU Guard, to prevent topology manipulation and loops.
- Isolate unused switch ports into a blackhole VLAN.

Configure Dynamic Routing Protocols

- Deploy OSPF (IPv4) for dynamic routing on the left-side network.
- Use OSPF (IPv4) where required for IPv4 connectivity on the right side.
- IPv6 routing is achieved through tunneling mechanisms over IPv4.
- Configure static routing for networks located behind the ASA firewall.

Deploy Core Network Services

- Configure an authenticated NTP server for left-side network time synchronization.

- Configure a Syslog server to centrally collect and store logs from the left-side network.
- Configure Router R5 on the right-side network to act as an NTP server (Master).
- Deploy enterprise application servers on the right-side network / DMZ, including:
    - DNS Server for internal and external name resolution.
    - Web Server providing HTTP and HTTPS services.
    - Mail Server supporting enterprise email communication (SMTP, POP3).
    - FTP Server for file transfer.

Enhance Management Security

- Implement AAA authentication using TACACS+, RADIUS, and local database fallback.
- Configure role-based access control (RBAC) using privilege levels to enforce administrative separation.

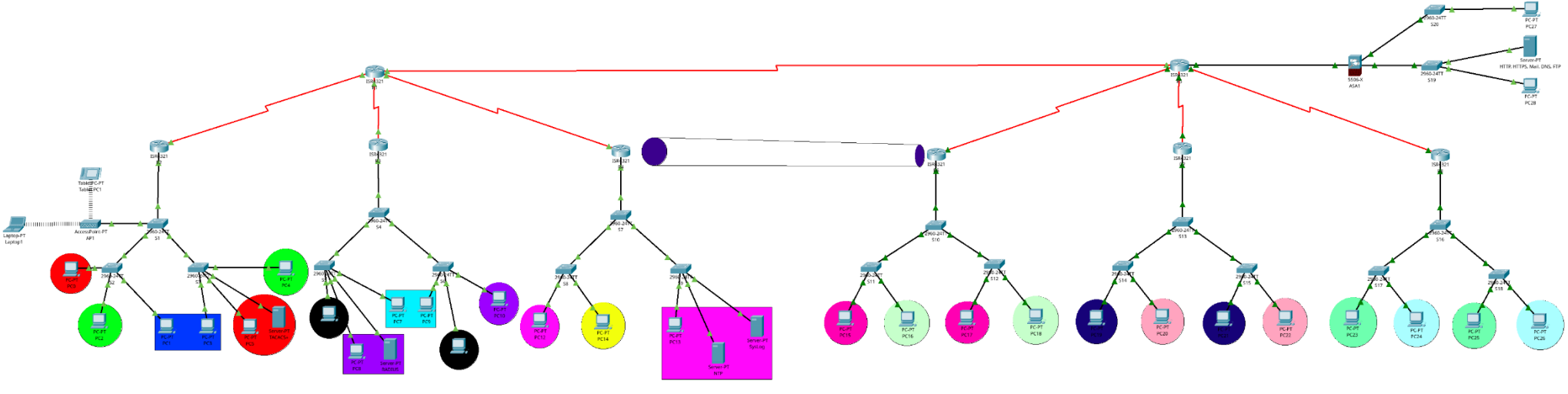
Strengthen Network Defense

- Configure a Zone-Based Policy Firewall (ZPF) on R1 to control ICMP, HTTP/HTTPS, DNS and FTP traffic.
- Deploy IOS IPS on R5 with stateful inspection, allowing traffic only when initiated from the inside network.
- Apply IPv6 ACLs on R7 to restrict unauthorized IPv6 inter-VLAN traffic.
- Configure the Cisco ASA firewall to protect the DMZ and server network by:
    - Applying security policies from INSIDE to DMZ to allow controlled internal access to servers.
    - Applying security policies from OUTSIDE to DMZ to permit only explicitly authorized public services.
- Secure wireless access using WPA2/WPA3 encryption.

Ensure Secure Inter-Site Connectivity

- Establish a Site-to-Site IPSec VPN tunnel over IPv4 between R4 and R6.
- Enable secure inter-domain communication between network segments using encrypted IPv4 transport.

Network Topology



IP Addressing Scheme

Global addressing summary

Type	Network	Notes
IPv4 Supernet	10.11.12.0 /24	Enterprise IPv4 space
IPv6 Global Prefix	2000:12:34:: /64	RHS VLANs (SLAAC)
IPv6 Tunnel Prefixes	2001:12:34:X:: /64	IPv6 over IPv4

Left side (L.H.S) – IPv4 only

Data VLANs

VLAN	Name	Network/Mask	Gateway	DHCP Range	Broadcast
10	IT	10.11.12.0 /29	10.11.12.1	10.11.12.3-6	10.11.12.7
20	Sales	10.11.12.8 /29	10.11.12.9	10.11.12.11-14	10.11.12.15
30	Support	10.11.12.16 /29	10.11.12.17	10.11.12.19-22	10.11.12.23
40	HR	10.11.12.24 /29	10.11.12.25	10.11.12.26-30	10.11.12.31
50	Managers	10.11.12.32 /29	10.11.12.33	10.11.12.34-38	10.11.12.39
60	Developers	10.11.12.40 /29	10.11.12.41	10.11.12.42-46	10.11.12.47
70	Finance	10.11.12.48 /29	10.11.12.49	10.11.12.50-54	10.11.12.55
80	Designers	10.11.12.56 /29	10.11.12.57	10.11.12.58-62	10.11.12.63
90	Access Points	10.11.12.64 /29	10.11.12.65	10.11.12.66-70	10.11.12.71

Management VLANs (Static)

VLAN	Network	Gateway	Assigned Devices
100	10.11.12.72 /29	10.11.12.73	Switch 1, 2, 3
110	10.11.12.80 /29	10.11.12.81	Switch 4, 5, 6
120	10.11.12.88 /29	10.11.12.89	Switch 7, 8, 9

Inter-Router IPv4 Links

Link	Network	Router A	Router B
R2–R1	10.11.12.200 /30	10.11.12.201	10.11.12.202
R3–R1	10.11.12.204 /30	10.11.12.205	10.11.12.206
R4–R1	10.11.12.208 /30	10.11.12.209	10.11.12.210
R1–R5	10.11.12.212 /30	10.11.12.213	10.11.12.214

Right side (R.H.S) – dual stack

Data VLANs (IPv4 + IPv6 SLAAC)

VLAN	Name	IPv4 Network	IPv4 GW	IPv6 Prefix	IPv6 GW
200	Instructors	10.11.12.96 /29	10.11.12.97	2000:12:34:200:: /64	::1
210	Researchers	10.11.12.104 /29	10.11.12.105	2000:12:34:210:: /64	::1
220	Graphics	10.11.12.112 /29	10.11.12.113	2000:12:34:220:: /64	::1
230	Branding	10.11.12.120 /29	10.11.12.121	2000:12:34:230:: /64	::1
240	Analysts	10.11.12.128 /29	10.11.12.129	2000:12:34:240:: /64	::1
250	Auditors	10.11.12.136 /29	10.11.12.137	2000:12:34:250:: /64	::1

Management VLANs (Dual Stack)

VLAN	IPv4 Network	IPv4 GW	IPv6 Prefix	IPv6 GW
260	10.11.12.144 /29	10.11.12.145	2000:12:34:260::/64	::1
270	10.11.12.152 /29	10.11.12.153	2000:12:34:270::/64	::1
280	10.11.12.160 /29	10.11.12.161	2000:12:34:280::/64	::1

Router Links (IPv4)

Link	Network	Router A	Router B
R6–R5	10.11.12.216 /30	10.11.12.217	10.11.12.218
R7–R5	10.11.12.220 /30	10.11.12.221	10.11.12.222
R8–R5	10.11.12.224 /30	10.11.12.225	10.11.12.226

IPv6 Tunnel Networks

Tunnel	IPv6 Prefix	Endpoint A	Endpoint B
Tunnel 0 (R6–R7)	2001:12:34:1::/64	::1	::2
Tunnel 1 (R6–R8)	2001:12:34:2::/64	::1	::2
Tunnel 2 (R7–R8)	2001:12:34:3::/64	::1	::2

Top right zone – ASA

ASA Interfaces

Interface	Network	IP Address
ASA ↔ R5 (OUTSIDE)	10.11.12.232 /29	10.11.12.234
ASA DMZ	10.11.12.184 /29	10.11.12.185
ASA INSIDE	10.11.12.192 /29	10.11.12.193

Configuration Steps

Switch S2

Step 1: Enter Privileged Mode and Global Configuration

This step prepares the switch for configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identification and Access Security

Set the hostname, banner, local user authentication, and enable secure remote access using SSH.

```
hostname S2

banner motd &#### Authorized Access Only ####&

username cisco privilege 15 secret cisco
enable secret cisco

service password-encryption
```

Step 3: Configure SSH for Secure Remote Management

Enable SSH by defining a domain name and generating RSA keys.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure console and VTY lines to use local authentication and allow only SSH.

```
line vty 0 4
login local
transport input ssh
```

```
exit

line console 0
login local
exit
```

Step 4: Create VLANs

Define VLANs for user traffic, management, trunking, and unused ports.

```
vlan 10
name IT
exit

vlan 20
name Sales
exit

vlan 30
name Support
exit

vlan 90
name Access-Point
exit

vlan 100
name Management
exit

vlan 205
name Unused-Ports
exit

vlan 201
name New-Native
exit
```

Step 5: Configure Access and Trunk Interfaces

Assign access ports to their respective VLANs.

```
interface fastEthernet 0/1
switchport mode access
```

```
switchport access vlan 10
exit

interface fastEthernet 0/2
switchport mode access
switchport access vlan 30
exit

interface fastEthernet 0/3
switchport mode access
switchport access vlan 20
exit
```

Configure the trunk interface with a non-default native VLAN and disable DTP.

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 10,20,30,90,100
switchport trunk native vlan 201
exit
```

Step 6: Configure Management VLAN Interface

Assign an IP address to the management VLAN and enable the interface.

```
interface vlan 100
ip address 10.11.12.74 255.255.255.248
no shutdown
exit
```

Set the default gateway for remote management.

```
ip default-gateway 10.11.12.73
```

Step 7: Secure Unused Ports

Move unused ports to a blackhole VLAN and shut them down.

```
interface range fastEthernet 0/4-24, gigabitEthernet 0/2
switchport access vlan 205
shutdown
exit
```

Step 8: Enable Port Security on Access Ports

Restrict each access port to a single device using sticky MAC addresses.

```
interface range fastEthernet 0/1-3
switchport port-security
switchport port-security maximum 1
```

```
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 9: Configure DHCP Snooping and Dynamic ARP Inspection

Protect the network against rogue DHCP servers and ARP spoofing.

```
ip dhcp snooping vlan 10,20,30,90
ip arp inspection vlan 10,20,30,90

ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface connected to the router or DHCP server.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Apply rate limiting and enable STP protection on access ports.

```
interface range fastEthernet 0/1-3
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 10: Configure IEEE 802.1X Authentication

Enable AAA and configure RADIUS-based authentication for port access control.

```
aaa new-model
radius-server host 10.11.12.34 key cisco

aaa authentication dot1x default group radius
dot1x system-auth-control
```

Apply 802.1X authentication on access ports.

```
interface range fastEthernet 0/1-3
authentication port-control auto
dot1x pae authenticator
exit
```

Step 11: Configure Logging and Time Synchronization

Enable timestamped logging for accurate event tracking.

```
service timestamps log datetime msec
```

Configure Syslog to send logs to the centralized server.

```
logging on
logging 10.11.12.51
```
Configure authenticated NTP for time synchronization.
```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```
Step 12: Save the Configuration

Ensure all changes are written to non-volatile memory.
```
do write
```
Switch S3

Step 1: Enter Privileged Mode and Global Configuration

Prepare the switch for configuration.
```
enable
configure terminal
```
Step 2: Configure Basic Device Identification and Local Security

Set the hostname, banner, local administrator account, and enable password encryption.
```
hostname S3

banner motd &#### Authorized Access Only ####&

username cisco privilege 15 secret cisco
enable secret cisco

service password-encryption
```
Step 3: Configure Secure Remote Management (SSH)

Enable SSH by configuring a domain name and generating RSA keys.
```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```
Configure console and VTY lines to use local authentication and allow only SSH access.
```
line vty 0 4
login local
transport input ssh
exit

line console 0
login local
```

```
exit
```

Step 4: Create VLANs

Define VLANs for user access, management, trunking, and unused ports.

```
vlan 10
name IT
exit

vlan 20
name Sales
exit

vlan 30
name Support
exit

vlan 90
name Access-Point
exit

vlan 100
name Management
exit

vlan 205
name Unused-Ports
exit

vlan 201
name New-Native
exit
```

Step 5: Configure Access and Trunk Interfaces

Assign access ports to their appropriate VLANs based on department requirements.

```
interface fastEthernet 0/1
switchport mode access
switchport access vlan 30
exit

interface fastEthernet 0/2
```

```
switchport mode access
switchport access vlan 20
exit

interface fastEthernet 0/3
switchport mode access
switchport access vlan 10
exit

interface fastEthernet 0/9
switchport mode access
switchport access vlan 10
exit
```

Configure the trunk interface with VLAN restrictions, a dedicated native VLAN, and disable DTP.

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 10,20,30,90,100
switchport trunk native vlan 201
exit
```

Step 6: Configure Management VLAN Interface

Assign an IP address to the management VLAN and enable the interface.

```
interface vlan 100
ip address 10.11.12.75 255.255.255.248
no shutdown
exit
```

Configure the default gateway for out-of-band management.

```
ip default-gateway 10.11.12.73
```

Step 7: Secure Unused Ports

Move all unused interfaces to a blackhole VLAN and administratively shut them down.

```
interface range fastEthernet 0/4-8, fastEthernet 0/10-24,
gigabitEthernet 0/2
switchport access vlan 205
shutdown
exit
```

Step 8: Enable Port Security on Access Ports

Restrict each access port to a single dynamically learned MAC address.

```
interface range fastEthernet 0/1-3, fastEthernet 0/9
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 9: Configure DHCP Snooping and Dynamic ARP Inspection

Enable Layer 2 protection against rogue DHCP servers and ARP spoofing attacks.

```
ip dhcp snooping vlan 10,20,30,90
ip arp inspection vlan 10,20,30,90

ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface connected to the router.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Apply rate limiting and STP protections on access ports.

```
interface range fastEthernet 0/1-3, fastEthernet 0/9
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 10: Configure IEEE 802.1X Port-Based Authentication

Enable AAA and configure RADIUS-based authentication for wired access control.

```
aaa new-model
radius-server host 10.11.12.34 key cisco

aaa authentication dot1x default group radius
dot1x system-auth-control
```

Apply 802.1X authentication to access ports.

```
interface range fastEthernet 0/1-3, fastEthernet 0/9
authentication port-control auto
dot1x pae authenticator
exit
```

Step 11: Configure Logging and Time Synchronization

Enable timestamped logging for accurate event correlation.

```
service timestamps log datetime msec
```

Send logs to the centralized Syslog server.

```
logging on
logging 10.11.12.51
```

Configure authenticated NTP for synchronized system time.

```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```

Step 12: Save the Configuration

Persist all configuration changes.

```
do write
```

Switch S1

Step 1: Enter Privileged Mode and Global Configuration

Access privileged EXEC mode and enter global configuration mode.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identification and Security

Define the hostname, login banner, local administrator credentials, and enable password encryption.

```
hostname S1

banner motd &#### Authorized Access Only ####&

username cisco privilege 15 secret cisco
enable secret cisco

service password-encryption
```

Step 3: Configure Secure Remote Management (SSH)

Enable SSH access by configuring the domain name and generating RSA keys.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure console and VTY lines to authenticate locally and accept only SSH connections.

```
line vty 0 4
login local
transport input ssh
```

```
exit

line console 0
login local
exit
```

Step 4: Create VLANs

Create VLANs for user access, wireless devices, management, trunking, and unused ports.

```
vlan 10
name IT
exit

vlan 20
name Sales
exit

vlan 30
name Support
exit

vlan 90
name Access-Point
exit

vlan 100
name Management
exit

vlan 205
name Unused-Ports
exit

vlan 201
name New-Native
exit
```

Step 5: Configure Trunk and Access Interfaces

Configure trunk links to access switches and upstream devices, restricting allowed VLANs and using a non-default native VLAN.

```
interface gigabitEthernet 0/1
```

```
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 10,20,30,90,100
switchport trunk native vlan 201
exit

interface gigabitEthernet 0/2
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 10,20,30,90,100
switchport trunk native vlan 201
exit

interface fastEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 10,20,30,90,100
switchport trunk native vlan 201
exit
```

Configure the access port connected to the wireless access point.

```
interface fastEthernet 0/3
switchport mode access
switchport access vlan 90
exit
```

Step 6: Configure Management VLAN Interface

Assign an IP address to the management VLAN SVI and bring it up.

```
interface vlan 100
ip address 10.11.12.76 255.255.255.248
no shutdown
exit
```

Configure the default gateway for management traffic.

```
ip default-gateway 10.11.12.73
```

Step 7: Secure Unused Interfaces

Place all unused ports into a blackhole VLAN and shut them down to prevent unauthorized access.

```
interface range fastEthernet 0/2, fastEthernet 0/4-24
switchport access vlan 205
shutdown
```

```
exit
```

Step 8: Enable Port Security on Access Ports

Apply port security on the access port connected to the wireless access point.

```
interface fastEthernet 0/3
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 9: Configure DHCP Snooping and Dynamic ARP Inspection

Enable Layer 2 protection mechanisms against DHCP spoofing and ARP poisoning.

```
ip dhcp snooping vlan 10,20,30,90
ip arp inspection vlan 10,20,30,90

ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust trunk interfaces connected to authorized DHCP sources.

```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Enable DHCP rate limiting and STP protections on access ports.

```
interface fastEthernet 0/3
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 10: Configure Logging and Time Synchronization

Enable precise log timestamps.

```
service timestamps log datetime msec
```

Send logs to the centralized Syslog server.

```
logging on
logging 10.11.12.51
```

Configure authenticated NTP for accurate time synchronization.

```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
```

```
ntp authentication-key 1 md5 cisco
```

Step 11: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

Router R2

Step 1: Enter Privileged Mode and Global Configuration

Access privileged EXEC mode, then enter global configuration mode.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identification and Security

Set the router hostname, define a warning banner, create a local administrative user, and secure the enable mode.

```
hostname R2

banner motd &##### Authorized Access Only ####&

username cisco privilege 15 secret cisco
enable secret cisco

service password-encryption
```

Step 3: Configure Secure Remote Management (SSH)

Enable SSH access by configuring the domain name and generating RSA encryption keys.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure console and VTY lines to authenticate using the local user database and allow only SSH access.

```
line vty 0 4
login local
transport input ssh
exit

line console 0
login local
exit
```

Step 4: Configure Inter-VLAN Routing (Router-on-a-Stick)

Create sub-interfaces on **GigabitEthernet 0/0/0** to provide default gateways for each VLAN using IEEE 802.1Q encapsulation.

VLAN 10 – IT

```
interface gigabitEthernet 0/0/0.10
encapsulation dot1Q 10
ip address 10.11.12.1 255.255.255.248
no shutdown
exit
```

VLAN 20 – Sales

```
interface gigabitEthernet 0/0/0.20
encapsulation dot1Q 20
ip address 10.11.12.9 255.255.255.248
no shutdown
exit
```

VLAN 30 – Support

```
interface gigabitEthernet 0/0/0.30
encapsulation dot1Q 30
ip address 10.11.12.17 255.255.255.248
no shutdown
exit
```

VLAN 90 – Access Point

```
interface gigabitEthernet 0/0/0.90
encapsulation dot1Q 90
ip address 10.11.12.65 255.255.255.248
no shutdown
exit
```

VLAN 100 – Management

```
interface gigabitEthernet 0/0/0.100
encapsulation dot1Q 100
ip address 10.11.12.73 255.255.255.248
no shutdown
exit
```

Enable the physical interface carrying all VLAN traffic.

```
interface gigabitEthernet 0/0/0
no shutdown
exit
```

Step 5: Configure WAN Serial Interface with OSPF Authentication

Assign an IP address to the serial interface and enable OSPF message-digest authentication for secure routing updates.

```
interface serial 0/1/1
```

```
ip address 10.11.12.201 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit
```

Step 6: Configure DHCPv4 Services

Exclude statically assigned gateway addresses from DHCP allocation.

```
ip dhcp excluded-address 10.11.12.1
ip dhcp excluded-address 10.11.12.2
ip dhcp excluded-address 10.11.12.9
ip dhcp excluded-address 10.11.12.17
ip dhcp excluded-address 10.11.12.65
```

Create DHCP pools for each VLAN to automatically assign IP addresses to clients.

VLAN 10 – IT

```
ip dhcp pool IT-VLAN-10
network 10.11.12.0 255.255.255.248
default-router 10.11.12.1
dns-server 10.11.12.235
exit
```

VLAN 20 – Sales

```
ip dhcp pool Sales-VLAN-20
network 10.11.12.8 255.255.255.248
default-router 10.11.12.9
dns-server 10.11.12.235
exit
```

VLAN 30 – Support

```
ip dhcp pool Support-VLAN-30
network 10.11.12.16 255.255.255.248
default-router 10.11.12.17
dns-server 10.11.12.235
exit
```

VLAN 90 – Access Point

```
ip dhcp pool Access_Point-VLAN-90
network 10.11.12.64 255.255.255.248
default-router 10.11.12.65
dns-server 10.11.12.235
exit
```

Step 7: Configure OSPFv2 Dynamic Routing

Enable OSPF process 1, assign a router ID, and advertise all connected networks in Area 0.

```
router ospf 1
router-id 2.2.2.2
network 10.11.12.0 0.0.0.7 area 0
network 10.11.12.8 0.0.0.7 area 0
network 10.11.12.16 0.0.0.7 area 0
network 10.11.12.64 0.0.0.7 area 0
network 10.11.12.72 0.0.0.7 area 0
network 10.11.12.200 0.0.0.3 area 0
exit
```

Step 8: Configure Privilege Level

Assign a limited privilege level to support users and permit basic troubleshooting commands.

```
privilege exec level 5 ping
username Support privilege 5 secret support
```

Step 9: Configure Logging and Time Synchronization

Enable precise log timestamps for troubleshooting and auditing.

```
service timestamps log datetime msec
```

Send logs to the centralized Syslog server.

```
logging on
logging 10.11.12.51
```

Configure authenticated NTP for accurate and secure time synchronization.

```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```

Step 10: Save the Configuration

Save the running configuration to NVRAM.

```
do write
```

Switch S5

Step 1: Enter Privileged and Global Configuration Modes

Access privileged EXEC mode and enter global configuration mode.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identification and Security

Assign a hostname, configure a warning banner, create a local administrative user, and secure privileged access.

```
hostname S5
```

```
banner motd &#### Authorized Access Only ####&

username cisco privilege 15 secret cisco
enable secret cisco

service password-encryption
```

Step 3: Enable Secure Remote Management (SSH)

Configure the domain name and generate RSA keys to enable SSH access.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure console and VTY lines to use local authentication and allow only SSH access.

```
line vty 0 4
login local
transport input ssh
exit

line console 0
login local
exit
```

Step 4: Create VLANs

Create and name VLANs to logically segment the network.

```
vlan 40
name HR
exit

vlan 50
name Managers
exit

vlan 60
name Developers
exit

vlan 110
name Management
exit
```

```
vlan 253
name Unused-Ports
exit

vlan 251
name New-Native
exit
```

Step 5: Configure Access Ports

Assign end-device ports to their corresponding VLANs.

```
interface fastEthernet 0/21
switchport mode access
switchport access vlan 40
exit

interface fastEthernet 0/10
switchport mode access
switchport access vlan 50
exit

interface fastEthernet 0/3
switchport mode access
switchport access vlan 50
exit

interface fastEthernet 0/23
switchport mode access
switchport access vlan 60
exit
```

Step 6: Configure Trunk Port

Configure the uplink port as a trunk, restrict allowed VLANs, disable DTP negotiation, and change the native VLAN for security.

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 40,50,60,110
switchport trunk native vlan 251
exit
```

Step 7: Configure Management VLAN Interface

Assign an IP address to the management VLAN to allow remote management of the switch.

```
interface vlan 110
ip address 10.11.12.82 255.255.255.248
no shutdown
exit
```

Step 8: Configure Default Gateway

Set the default gateway so the switch can communicate with devices outside its local subnet.

```
ip default-gateway 10.11.12.81
```

Step 9: Secure Unused Ports

Move all unused ports to a dedicated VLAN and shut them down to prevent unauthorized access.

```
interface range fastEthernet 0/1-2, fastEthernet 0/4-9,
fastEthernet 0/11-20, fastEthernet 0/22, fastEthernet 0/24,
gigabitEthernet 0/2
switchport access vlan 253
shutdown
exit
```

Step 10: Configure Port Security

Enable port security on user-facing access ports to limit the number of allowed MAC addresses and mitigate MAC flooding attacks.

```
interface range fastEthernet 0/3, fastEthernet 0/10,
fastEthernet 0/21, fastEthernet 0/23
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 11: Enable DHCP Snooping and Dynamic ARP Inspection

Protect the network against rogue DHCP servers and ARP spoofing attacks.

```
ip dhcp snooping vlan 40,50,60
ip arp inspection vlan 40,50,60
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface connected to the router or distribution switch.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
```

```
exit
```
Apply rate limiting and enable spanning-tree protections on access ports.
```
interface range fastEthernet 0/3, fastEthernet 0/10,
fastEthernet 0/21, fastEthernet 0/23
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```
Step 12: Configure 802.1X Port-Based Authentication

Enable AAA, configure the RADIUS server, and activate 802.1X authentication for enhanced access control.
```
aaa new-model
radius-server host 10.11.12.34 key cisco

aaa authentication dot1x default group radius
dot1x system-auth-control
```
Apply 802.1X authentication to selected access ports.
```
interface range fastEthernet 0/10, fastEthernet 0/21,
fastEthernet 0/23
authentication port-control auto
dot1x pae authenticator
exit
```
Step 13: Configure Logging and Time Synchronization

Enable detailed timestamps for log entries.
```
service timestamps log datetime msec
```
Send logs to the centralized Syslog server.
```
logging on
logging 10.11.12.51
```
Configure authenticated NTP to ensure accurate time synchronization.
```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```
Step 14: Save the Configuration

Save the running configuration to NVRAM.
```
do write
```

Switch S6

Step 1: Enter Privileged and Global Configuration Modes

Access privileged EXEC mode and enter global configuration mode.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identification and Security

Set the hostname, configure a warning banner, create a privileged local user, and secure passwords.

```
hostname S6

banner motd &#### Authorized Access Only ####&

username cisco privilege 15 secret cisco
enable secret cisco

service password-encryption
```

Step 3: Enable Secure Remote Management (SSH)

Configure the domain name and generate RSA keys to enable SSH access.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure console and VTY access using local authentication and restrict remote access to SSH only.

```
line vty 0 4
login local
transport input ssh
exit

line console 0
login local
exit
```

Step 4: Create VLANs

Define VLANs to segment users, management traffic, unused ports, and the native VLAN.

```
vlan 40
name HR
exit

vlan 50
name Managers
```

```
exit

vlan 60
name Developers
exit

vlan 110
name Management
exit

vlan 253
name Unused-Ports
exit

vlan 251
name New-Native
exit
```

Step 5: Configure Access Ports

Assign end-device ports to their appropriate VLANs.

```
interface fastEthernet 0/5
switchport mode access
switchport access vlan 60
exit

interface fastEthernet 0/3
switchport mode access
switchport access vlan 40
exit

interface fastEthernet 0/24
switchport mode access
switchport access vlan 50
exit
```

Step 6: Configure Trunk Port

Configure the uplink interface as a trunk, disable DTP negotiation, restrict allowed VLANs, and change the native VLAN for security.

```
interface gigabitEthernet 0/1
switchport mode trunk
```

```
switchport nonegotiate
switchport trunk allowed vlan 40,50,60,110
switchport trunk native vlan 251
exit
```

Step 7: Configure Management VLAN Interface

Assign an IP address to the management VLAN interface to enable remote management.

```
interface vlan 110
ip address 10.11.12.83 255.255.255.248
no shutdown
exit
```

Step 8: Configure Default Gateway

Set the default gateway to allow the switch to communicate outside its local subnet.

```
ip default-gateway 10.11.12.81
```

Step 9: Secure Unused Ports

Move all unused interfaces to a dedicated blackhole VLAN and administratively shut them down.

```
interface range fastEthernet 0/1-2, fastEthernet 0/4,
fastEthernet 0/6-23, gigabitEthernet 0/2
switchport access vlan 253
shutdown
exit
```

Step 10: Configure Port Security

Enable port security on access ports to restrict devices and prevent MAC flooding attacks.

```
interface range fastEthernet 0/3, fastEthernet 0/5, fastEthernet
0/24
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 11: Enable DHCP Snooping and Dynamic ARP Inspection

Protect the network from rogue DHCP servers and ARP spoofing attacks.

```
ip dhcp snooping vlan 40,50,60
ip arp inspection vlan 40,50,60
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface connected to the upstream device.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```
Apply rate limiting and spanning-tree protections on access ports.
```
interface range fastEthernet 0/3, fastEthernet 0/5, fastEthernet
0/24
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```
Step 12: Configure 802.1X Authentication

Enable AAA, configure the RADIUS server, and activate port-based authentication.
```
aaa new-model
radius-server host 10.11.12.34 key cisco

aaa authentication dot1x default group radius
dot1x system-auth-control
```
Apply 802.1X authentication to user-facing access ports.
```
interface range fastEthernet 0/3, fastEthernet 0/5, fastEthernet
0/24
authentication port-control auto
dot1x pae authenticator
exit
```
Step 13: Configure Logging and Time Synchronization

Enable detailed timestamps for log messages.
```
service timestamps log datetime msec
```
Forward logs to the centralized Syslog server.
```
logging on
logging 10.11.12.51
```
Configure authenticated NTP to ensure consistent time across the network.
```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```
Step 14: Save the Configuration

Save the running configuration to NVRAM.
```
do write
```

Switch S4

Step 1: Enter Privileged and Global Configuration Modes

Access privileged EXEC mode and enter global configuration mode.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identification and Security

Set the hostname, configure a legal warning banner, create a privileged local user, and secure device passwords.

```
hostname S4

banner motd &#### Authorized Access Only ####&

username cisco privilege 15 secret cisco
enable secret cisco

service password-encryption
```

Step 3: Enable Secure Remote Management (SSH)

Configure the domain name and generate RSA keys to enable SSH access.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure console and VTY lines to use local authentication and allow only SSH for remote access.

```
line vty 0 4
login local
transport input ssh
exit

line console 0
login local
exit
```

Step 4: Create VLANs

Define VLANs for users, management, unused ports, and a non-default native VLAN to enhance security.

```
vlan 40
name HR
exit

vlan 50
```

```
name Managers
exit

vlan 60
name Developers
exit

vlan 110
name Management
exit

vlan 253
name Unused-Ports
exit

vlan 251
name New-Native
exit
```

Step 5: Configure Trunk Interfaces

Configure uplink interfaces as trunks, disable DTP negotiation, restrict allowed VLANs, and change the native VLAN to prevent VLAN hopping attacks.

```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 40,50,60,110
switchport trunk native vlan 251
exit
```

Step 6: Configure Management VLAN Interface

Assign an IP address to the management VLAN interface to allow secure remote management of the switch.

```
interface vlan 110
ip address 10.11.12.84 255.255.255.248
no shutdown
exit
```

Step 7: Configure Default Gateway

Set the default gateway so the switch can communicate with devices outside its management subnet.

```
ip default-gateway 10.11.12.81
```

Step 8: Secure Unused Ports

Move all unused interfaces to a dedicated blackhole VLAN and shut them down to reduce the attack surface.

```
interface range fastEthernet 0/2-24
switchport access vlan 253
shutdown
exit
```

Step 9: Enable DHCP Snooping and Dynamic ARP Inspection

Protect the access layer against rogue DHCP servers and ARP spoofing attacks.

```
ip dhcp snooping vlan 40,50,60
ip arp inspection vlan 40,50,60
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust uplink trunk interfaces connected to upstream switches or routers.

```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Step 10: Configure Logging and Time Synchronization

Enable precise timestamps for log messages.

```
service timestamps log datetime msec
```

Send logs to the centralized Syslog server.

```
logging on
logging 10.11.12.51
```

Configure authenticated NTP to ensure consistent time across the network.

```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```

Step 11: Save the Configuration

Save the running configuration to NVRAM.

```
do write
```

Router R3

Step 1: Enter Privileged and Global Configuration Modes

Access privileged EXEC mode and enter global configuration mode.

```
enable
```

```
configure terminal
```

Step 2: Configure Basic Device Identification and Security

Set the router hostname, configure a security banner, create a privileged local user, and secure stored passwords.

```
hostname R3

banner motd &#### Authorized Access Only ####&

username cisco privilege 15 secret cisco
enable secret cisco

service password-encryption
```

Step 3: Enable Secure Remote Management (SSH)

Configure the domain name and generate RSA keys to enable SSH access.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure console and VTY lines to use local authentication and restrict remote access to SSH only.

```
line vty 0 4
login local
transport input ssh
exit

line console 0
login local
exit
```

Step 4: Configure Router-on-a-Stick Sub-Interfaces

Create 802.1Q sub-interfaces to provide inter-VLAN routing for HR, Managers, Developers, and Management VLANs.

```
interface gigabitEthernet 0/0/0.40
encapsulation dot1Q 40
ip address 10.11.12.25 255.255.255.248
no shutdown
exit

interface gigabitEthernet 0/0/0.50
encapsulation dot1Q 50
ip address 10.11.12.33 255.255.255.248
```

```
no shutdown
exit

interface gigabitEthernet 0/0/0.60
encapsulation dot1Q 60
ip address 10.11.12.41 255.255.255.248
no shutdown
exit

interface gigabitEthernet 0/0/0.110
encapsulation dot1Q 110
ip address 10.11.12.81 255.255.255.248
no shutdown
exit
```

Enable the physical interface connected to the trunk link.

```
interface gigabitEthernet 0/0/0
no shutdown
exit
```

Step 5: Configure WAN Interface and OSPF Authentication

Assign an IP address to the serial WAN interface and enable OSPF MD5 authentication to secure routing updates.

```
interface serial 0/1/0
ip address 10.11.12.205 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit
```

Step 6: Configure DHCPv4 Services

Exclude reserved IP addresses and configure DHCP pools for VLANs served by R3.

```
ip dhcp excluded-address 10.11.12.25
ip dhcp excluded-address 10.11.12.33
ip dhcp excluded-address 10.11.12.34
ip dhcp excluded-address 10.11.12.40
```

Configure DHCP pools.

```
ip dhcp pool HR-VLAN-40
network 10.11.12.24 255.255.255.248
default-router 10.11.12.25
dns-server 10.11.12.235
```

```
exit

ip dhcp pool Managers-VLAN-50
network 10.11.12.32 255.255.255.248
default-router 10.11.12.33
dns-server 10.11.12.235
exit

ip dhcp pool Developers-VLAN-60
network 10.11.12.40 255.255.255.248
default-router 10.11.12.41
dns-server 10.11.12.235
exit
```

Step 7: Configure OSPFv2 Dynamic Routing

Enable OSPF, assign a router ID, and advertise all connected VLAN and WAN networks into Area 0.

```
router ospf 1
router-id 3.3.3.3
network 10.11.12.24 0.0.0.7 area 0
network 10.11.12.32 0.0.0.7 area 0
network 10.11.12.40 0.0.0.7 area 0
network 10.11.12.80 0.0.0.7 area 0
network 10.11.12.204 0.0.0.3 area 0
exit
```

Step 8: Configure AAA Authentication (TACACS+ and RADIUS)

Enable AAA and configure TACACS+ and RADIUS servers for centralized authentication with local fallback.

```
aaa new-model

tacacs-server host 10.11.12.2 single-connection key cisco

radius server SERVER-R
address ipv4 10.11.12.34 auth-port 1645
key cisco
exit
```

Apply the authentication method list.

```
aaa authentication login default group tacacs+ group radius
local
```

Step 9: Configure Logging and Time Synchronization

Enable detailed timestamps for log messages.

```
service timestamps log datetime msec
```

Send logs to the centralized Syslog server.

```
logging on
logging 10.11.12.51
```

Configure authenticated NTP for time synchronization.

```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```

Step 10: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

Switch S8

Step 1: Enter Privileged and Global Configuration Mode

The initial step is to access privileged EXEC mode and then enter global configuration mode to start configuring the switch.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Set the hostname, configure a login banner to warn unauthorized users, and create a local administrative user with full privileges.

```
hostname S8
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption to protect stored credentials.

```
service password-encryption
```

Step 3: Enable SSH for Secure Remote Management

Configure the domain name and generate RSA keys to allow secure SSH access to the switch.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines to use local authentication and allow only SSH connections.

```
line vty 0 4
login local
transport input ssh
exit
```

Configure console access to use local authentication.

```
line console 0
login local
exit
```

Set an encrypted enable password.

```
enable secret cisco
```

Step 4: Create and Name VLANs

Define VLANs to logically segment the network based on department roles and security requirements.

```
vlan 70
name Finance
exit

vlan 80
name Designers
exit

vlan 120
name Management
exit

vlan 276
name Unused-Ports
exit

vlan 271
name New-Native
exit
```

Step 5: Configure Access Ports for End Devices

Assign access ports to their respective VLANs to connect user devices.

```
interface fastEthernet 0/22
switchport mode access
switchport access vlan 70
exit

interface fastEthernet 0/23
switchport mode access
switchport access vlan 80
```

```
exit
```

Step 6: Configure Trunk Port to the Distribution Layer

Configure the trunk link to carry multiple VLANs securely and change the native VLAN for security hardening.

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 70,80,120
switchport trunk native vlan 271
exit
```

Step 7: Configure Management VLAN Interface (SVI)

Assign an IP address to the management VLAN interface to enable remote management of the switch.

```
interface vlan 120
ip address 10.11.12.90 255.255.255.248
no shutdown
exit
```

Configure the default gateway to allow management traffic to reach other networks.

```
ip default-gateway 10.11.12.89
```

Step 8: Secure Unused Ports

Move all unused ports into a dedicated VLAN and shut them down to prevent unauthorized access.

```
interface range fastEthernet 0/1-21, fastEthernet 0/24,
gigabitEthernet 0/2
switchport access vlan 276
shutdown
exit
```

Step 9: Enable Port Security on Access Ports

Apply port security to limit the number of MAC addresses and prevent unauthorized devices.

```
interface range fastEthernet 0/22-23
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 10: Enable DHCP Snooping and Dynamic ARP Inspection (DAI)

Enable DHCP Snooping and ARP Inspection to protect against DHCP spoofing and ARP poisoning attacks.

```
ip dhcp snooping vlan 70,80
ip arp inspection vlan 70,80
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Mark the trunk port as trusted for DHCP and ARP traffic.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Limit DHCP request rates and enable STP protections on access ports.

```
interface range fastEthernet 0/22-23
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 11: Configure IEEE 802.1X Port-Based Authentication

Enable AAA services and configure the RADIUS server for centralized authentication.

```
aaa new-model
radius-server host 10.11.12.34 key cisco
aaa authentication dot1x default group radius
```

Enable 802.1X globally on the switch.

```
dot1x system-auth-control
```

Apply 802.1X authentication to user-facing access ports.

```
interface range fastEthernet 0/22-23
authentication port-control auto
dot1x pae authenticator
exit
```

Step 12: Configure Logging and Time Synchronization

Enable timestamping on logs for accurate event tracking.

```
service timestamps log datetime msec
```

Configure a Syslog server to centralize logging.

```
logging on
logging 10.11.12.51
```

Synchronize the switch clock with an authenticated NTP server.

```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
```

```
ntp authentication-key 1 md5 cisco
```

Step 13: Save the Configuration

Finally, save the running configuration to ensure persistence after a reboot.

```
do write
```

Switch S9

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration mode to begin configuring the switch.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign a hostname to the switch, configure a security banner to warn unauthorized users, and create a local administrative account with full privileges.

```
hostname S9
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
Enable password encryption to secure stored credentials.
service password-encryption
```

Step 3: Enable Secure Remote Management Using SSH

Define the domain name and generate RSA keys to enable SSH-based secure remote access.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure the VTY lines to use local authentication and restrict remote access to SSH only.

```
line vty 0 4
login local
transport input ssh
exit
```

Configure console access to authenticate using the local user database.

```
line console 0
login local
exit
```

Set an encrypted enable secret for privileged mode access.

```
enable secret cisco
```

Step 4: Create and Name VLANs

Create VLANs to segment the network based on organizational roles and security requirements.

```
vlan 70
name Finance
```

```
exit

vlan 80
name Desginers
exit

vlan 120
name Management
exit

vlan 276
name Unused-Ports
exit

vlan 271
name New-Native
exit
```

Step 5: Configure Access Ports for End Devices

Assign selected FastEthernet ports to VLAN 70 to connect Finance department end devices.

```
interface range fastEthernet 0/22, fastEthernet 0/3,
fastEthernet 0/1
switchport mode access
switchport access vlan 70
exit
```

Step 6: Configure Trunk Port to the Distribution Layer

Configure the trunk port to carry multiple VLANs securely and harden it by disabling DTP and changing the native VLAN.

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 70,80,120
switchport trunk native vlan 271
exit
```

Step 7: Configure Management VLAN Interface (SVI)

Configure a switched virtual interface (SVI) for the management VLAN to allow remote management of the switch.

```
interface vlan 120
ip address 10.11.12.91 255.255.255.248
```

```
no shutdown
exit
```
Define the default gateway to allow management traffic to reach external networks.
```
ip default-gateway 10.11.12.89
```
Step 8: Secure Unused Switch Ports

Move all unused ports into a dedicated VLAN and administratively shut them down to prevent unauthorized access.
```
interface range fastEthernet 0/2, fastEthernet 0/4-21,
fastEthernet 0/23-24, gigabitEthernet 0/2
switchport access vlan 276
shutdown
exit
```
Step 9: Enable Port Security on User Access Ports

Apply port security to restrict each access port to a single learned MAC address and define the violation behavior.
```
interface range fastEthernet 0/1, fastEthernet 0/3, fastEthernet
0/22
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```
Step 10: Enable DHCP Snooping and Dynamic ARP Inspection (DAI)

Enable DHCP Snooping and ARP Inspection on user VLANs to protect against DHCP spoofing and ARP poisoning attacks.
```
ip dhcp snooping vlan 70,80
ip arp inspection vlan 70,80
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```
Mark the trunk port as trusted to allow legitimate DHCP and ARP traffic.
```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```
Apply DHCP rate limiting and enable spanning tree protections on access ports.
```
interface range fastEthernet 0/1, fastEthernet 0/3, fastEthernet
0/22
```

```
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 11: Configure IEEE 802.1X Port-Based Authentication

Enable the AAA framework and configure the RADIUS server for centralized authentication.

```
aaa new-model
radius-server host 10.11.12.34 key cisco
aaa authentication dot1x default group radius
```

Enable 802.1X globally on the switch.

```
dot1x system-auth-control
```

Apply 802.1X authentication to the user-facing access ports.

```
interface range fastEthernet 0/1, fastEthernet 0/3, fastEthernet
0/22
authentication port-control auto
dot1x pae authenticator
exit
```

Step 12: Configure Logging and Time Synchronization

Enable detailed timestamps on logs to improve troubleshooting and auditing.

```
service timestamps log datetime msec
```

Configure a centralized Syslog server to collect and store logs.

```
logging on
logging 10.11.12.51
```

Synchronize system time using an authenticated NTP server.

```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```

Step 13: Save the Configuration

Save the running configuration to non-volatile memory to ensure persistence after a reboot.

```
do write
```

Switch S7

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and move into global configuration mode to begin device setup.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign a hostname to uniquely identify the switch, configure a warning banner, and create a privileged local user.

```
hostname S7
banner motd &##### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption to protect all stored credentials.

```
service password-encryption
```

Step 3: Enable Secure Remote Access Using SSH

Define the domain name and generate RSA keys to enable SSH for secure remote management.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines to use local authentication and allow SSH access only.

```
line vty 0 4
login local
transport input ssh
exit
```

Configure console access to authenticate using the local user database.

```
line console 0
login local
exit
```

Configure an encrypted enable secret for privileged mode access.

```
enable secret cisco
```

Step 4: Create and Name VLANs

Create VLANs to logically segment the network based on department roles and security requirements.

```
vlan 70
name Finance
exit

vlan 80
name Desginers
exit

vlan 120
name Management
exit

vlan 276
```

```
name Unused-Ports
exit

vlan 271
name New-Native
exit
```

Step 5: Configure Trunk Interfaces

Configure trunk links toward the distribution/core layer to carry multiple VLANs securely, disable DTP negotiation, and change the native VLAN.

```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 70,80,120
switchport trunk native vlan 271
exit
```

Step 6: Configure Management VLAN Interface (SVI)

Configure the switched virtual interface (SVI) for the management VLAN to allow remote management access to the switch.

```
interface vlan 120
ip address 10.11.12.92 255.255.255.248
no shutdown
exit
```

Define the default gateway to allow management traffic to reach external networks.

```
ip default-gateway 10.11.12.89
```

Step 7: Secure Unused Switch Ports

Move all unused access ports into a dedicated VLAN and shut them down to prevent unauthorized access.

```
interface range fastEthernet 0/2-24
switchport access vlan 276
shutdown
exit
```

Step 8: Enable DHCP Snooping and Dynamic ARP Inspection (DAI)

Enable DHCP Snooping and Dynamic ARP Inspection on user VLANs to protect against DHCP spoofing and ARP poisoning attacks.

```
ip dhcp snooping vlan 70,80
ip arp inspection vlan 70,80
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
```

```
ip arp inspection validate ip
```
Mark trunk interfaces as trusted to allow legitimate DHCP and ARP traffic.
```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```
Step 9: Configure Logging and Time Synchronization
Enable precise timestamps for system logs to support monitoring and troubleshooting.
```
service timestamps log datetime msec
```
Configure centralized logging by forwarding logs to the Syslog server.
```
logging on
logging 10.11.12.51
```
Synchronize system time using an authenticated NTP server.
```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```
Step 10: Save the Configuration
Save the running configuration to ensure all settings persist after a reboot.
```
do write
```

Router R4

Step 1: Enter Privileged and Global Configuration Mode
Access privileged EXEC mode, then enter global configuration mode to start configuring the router.
```
enable
configure terminal
```
Step 2: Configure Basic Device Identity and Security
Assign a hostname to the router, configure a legal warning banner, and create a privileged local user account.
```
hostname R4
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```
Enable password encryption to secure all plaintext passwords.
```
service password-encryption
```
Step 3: Enable Secure Remote Access Using SSH
Configure the domain name and generate RSA keys to enable SSH access.
```
ip domain-name cisco.local
```

```
crypto key generate rsa general-keys modulus 1024
```
Configure VTY lines to authenticate using the local user database and allow only SSH access.
```
line vty 0 4
login local
transport input ssh
exit
```
Configure console access to use local authentication.
```
line console 0
login local
exit
```
Configure an encrypted enable secret for privileged access.
```
enable secret cisco
```
Step 4: Configure Router-on-a-Stick Sub-Interfaces

Configure sub-interfaces on the Gigabit Ethernet interface to enable inter-VLAN routing using IEEE 802.1Q encapsulation.
```
interface gigabitEthernet 0/0/0.70
encapsulation dot1Q 70
ip address 10.11.12.49 255.255.255.248
no shutdown
exit

interface gigabitEthernet 0/0/0.80
encapsulation dot1Q 80
ip address 10.11.12.57 255.255.255.248
no shutdown
exit

interface gigabitEthernet 0/0/0.120
encapsulation dot1Q 120
ip address 10.11.12.89 255.255.255.248
no shutdown
exit
```
Enable the physical Gigabit Ethernet interface.
```
interface gigabitEthernet 0/0/0
no shutdown
exit
```
Step 5: Configure WAN Serial Interface with OSPF Authentication

Configure the serial interface for WAN connectivity and enable OSPF MD5 authentication to secure routing updates.

```
interface serial 0/1/0
ip address 10.11.12.209 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit
```

Step 6: Configure DHCPv4 Services

Exclude gateway and infrastructure addresses from DHCP allocation.

```
ip dhcp excluded-address 10.11.12.49
ip dhcp excluded-address 10.11.12.50
ip dhcp excluded-address 10.11.12.51
ip dhcp excluded-address 10.11.12.57
ip dhcp excluded-address 10.11.12.89
```

Create DHCP pools for Finance and Designers VLANs and specify their default gateways.

```
ip dhcp pool Finance-VLAN-70
network 10.11.12.48 255.255.255.248
default-router 10.11.12.49
dns-server 10.11.12.235
exit

ip dhcp pool Desginers-VLAN-80
network 10.11.12.56 255.255.255.248
default-router 10.11.12.57
dns-server 10.11.12.235
exit
```

Step 7: Enable OSPFv2 Dynamic Routing

Enable OSPFv2, assign a router ID, and advertise all connected networks into Area 0.

```
router ospf 1
router-id 4.4.4.4
network 10.11.12.48 0.0.0.7 area 0
network 10.11.12.56 0.0.0.7 area 0
network 10.11.12.88 0.0.0.7 area 0
network 10.11.12.208 0.0.0.3 area 0
exit
```

Step 8: Configure AAA Authentication

Enable AAA and configure both TACACS+ and RADIUS servers for centralized authentication with local fallback.

```
aaa new-model
tacacs-server host 10.11.12.2 single-connection key cisco
```

Configure the RADIUS server.

```
radius server SERVER-R
address ipv4 10.11.12.34 auth-port 1645
key cisco
exit
```

Apply the authentication method list.

```
authentication login default group radius group tacacs+ local
```

Step 9: Configure IPsec Site-to-Site VPN

9.1 Configure ISAKMP (IKE Phase 1) Policy

Define the ISAKMP policy parameters for secure key exchange.

```
crypto isakmp policy 1
group 5
authentication pre-share
hash sha
encryption aes
lifetime 3600
exit
```

Configure the pre-shared key for the remote peer.

```
crypto isakmp key cisco address 10.11.12.217
```

9.2 Define Interesting Traffic Using an Access Control List

Specify the networks that should be encrypted through the VPN tunnel.

```
ip access-list extended VPN-Connection
permit ip 10.11.12.48 0.0.0.7 10.11.12.96 0.0.0.7
permit ip 10.11.12.48 0.0.0.7 10.11.12.104 0.0.0.7
permit ip 10.11.12.48 0.0.0.7 10.11.12.144 0.0.0.7
permit ip 10.11.12.56 0.0.0.7 10.11.12.96 0.0.0.7
permit ip 10.11.12.56 0.0.0.7 10.11.12.104 0.0.0.7
permit ip 10.11.12.56 0.0.0.7 10.11.12.144 0.0.0.7
permit ip 10.11.12.88 0.0.0.7 10.11.12.96 0.0.0.7
permit ip 10.11.12.88 0.0.0.7 10.11.12.104 0.0.0.7
permit ip 10.11.12.88 0.0.0.7 10.11.12.144 0.0.0.7
exit
```

9.3 Configure IPsec Phase 2 Parameters

Define the IPsec transform set.

```
crypto ipsec transform-set R4-R6 esp-aes
```
Create and configure the crypto map.
```
crypto map R4-R6_MAP 10 ipsec-isakmp
match address VPN-Connection
set transform-set R4-R6
set peer 10.11.12.217
set pfs group5
set security-association lifetime seconds 900
exit
```
Apply the crypto map to the WAN interface.
```
interface serial 0/1/0
crypto map R4-R6_MAP
exit
```
Step 10: Configure Logging and Time Synchronization

Enable timestamping for system logs.
```
service timestamps log datetime msec
```
Configure centralized Syslog logging.
```
logging on
logging 10.11.12.51
```
Configure authenticated NTP for time synchronization.
```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```
Step 11: Save the Configuration

Save the running configuration to non-volatile memory.
```
do write
```
Router R1

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration mode.
```
enable
configure terminal
```
Step 2: Configure Basic Device Identity and Security

Assign the hostname, configure a warning banner, and create a privileged local user.
```
hostname R1
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption for all plaintext passwords.

```
service password-encryption
```

Step 3: Enable Secure Remote Management (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Restrict VTY access to SSH only and authenticate using the local user database.

```
line vty 0 4
login local
transport input ssh
exit
```

Configure console access authentication.

```
line console 0
login local
exit
```

Configure an encrypted enable secret.

```
enable secret cisco
```

Step 4: Configure WAN Serial Interfaces with OSPF Authentication

Configure all serial interfaces connecting to other routers. Each interface uses IP addressing and OSPF MD5 authentication to protect routing updates.

```
interface serial 0/1/1
ip address 10.11.12.202 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit

interface serial 0/2/1
ip address 10.11.12.210 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit

interface serial 0/2/0
ip address 10.11.12.206 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
```

```
no shutdown
exit

interface serial 0/1/0
ip address 10.11.12.213 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit
```

Step 5: Enable OSPFv2 Dynamic Routing

Enable OSPFv2, assign a unique router ID, and advertise all WAN networks into Area 0.

```
router ospf 1
router-id 1.1.1.1
network 10.11.12.200 0.0.0.3 area 0
network 10.11.12.208 0.0.0.3 area 0
network 10.11.12.204 0.0.0.3 area 0
network 10.11.12.212 0.0.0.3 area 0
exit
```

Step 6: Configure Zone-Based Policy Firewall (ZPF)

Create security zones to separate trusted internal traffic from external traffic.

```
zone security IN
exit
zone security OUT
exit
```

Step 7: Define Traffic Classification for Firewall Policies

Create a class map to match common inside-to-outside protocols.

```
class-map type inspect match-any CLASS_IN2OUT
match protocol icmp
match protocol http
match protocol https
match protocol ftp
match protocol dns
exit
```

Create an access control list to allow IPsec-related traffic.

```
ip access-list extended ACL_IPsec
permit udp any any eq 500
permit udp any any eq 4500
permit esp any any
```

```
exit
```
Match the IPsec traffic using a class map.
```
class-map type inspect match-any CLASS-IPsec
match access-group name ACL_IPsec
exit
```
Step 8: Create Zone-Based Firewall Policies

Define the policy for traffic flowing from the inside zone to the outside zone.
```
policy-map type inspect POLICY_IN2OUT
class CLASS-IPsec
pass
class CLASS_IN2OUT
inspect
exit
exit
```
Define the policy for traffic flowing from the outside zone to the inside zone.
```
policy-map type inspect POLICY_OUT2IN
class CLASS-IPsec
pass
exit
exit
```
Step 9: Apply Firewall Policies Using Zone Pairs

Bind the security policies to zone pairs.
```
zone-pair security PAIR_IN2OUT source IN destination OUT
service-policy type inspect POLICY_IN2OUT
exit

zone-pair security PAIR_OUT2IN source OUT destination IN
service-policy type inspect POLICY_OUT2IN
exit
```
Step 10: Assign Interfaces to Security Zones

Assign each serial interface to its appropriate security zone.
```
interface serial 0/1/1
zone-member security IN
exit

interface serial 0/2/0
zone-member security IN
exit
```

```
interface serial 0/2/1
zone-member security IN
exit

interface serial 0/1/0
zone-member security OUT
exit
```

Step 11: Configure Logging and Time Synchronization

Enable timestamping for system logs.

```
service timestamps log datetime msec
```

Configure centralized Syslog logging.

```
logging on
logging 10.11.12.51
```

Configure authenticated NTP to ensure accurate time synchronization.

```
ntp server 10.11.12.50
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 cisco
```

Step 12: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

Switch S11

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration mode.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the hostname, configure a warning banner, and create a privileged local user.

```
hostname S11
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption to secure stored credentials.

```
service password-encryption
```

Step 3: Enable Secure Remote Management (SSH)

Configure the domain name and generate RSA keys required for SSH access.

```
ip domain-name cisco.local
```

```
crypto key generate rsa general-keys modulus 1024
```
Restrict VTY access to SSH only and authenticate using the local user database.
```
line vty 0 4
login local
transport input ssh
exit
```
Enable console access authentication.
```
line console 0
login local
exit
```
Configure an encrypted enable secret.
```
enable secret cisco
```
Step 4: Create VLANs for Network Segmentation

Create VLANs to logically separate user groups, management traffic, unused ports, and the native VLAN.
```
vlan 200
name Instructors
exit

vlan 210
name Researchers
exit

vlan 260
name Management
exit

vlan 300
name Unused-Ports
exit

vlan 305
name New-Native
exit
```
Step 5: Configure Access and Trunk Ports

Assign access ports to their respective VLANs.
```
interface fastEthernet 0/23
switchport mode access
```

```
switchport access vlan 200
exit

interface fastEthernet 0/20
switchport mode access
switchport access vlan 210
exit
```

Configure the trunk port with a restricted VLAN list and a secure native VLAN.

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 200,210,260
switchport trunk native vlan 305
exit
```

Step 6: Enable IPv6 Support (Dual-Stack Operation)

Change the SDM template to support IPv4 and IPv6, save the configuration, and reload the switch.

```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```

After reload, enable IPv6 routing globally.

```
ipv6 unicast-routing
```

Step 7: Configure Management VLAN with IPv4 and IPv6

Assign both IPv4 and IPv6 addresses to the management VLAN interface.

```
interface vlan 260
ip address 10.11.12.146 255.255.255.248
ipv6 address 2000:12:34:260::2/64
ipv6 enable
no shutdown
exit
```

Step 8: Configure Default Gateways

Configure the IPv6 default route for management traffic.

```
ipv6 route ::/0 2000:12:34:260::1
```

Configure the IPv4 default gateway for switch management.

```
ip default-gateway 10.11.12.145
```

Step 9: Isolate and Disable Unused Ports

Move all unused interfaces to a dedicated blackhole VLAN and shut them down.

```
interface range fastEthernet 0/1-19, fastEthernet 0/21-22,
fastEthernet 0/24, gigabitEthernet 0/2
switchport access vlan 300
shutdown
exit
```

Step 10: Enable Port Security on Access Ports

Restrict each access port to a single learned MAC address using sticky MAC learning.

```
interface range fastEthernet 0/20, fastEthernet 0/23
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 11: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection (DAI) to protect against spoofing attacks.

```
ip dhcp snooping vlan 200,210
ip arp inspection vlan 200,210
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface connected to the router or core switch.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Step 12: Apply STP Protection and Rate Limiting

Enable PortFast, BPDU Guard, and limit DHCP request rates on access ports.

```
interface range fastEthernet 0/20, fastEthernet 0/23
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 13: Configure Logging and Time Synchronization

Enable timestamps for system logs.

```
service timestamps log datetime msec
```

Configure NTP for accurate time synchronization.

```
ntp server 10.11.12.218
```

Step 14: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

Switch S12

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration mode.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Set the switch hostname, configure a legal warning banner, and create a privileged local user.

```
hostname S12
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH access.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Restrict VTY access to SSH and authenticate using the local database.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable console authentication.

```
line console 0
login local
exit
```

Configure an encrypted enable password.

```
enable secret cisco
```

Step 4: Create VLANs

Create VLANs for user segmentation, management, unused ports, and a secure native VLAN.

```
vlan 200
name Instructors
exit

vlan 210
```

```
name Researchers
exit

vlan 260
name Management
exit

vlan 300
name Unused-Ports
exit

vlan 305
name New-Native
exit
```

Step 5: Configure Access and Trunk Interfaces

Assign access ports to their respective VLANs.

```
interface fastEthernet 0/22
switchport mode access
switchport access vlan 200
exit

interface fastEthernet 0/21
switchport mode access
switchport access vlan 210
exit
```

Configure the trunk interface with VLAN restrictions and disable DTP.

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 200,210,260
switchport trunk native vlan 305
exit
```

Step 6: Enable Dual-Stack IPv4/IPv6 Support

Change the SDM template to support both IPv4 and IPv6, then save and reload the switch.

```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```

After reload, enable IPv6 routing.

```
ipv6 unicast-routing
```

Step 7: Configure Management VLAN Interface

Assign IPv4 and IPv6 addresses to the management SVI.

```
interface vlan 260
ip address 10.11.12.147 255.255.255.248
ipv6 address 2000:12:34:260::3/64
ipv6 enable
no shutdown
exit
```

Step 8: Configure Default Gateways

Configure the IPv6 default route.

```
ipv6 route ::/0 2000:12:34:260::1
```

Configure the IPv4 default gateway.

```
ip default-gateway 10.11.12.145
```

Step 9: Secure Unused Interfaces

Move all unused ports to a dedicated VLAN and shut them down.

```
interface range fastEthernet 0/1-20, fastEthernet 0/23-24,
gigabitEthernet 0/2
switchport access vlan 300
shutdown
exit
```

Step 10: Enable Port Security on Access Ports

Limit each access port to a single learned MAC address using sticky learning.

```
interface range fastEthernet 0/21-22
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 11: Enable Layer 2 Protection Mechanisms

Enable DHCP Snooping and Dynamic ARP Inspection for user VLANs.

```
ip dhcp snooping vlan 200,210
ip arp inspection vlan 200,210
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface connected to the distribution layer.

```
interface gigabitEthernet 0/1
```

```
ip dhcp snooping trust
ip arp inspection trust
exit
```

Step 12: Apply Spanning Tree and Rate Limiting Protections

Enable PortFast, BPDU Guard, and limit DHCP request rates on access ports.

```
interface range fastEthernet 0/21-22
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 13: Enable Logging and Time Synchronization

Enable timestamps on system logs.

```
service timestamps log datetime msec
```

Configure NTP for accurate time synchronization.

```
ntp server 10.11.12.218
```

Step 14: Save the Configuration

Save the running configuration to NVRAM.

```
do write
```

Switch S10

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and move to global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Set the hostname, configure a warning banner, and create a privileged local user.

```
hostname S10
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Management (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Restrict VTY access to SSH using local authentication.

```
line vty 0 4
login local
```

```
transport input ssh
exit
```
Enable console authentication.
```
line console 0
login local
exit
```
Configure a secure enable password.
```
enable secret cisco
```
Step 4: Create VLANs

Create VLANs for users, management, unused ports, and a secure native VLAN.
```
vlan 200
name Instructors
exit

vlan 210
name Researchers
exit

vlan 260
name Management
exit

vlan 300
name Unused-Ports
exit

vlan 305
name New-Native
exit
```
Step 5: Configure Trunk Interfaces

Configure uplink and inter-switch links as trunks, disable DTP negotiation, restrict allowed VLANs, and assign a non-default native VLAN.
```
interface range gigabitEthernet 0/1, fastEthernet 0/1,
fastEthernet 0/24
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 200,210,260
switchport trunk native vlan 305
```

```
exit
```

Step 6: Enable Dual-Stack IPv4/IPv6 Support

Modify the SDM template to support IPv4 and IPv6, then save and reload the switch.

```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```

After reload, enable IPv6 routing.

```
ipv6 unicast-routing
```

Step 7: Configure Management VLAN Interface

Assign IPv4 and IPv6 addresses to the management SVI.

```
interface vlan 260
ip address 10.11.12.148 255.255.255.248
ipv6 address 2000:12:34:260::4/64
ipv6 enable
no shutdown
exit
```

Step 8: Enable Layer 2 Security Mechanisms

Enable DHCP Snooping and Dynamic ARP Inspection for user VLANs.

```
ip dhcp snooping vlan 200,210
ip arp inspection vlan 200,210
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Mark trunk interfaces as trusted for DHCP Snooping and DAI.

```
interface range gigabitEthernet 0/1, fastEthernet 0/1,
fastEthernet 0/2
ip dhcp snooping trust
ip arp inspection trust
exit
```

Step 9: Configure Default Gateways

Configure the IPv6 default route toward the distribution router.

```
ipv6 route ::/0 2000:12:34:260::1
```

Configure the IPv4 default gateway.

```
ip default-gateway 10.11.12.145
```

Step 10: Secure Unused Interfaces

Move all unused ports to a dedicated VLAN and shut them down.

```
interface range fastEthernet 0/2-23, gigabitEthernet 0/2
switchport access vlan 300
```

```
shutdown
exit
```

Step 11: Enable Logging and Time Synchronization

Enable timestamping on system logs.

```
service timestamps log datetime msec
```

Configure NTP to synchronize time with the centralized time server.

```
ntp server 10.11.12.218
```

Step 12: Save the Configuration

Save the running configuration to NVRAM.

```
do write
```

Router R6

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Set the router hostname, configure a security warning banner, and create a privileged local user.

```
hostname R6
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Management (SSH)

Configure the domain name and generate RSA keys for SSH access.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Restrict VTY access to SSH using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable console authentication.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Enable IPv6 Routing

Activate IPv6 routing to support dual-stack operation.

```
ipv6 unicast-routing
```

Step 5: Configure Router-on-a-Stick Subinterfaces

Configure subinterfaces for VLANs 200, 210, and 260 with both IPv4 and IPv6 addressing.

```
interface gigabitEthernet 0/0/0.200
encapsulation dot1Q 200
ip address 10.11.12.97 255.255.255.248
ipv6 address 2000:12:34:200::1/64
ipv6 enable
no shutdown
exit
interface gigabitEthernet 0/0/0.210
encapsulation dot1Q 210
ip address 10.11.12.105 255.255.255.248
ipv6 address 2000:12:34:210::1/64
ipv6 enable
no shutdown
exit
interface gigabitEthernet 0/0/0.260
encapsulation dot1Q 260
ip address 10.11.12.145 255.255.255.248
ipv6 address 2000:12:34:260::1/64
ipv6 enable
no shutdown
exit
```

Enable the physical interface.

```
interface gigabitEthernet 0/0/0
no shutdown
exit
```

Step 6: Configure Serial WAN Interface

Assign an IPv4 address and enable OSPF MD5 authentication on the serial link.

```
interface serial 0/1/0
ip address 10.11.12.217 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit
```

Step 7: Configure IPv6-over-IPv4 Tunnel to R7

Create an IPv6 tunnel over IPv4 to reach R7 via R5.

```
interface Tunnel0
ipv6 address 2001:12:34:1::1/64
tunnel source Se0/1/0
tunnel destination 10.11.12.221
tunnel mode ipv6ip
exit
```

Add static IPv6 routes to R7's LANs through the tunnel.

```
ipv6 route 2000:12:34:220::/64 2001:12:34:1::2
ipv6 route 2000:12:34:230::/64 2001:12:34:1::2
ipv6 route 2000:12:34:270::/64 2001:12:34:1::2
```

Step 8: Configure IPv6-over-IPv4 Tunnel to R8

Create a second IPv6 tunnel to reach R8 via R5.

```
interface Tunnel1
ipv6 address 2001:12:34:2::1/64
tunnel source Se0/1/0
tunnel destination 10.11.12.225
tunnel mode ipv6ip
exit
```

Add static IPv6 routes to R8's LANs through the tunnel.

```
ipv6 route 2000:12:34:240::/64 2001:12:34:2::2
ipv6 route 2000:12:34:250::/64 2001:12:34:2::2
ipv6 route 2000:12:34:280::/64 2001:12:34:2::2
```

Step 9: Enable OSPFv2 Routing

Configure OSPF with a unique router ID and advertise all connected networks.

```
router ospf 1
router-id 6.6.6.6
network 10.11.12.96 0.0.0.7 area 0
network 10.11.12.104 0.0.0.7 area 0
network 10.11.12.144 0.0.0.7 area 0
network 10.11.12.216 0.0.0.3 area 0
exit
```

Step 10: Configure DHCPv4 Services

Exclude gateway IP addresses from DHCP allocation.

```
ip dhcp excluded-address 10.11.12.97
ip dhcp excluded-address 10.11.12.105
```

Create DHCP pools for VLAN 200 and VLAN 210.

```
ip dhcp pool Instructors-VLAN-200
network 10.11.12.96 255.255.255.248
default-router 10.11.12.97
dns-server 10.11.12.235
exit
ip dhcp pool Researchers-VLAN-210
network 10.11.12.104 255.255.255.248
default-router 10.11.12.105
dns-server 10.11.12.235
exit
```

Step 11: Configure Role-Based CLI Views

Enable AAA and activate role-based views.

```
aaa new-model
exit
enable view
```

Create a read-only monitoring view.

```
parser view SHOW
secret show
commands exec include all show
exit
```

Create a restricted DHCP configuration view.

```
parser view DHCP_Conf
secret dhcp
commands exec include configure terminal
command configure include all ip dhcp
command configure include network
command configure include default-router
command configure include dns-server
command configure include exit
command configure include no
commands exec include all show ip dhcp
exit
```

Step 12: Configure IPsec VPN with R4

Create an ISAKMP policy and define the pre-shared key.

```
crypto isakmp policy 1
group 5
authentication pre-share
hash sha
```

```
encryption aes
lifetime 3600
exit

crypto isakmp key cisco address 10.11.12.209
```
Define interesting traffic for the VPN.
```
ip access-list extended VPN-Connection
permit ip 10.11.12.96 0.0.0.7 10.11.12.48 0.0.0.7
permit ip 10.11.12.96 0.0.0.7 10.11.12.56 0.0.0.7
permit ip 10.11.12.96 0.0.0.7 10.11.12.88 0.0.0.7
permit ip 10.11.12.104 0.0.0.7 10.11.12.48 0.0.0.7
permit ip 10.11.12.104 0.0.0.7 10.11.12.56 0.0.0.7
permit ip 10.11.12.104 0.0.0.7 10.11.12.88 0.0.0.7
permit ip 10.11.12.144 0.0.0.7 10.11.12.48 0.0.0.7
permit ip 10.11.12.144 0.0.0.7 10.11.12.56 0.0.0.7
permit ip 10.11.12.144 0.0.0.7 10.11.12.88 0.0.0.7
exit
```
Configure IPsec transform set and crypto map.
```
crypto ipsec transform-set R4-R6 esp-aes
crypto map R4-R6_MAP 10 ipsec-isakmp
match address VPN-Connection
set transform-set R4-R6
set peer 10.11.12.209
set pfs group5
set security-association lifetime seconds 900
exit
```
Apply the crypto map to the WAN interface.
```
interface serial 0/1/0
crypto map R4-R6_MAP
exit
```
Step 13: Enable Logging and Time Synchronization

Enable timestamps on system logs.
```
service timestamps log datetime msec
```
Configure NTP synchronization.
```
ntp server 10.11.12.218
```
Step 14: Save the Configuration

Save the running configuration to NVRAM.
```
do write
```

Switch S14

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and move to global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the hostname, configure a warning banner, and create a privileged local user.

```
hostname S14
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Define the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines to allow SSH access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Create VLANs

Create and name all required VLANs, including user, management, and unused-port VLANs.

```
vlan 220
name Graphics
exit

vlan 230
name Branding
exit

vlan 270
```

```
name Management
exit

vlan 330
name Unused-Ports
exit

vlan 335
name New-Native
exit
```

Step 5: Configure Access and Trunk Ports

Assign access ports to their respective VLANs.

```
interface fastEthernet 0/22
switchport mode access
switchport access vlan 220
exit
interface fastEthernet 0/20
switchport mode access
switchport access vlan 230
exit
```

Configure the trunk interface with a restricted VLAN list and a new native VLAN.

```
interface gigabitEthernet 0/2
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 220,230,270
switchport trunk native vlan 335
exit
```

Step 6: Enable IPv6 Support (SDM Template)

Modify the SDM template to support IPv6 and reload the switch.

```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```

Step 7: Configure Management VLAN Interface

Assign IPv4 and IPv6 addresses to the management SVI and enable it.

```
interface vlan 270
ip address 10.11.12.154 255.255.255.248
ipv6 address 2000:12:34:270::2/64
ipv6 enable
```

```
no shutdown
exit
```
Enable IPv6 routing.
```
ipv6 unicast-routing
```
Step 8: Configure Default Gateways

Configure both IPv4 and IPv6 default gateways for management connectivity.
```
ip default-gateway 10.11.12.153
ipv6 route ::/0 2000:12:34:270::1
```
Step 9: Secure Unused Ports

Assign all unused ports to a dedicated VLAN and administratively shut them down.
```
interface range fastEthernet 0/1-19, fastEthernet 0/21,
fastEthernet 0/23, fastEthernet 0/24, gigabitEthernet 0/1
switchport access vlan 330
shutdown
exit
```
Step 10: Enable Port Security on Access Ports

Restrict each access port to a single learned MAC address using sticky MAC addressing.
```
interface range fastEthernet 0/20, fastEthernet 0/22
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```
Step 11: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection for user VLANs.
```
ip dhcp snooping vlan 220,230
ip arp inspection vlan 220,230
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```
Trust the trunk interface.
```
interface gigabitEthernet 0/2
ip dhcp snooping trust
ip arp inspection trust
exit
```
Apply rate limiting and spanning-tree protections on access ports.
```
interface range fastEthernet 0/20, fastEthernet 0/22
ip dhcp snooping limit rate 6
```

```
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 12: Enable Logging and Time Synchronization

Enable timestamping for system logs.

```
service timestamps log datetime msec
```

Configure NTP synchronization.

```
ntp server 10.11.12.222
```

Step 13: Save the Configuration

Save the running configuration to NVRAM.

```
do write
```

Switch S15

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the switch hostname, configure a security banner, and create a privileged local user.

```
hostname S15
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines for SSH-only access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Create VLANs

Create and name all required VLANs, including user, management, and unused-port VLANs.

```
vlan 220
name Graphics
exit

vlan 230
name Branding
exit

vlan 270
name Management
exit

vlan 330
name Unused-Ports
exit

vlan 335
name New-Native
exit
```

Step 5: Configure Access and Trunk Ports

Assign access ports to their corresponding VLANs.

```
interface fastEthernet 0/24
switchport mode access
switchport access vlan 220
exit
interface fastEthernet 0/19
switchport mode access
switchport access vlan 230
exit
```

Configure the trunk interface, restrict allowed VLANs, disable DTP negotiation, and assign a new native VLAN.

```
interface gigabitEthernet 0/2
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 220,230,270
```

```
switchport trunk native vlan 335
exit
```

Step 6: Enable IPv6 Support (SDM Template)

Change the SDM template to support IPv6 operation and reload the switch.

```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```

Step 7: Configure the Management VLAN Interface

Assign IPv4 and IPv6 addresses to the management VLAN interface and enable it.

```
interface vlan 270
ip address 10.11.12.155 255.255.255.248
ipv6 address 2000:12:34:270::3/64
ipv6 enable
no shutdown
exit
```

Enable IPv6 routing on the switch.

```
ipv6 unicast-routing
```

Step 8: Configure Default Gateways

Configure both IPv4 and IPv6 default gateways to allow management traffic to reach external networks.

```
ip default-gateway 10.11.12.153
ipv6 route ::/0 2000:12:34:270::1
```

Step 9: Secure Unused Ports

Move all unused interfaces to a dedicated VLAN and administratively shut them down.

```
interface range fastEthernet 0/1-18, fastEthernet 0/20-23,
gigabitEthernet 0/1
switchport access vlan 330
shutdown
exit
```

Step 10: Enable Port Security on Access Ports

Limit access ports to a single MAC address using sticky MAC learning and restrict violations.

```
interface range fastEthernet 0/19, fastEthernet 0/24
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 11: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection on user VLANs.

```
ip dhcp snooping vlan 220,230
ip arp inspection vlan 220,230
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface.

```
interface gigabitEthernet 0/2
ip dhcp snooping trust
ip arp inspection trust
exit
```

Apply rate limiting and spanning-tree protections on access ports.

```
interface range fastEthernet 0/19, fastEthernet 0/24
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 12: Enable Logging and Time Synchronization

Enable timestamping for system logs.

```
service timestamps log datetime msec
```

Configure NTP for time synchronization.

```
ntp server 10.11.12.222
```

Step 13: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

Switch S13

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the switch hostname, configure a security banner, and create a privileged local user.

```
hostname S13
banner motd &##### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines for SSH-only access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Create VLANs

Create and name all required VLANs, including user, management, and unused-port VLANs.

```
vlan 220
name Graphics
exit

vlan 230
name Branding
exit

vlan 270
name Management
exit

vlan 330
name Unused-Ports
exit

vlan 335
name New-Native
exit
```

Step 5: Configure Trunk Ports

Configure trunk interfaces, restrict allowed VLANs, disable DTP negotiation, and assign a new native VLAN.

```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 220,230,270
switchport trunk native vlan 335
exit
```

Step 6: Enable IPv6 Support (SDM Template)

Change the SDM template to support IPv6 operation and reload the switch.

```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```

Step 7: Configure the Management VLAN Interface

Assign IPv4 and IPv6 addresses to the management VLAN interface and enable it.

```
interface vlan 270
ip address 10.11.12.156 255.255.255.248
ipv6 address 2000:12:34:270::4/64
ipv6 enable
no shutdown
exit
```

Enable IPv6 routing on the switch.

```
ipv6 unicast-routing
```

Step 8: Configure Default Gateways

Configure both IPv4 and IPv6 default gateways to allow management traffic to reach external networks.

```
ip default-gateway 10.11.12.153
ipv6 route ::/0 2000:12:34:270::1
```

Step 9: Secure Unused Ports

Move all unused interfaces to a dedicated VLAN and administratively shut them down.

```
interface range fastEthernet 0/2-24
switchport access vlan 330
shutdown
exit
```

Step 10: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection on user VLANs.

```
ip dhcp snooping vlan 220,230
ip arp inspection vlan 220,230
```

```
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```
Trust trunk interfaces for DHCP and ARP inspection.
```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```
Step 11: Enable Logging and Time Synchronization
Enable timestamping for system logs.
```
service timestamps log datetime msec
```
Configure NTP for time synchronization.
```
ntp server 10.11.12.222
```
Step 12: Save the Configuration
Save the running configuration to non-volatile memory.
```
do write
```
Router R7
Step 1: Enter Privileged and Global Configuration Mode
Access privileged EXEC mode and enter global configuration.
```
enable
configure terminal
```
Step 2: Configure Basic Device Identity and Security
Assign the router hostname, configure a security banner, and create a privileged local user.
```
hostname R7
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```
Enable password encryption.
```
service password-encryption
```
Step 3: Enable Secure Remote Access (SSH)
Configure the domain name and generate RSA keys required for SSH.
```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```
Configure VTY lines for SSH-only access using local authentication.
```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Enable IPv6 Routing

Enable IPv6 routing globally on the router.

```
ipv6 unicast-routing
```

Step 5: Configure Router-on-a-Stick Subinterfaces

Configure VLAN subinterfaces with IPv4 and IPv6 addressing.

Graphics VLAN (220)

```
interface gigabitEthernet 0/0/0.220
encapsulation dot1Q 220
ip address 10.11.12.113 255.255.255.248
ipv6 address 2000:12:34:220::1/64
ipv6 enable
no shutdown
exit
```

Branding VLAN (230)

```
interface gigabitEthernet 0/0/0.230
encapsulation dot1Q 230
ip address 10.11.12.121 255.255.255.248
ipv6 address 2000:12:34:230::1/64
ipv6 enable
no shutdown
exit
```

Management VLAN (270)

```
interface gigabitEthernet 0/0/0.270
encapsulation dot1Q 270
ip address 10.11.12.153 255.255.255.248
ipv6 address 2000:12:34:270::1/64
ipv6 enable
no shutdown
exit
```

Enable the physical interface.

```
interface gigabitEthernet 0/0/0
no shutdown
```

```
exit
```

Step 6: Configure WAN Serial Interface

Configure the serial interface and enable OSPF authentication.

```
interface serial 0/1/0
ip address 10.11.12.221 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit
```

Step 7: Configure IPv6-over-IPv4 Tunnel to Router R6

Create a tunnel interface to carry IPv6 traffic over the IPv4 network.

```
interface Tunnel0
ipv6 address 2001:12:34:1::2/64
tunnel source Se0/1/0
tunnel destination 10.11.12.217
tunnel mode ipv6ip
exit
```

Configure IPv6 static routes for R6 networks via the tunnel.

```
ipv6 route 2000:12:34:200::/64 2001:12:34:1::1
ipv6 route 2000:12:34:210::/64 2001:12:34:1::1
ipv6 route 2000:12:34:260::/64 2001:12:34:1::1
```

Step 8: Configure IPv6-over-IPv4 Tunnel to Router R8

Create a tunnel interface toward R8.

```
interface Tunnel2
ipv6 address 2001:12:34:3::1/64
tunnel source Se0/1/0
tunnel destination 10.11.12.225
tunnel mode ipv6ip
exit
```

Configure IPv6 static routes for R8 networks via the tunnel.

```
ipv6 route 2000:12:34:240::/64 2001:12:34:3::2
ipv6 route 2000:12:34:250::/64 2001:12:34:3::2
ipv6 route 2000:12:34:280::/64 2001:12:34:3::2
```

Step 9: Enable OSPFv2 Routing

Configure OSPFv2 for IPv4 routing.

```
router ospf 1
router-id 7.7.7.7
network 10.11.12.112 0.0.0.7 area 0
```

```
network 10.11.12.120 0.0.0.7 area 0
network 10.11.12.152 0.0.0.7 area 0
network 10.11.12.220 0.0.0.3 area 0
exit
```

Step 10: Configure DHCPv4 Services

Exclude gateway addresses from DHCP.

```
ip dhcp excluded-address 10.11.12.113
ip dhcp excluded-address 10.11.12.121
```

Create DHCP pool for Graphics VLAN.

```
ip dhcp pool Graphics-VLAN-220
network 10.11.12.112 255.255.255.248
default-router 10.11.12.113
dns-server 10.11.12.235
exit
```

Create DHCP pool for Branding VLAN.

```
ip dhcp pool Branding-VLAN-230
network 10.11.12.120 255.255.255.248
default-router 10.11.12.121
dns-server 10.11.12.235
exit
```

Step 11: Configure IPv6 Access Control List

Create an IPv6 ACL to control Branding VLAN traffic.

```
ipv6 access-list Branding2Out
permit icmp 2000:12:34:230::0/64 any nd-na
permit icmp 2000:12:34:230::0/64 any nd-ns
permit icmp 2000:12:34:230::0/64 any echo-reply
exit
```

Apply the IPv6 ACL inbound on the Branding subinterface.

```
interface gigabitEthernet 0/0/0.230
ipv6 traffic-filter Branding2Out in
exit
```

Step 12: Enable Logging and Time Synchronization

Enable timestamps for system logs.

```
service timestamps log datetime msec
```

Configure NTP for time synchronization.

```
ntp server 10.11.12.222
```

Step 13: Save the Configuration

Save the running configuration.

```
do write
```

Switch S17

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the switch hostname, configure a security banner, and create a privileged local user.

```
hostname S17
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines for SSH-only access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Create VLANs

Create and name all required VLANs, including user, management, and unused-port VLANs.

```
vlan 240
name Analysts
exit

vlan 250
name Auditors
exit
```

```
vlan 280
name Management
exit

vlan 360
name Unused-Ports
exit

vlan 365
name New-Native
exit
```

Step 5: Configure Access and Trunk Ports

Assign access ports to their corresponding VLANs.

Analysts VLAN (240)

```
interface fastEthernet 0/23
switchport mode access
switchport access vlan 240
exit
```

Auditors VLAN (250)

```
interface fastEthernet 0/21
switchport mode access
switchport access vlan 250
exit
```

Configure the trunk interface, restrict allowed VLANs, disable DTP negotiation, and assign a new native VLAN.

```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 240,250,280
switchport trunk native vlan 365
exit
```

Step 6: Enable IPv6 Support (SDM Template)

Change the SDM template to support IPv6 operation and reload the switch.

```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```

Step 7: Configure the Management VLAN Interface

Assign IPv4 and IPv6 addresses to the management VLAN interface and enable it.

```
interface vlan 280
ip address 10.11.12.162 255.255.255.248
ipv6 address 2000:12:34:280::2/64
ipv6 enable
no shutdown
exit
```

Enable IPv6 routing on the switch.

```
ipv6 unicast-routing
```

Step 8: Configure Default Gateways

Configure both IPv4 and IPv6 default gateways for management traffic.

```
ip default-gateway 10.11.12.161
ipv6 route ::/0 2000:12:34:280::1
```

Step 9: Secure Unused Ports

Move all unused interfaces to a dedicated VLAN and administratively shut them down.

```
interface range fastEthernet 0/1-20, fastEthernet 0/22,
fastEthernet 0/24, gigabitEthernet 0/2
switchport access vlan 360
shutdown
exit
```

Step 10: Enable Port Security on Access Ports

Restrict access ports to a single MAC address using sticky MAC learning.

```
interface range fastEthernet 0/21, fastEthernet 0/23
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 11: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection on user VLANs.

```
ip dhcp snooping vlan 240,250
ip arp inspection vlan 240,250
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
```

```
ip arp inspection trust
exit
```
Apply rate limiting and spanning-tree protections on access ports.
```
interface range fastEthernet 0/21, fastEthernet 0/23
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```
Step 12: Enable Logging and Time Synchronization
Enable timestamping for system logs.
```
service timestamps log datetime msec
```
Configure NTP for time synchronization.
```
ntp server 10.11.12.226
```
Step 13: Save the Configuration
Save the running configuration to non-volatile memory.
```
do write
```
Switch S18
Step 1: Enter Privileged and Global Configuration Mode
Access privileged EXEC mode and enter global configuration.
```
enable
configure terminal
```
Step 2: Configure Basic Device Identity and Security
Assign the switch hostname, configure a security banner, and create a privileged local user.
```
hostname S18
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```
Enable password encryption.
```
service password-encryption
```
Step 3: Enable Secure Remote Access (SSH)
Configure the domain name and generate RSA keys required for SSH.
```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```
Configure VTY lines for SSH-only access using local authentication.
```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Create VLANs

Create and name all required VLANs, including user, management, and unused-port VLANs.

```
vlan 240
name Analysts
exit

vlan 250
name Auditors
exit

vlan 280
name Management
exit

vlan 360
name Unused-Ports
exit

vlan 365
name New-Native
exit
```

Step 5: Configure Access and Trunk Ports

Assign access ports to their corresponding VLANs.

Analysts VLAN (240)

```
interface fastEthernet 0/21
switchport mode access
switchport access vlan 240
exit
```

Auditors VLAN (250)

```
interface fastEthernet 0/22
switchport mode access
switchport access vlan 250
```

```
exit
```
Configure the trunk interface, restrict allowed VLANs, disable DTP negotiation, and assign a new native VLAN.
```
interface gigabitEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 240,250,280
switchport trunk native vlan 365
exit
```
Step 6: Enable IPv6 Support (SDM Template)
Change the SDM template to support IPv6 operation and reload the switch.
```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```
Step 7: Configure the Management VLAN Interface
Assign IPv4 and IPv6 addresses to the management VLAN interface and enable it.
```
interface vlan 280
ip address 10.11.12.163 255.255.255.248
ipv6 address 2000:12:34:280::3/64
ipv6 enable
no shutdown
exit
```
Enable IPv6 routing on the switch.
```
ipv6 unicast-routing
```
Step 8: Configure Default Gateways
Configure both IPv4 and IPv6 default gateways for management traffic.
```
ip default-gateway 10.11.12.161
ipv6 route ::/0 2000:12:34:280::1
```
Step 9: Secure Unused Ports
Move all unused interfaces to a dedicated VLAN and administratively shut them down.
```
interface range fastEthernet 0/1-20, fastEthernet 0/23-24,
gigabitEthernet 0/2
switchport access vlan 360
shutdown
exit
```
Step 10: Enable Port Security on Access Ports
Restrict access ports to a single MAC address using sticky MAC learning.
```
interface range fastEthernet 0/21-22
```

```
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 11: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection on user VLANs.

```
ip dhcp snooping vlan 240,250
ip arp inspection vlan 240,250
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the trunk interface.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Apply rate limiting and spanning-tree protections on access ports.

```
interface range fastEthernet 0/21-22
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 12: Enable Logging and Time Synchronization

Enable timestamping for system logs.

```
service timestamps log datetime msec
```

Configure NTP for time synchronization.

```
ntp server 10.11.12.226
```

Step 13: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

Switch S16

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the switch hostname, configure a security banner, and create a privileged local user.

```
hostname S16
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines for SSH-only access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Create VLANs

Create and name all required VLANs, including user, management, and unused-port VLANs.

```
vlan 240
name Analysts
exit

vlan 250
name Auditors
exit

vlan 280
name Management
exit

vlan 360
name Unused-Ports
exit
```

```
vlan 365
name New-Native
exit
```

Step 5: Configure Trunk Interfaces

Configure all uplink interfaces as trunks, restrict allowed VLANs, disable DTP negotiation, and assign a new native VLAN.

```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 240,250,280
switchport trunk native vlan 365
exit
```

Step 6: Enable IPv6 Support (SDM Template)

Change the SDM template to support IPv6 operation and reload the switch.

```
sdm prefer dual-ipv4-and-ipv6 default
do write
do reload
```

Step 7: Configure the Management VLAN Interface

Assign IPv4 and IPv6 addresses to the management VLAN interface and enable it.

```
interface vlan 280
ip address 10.11.12.164 255.255.255.248
ipv6 address 2000:12:34:280::4/64
ipv6 enable
no shutdown
exit
```

Enable IPv6 routing on the switch.

```
ipv6 unicast-routing
```

Step 8: Configure Default Gateways

Configure both IPv4 and IPv6 default gateways for management traffic.

```
ip default-gateway 10.11.12.161
ipv6 route ::/0 2000:12:34:280::1
```

Step 9: Secure Unused Ports

Move all unused access interfaces to a dedicated VLAN and administratively shut them down.

```
interface range fastEthernet 0/2-24
switchport access vlan 360
shutdown
exit
```

Step 10: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection on user VLANs.

```
ip dhcp snooping vlan 240,250
ip arp inspection vlan 240,250
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust trunk interfaces connected to infrastructure devices.

```
interface range gigabitEthernet 0/1-2, fastEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Step 11: Enable Logging and Time Synchronization

Enable timestamping for system logs.

```
service timestamps log datetime msec
```

Configure NTP for time synchronization.

```
ntp server 10.11.12.226
```

Step 12: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

Router R8

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the router hostname, configure a security banner, and create a privileged local user.

```
hostname R8
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines for SSH-only access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```
Enable authentication on the console line.
```
line console 0
login local
exit
```
Configure a secure enable password.
```
enable secret cisco
```
Step 4: Enable IPv6 Routing

Enable IPv6 packet forwarding on the router.
```
ipv6 unicast-routing
```
Step 5: Configure Router-on-a-Stick Subinterfaces

Configure subinterfaces on **GigabitEthernet0/0/0** to provide inter-VLAN routing for IPv4 and IPv6.

VLAN 240 – Analysts
```
interface gigabitEthernet 0/0/0.240
encapsulation dot1Q 240
ip address 10.11.12.129 255.255.255.248
ipv6 address 2000:12:34:240::1/64
ipv6 enable
no shutdown
exit
```
VLAN 250 – Auditors
```
interface gigabitEthernet 0/0/0.250
encapsulation dot1Q 250
ip address 10.11.12.137 255.255.255.248
ipv6 address 2000:12:34:250::1/64
ipv6 enable
no shutdown
exit
```
VLAN 280 – Management
```
interface gigabitEthernet 0/0/0.280
encapsulation dot1Q 280
ip address 10.11.12.161 255.255.255.248
ipv6 address 2000:12:34:280::1/64
ipv6 enable
```

```
no shutdown
exit
```
Enable the physical interface.
```
interface gigabitEthernet 0/0/0
no shutdown
exit
```
Step 6: Configure WAN Serial Interface

Assign an IPv4 address to the serial interface and enable OSPF MD5 authentication.
```
interface serial 0/1/1
ip address 10.11.12.225 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit
```
Step 7: Configure IPv6-over-IPv4 Tunnel to R6

Create a tunnel interface to provide IPv6 connectivity to R6 through an IPv4-only path.
```
interface Tunnel1
ipv6 address 2001:12:34:2::2/64
tunnel source Se0/1/1
tunnel destination 10.11.12.217
tunnel mode ipv6ip
exit
```
Add static IPv6 routes for R6's LANs through the tunnel.
```
ipv6 route 2000:12:34:200::/64 2001:12:34:2::1
ipv6 route 2000:12:34:210::/64 2001:12:34:2::1
ipv6 route 2000:12:34:260::/64 2001:12:34:2::1
```
Step 8: Configure IPv6-over-IPv4 Tunnel to R7

Create a second tunnel interface to provide IPv6 connectivity to R7.
```
interface Tunnel2
ipv6 address 2001:12:34:3::2/64
tunnel source Se0/1/1
tunnel destination 10.11.12.221
tunnel mode ipv6ip
exit
```
Add static IPv6 routes for R7's LANs through the tunnel.
```
ipv6 route 2000:12:34:220::/64 2001:12:34:3::1
ipv6 route 2000:12:34:230::/64 2001:12:34:3::1
ipv6 route 2000:12:34:270::/64 2001:12:34:3::1
```

Step 9: Enable OSPFv2 Routing

Configure OSPFv2 for IPv4 routing and advertise all connected networks.

```
router ospf 1
router-id 8.8.8.8
network 10.11.12.128 0.0.0.7 area 0
network 10.11.12.136 0.0.0.7 area 0
network 10.11.12.160 0.0.0.7 area 0
network 10.11.12.224 0.0.0.3 area 0
exit
```

Step 10: Configure DHCPv4 Services

Exclude gateway addresses from DHCP allocation.

```
ip dhcp excluded-address 10.11.12.129
ip dhcp excluded-address 10.11.12.137
```

Create a DHCP pool for the Analysts VLAN.

```
ip dhcp pool Analysts-VLAN-240
network 10.11.12.128 255.255.255.248
default-router 10.11.12.129
dns-server 10.11.12.235
exit
```

Create a DHCP pool for the Auditors VLAN.

```
ip dhcp pool Auditors-VLAN-250
network 10.11.12.136 255.255.255.248
default-router 10.11.12.137
dns-server 10.11.12.235
exit
```

Step 11: Enable Logging and Time Synchronization

Enable timestamping for system logs.

```
service timestamps log datetime msec
```

Configure NTP for time synchronization.

```
ntp server 10.11.12.226
```

Step 12: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

Router R5

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
```

```
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the router hostname, configure a security banner, and create a privileged local user.

```
hostname R5
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines for SSH-only access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Configure WAN and LAN Interfaces

Assign IPv4 addresses to all serial and Gigabit interfaces and enable OSPF MD5 authentication on WAN links.

Serial Interfaces

```
interface serial 0/1/0
ip address 10.11.12.214 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit

interface serial 0/1/1
ip address 10.11.12.218 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
```

```
no shutdown
exit

interface serial 0/2/0
ip address 10.11.12.222 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit

interface serial 0/2/1
ip address 10.11.12.226 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
no shutdown
exit
```

GigabitEthernet Interface

```
interface gigabitEthernet 0/0/0
ip address 10.11.12.233 255.255.255.248
no shutdown
exit
```

Loopback Interface (Router ID Stability)

```
interface loopback 0
ip address 5.5.5.5 255.255.255.0
no shutdown
exit
```

Step 5: Enable OSPFv2 Routing

Configure OSPFv2, set a stable router ID, and advertise all connected networks.

```
router ospf 1
router-id 5.5.5.5
network 10.11.12.212 0.0.0.3 area 0
network 10.11.12.216 0.0.0.3 area 0
network 10.11.12.220 0.0.0.3 area 0
network 10.11.12.224 0.0.0.3 area 0
network 10.11.12.228 0.0.0.3 area 0
network 10.11.12.232 0.0.0.3 area 0
exit
```

Step 6: Configure Static Routes for Inside Hosts

Add host-specific static routes for internal devices.

```
ip route 10.11.12.235 255.255.255.255 10.11.12.234
ip route 10.11.12.237 255.255.255.255 10.11.12.234
```

Step 7: Enable IOS Intrusion Prevention System (IPS)

Create a local directory for IPS files and define an IPS policy.

```
mkdir ipsdir
configure terminal
ip ips config location ipsdir
ip ips name iosips
```

Enable only the basic IOS IPS signature category.

```
ip ips signature-category
category all
retired true
exit
category ios_ips basic
retired false
exit
exit
```

Apply the IPS policy outbound on WAN interfaces.

```
interface serial 0/1/1
ip ips iosips out
exit

interface serial 0/2/0
ip ips iosips out
exit

interface serial 0/2/1
ip ips iosips out
exit
```

Step 8: Configure IPS ICMP Inspection

Enable IPS inspection for ICMP traffic and drop malicious packets inline.

```
ip ips signature-definition
signature 2004 0
status
retired false
enabled true
exit
```

```
engine
event-action deny-packet-inline
event-action produce-alert
exit
exit
exit
```

Step 9: Enable Logging and Time Synchronization

Enable timestamping for system logs.

```
service timestamps log datetime msec
exit
```

Manually set the system clock and configure the router as an NTP master.

```
clock set 19:14:50 jan 31 2025
configure terminal
ntp master 1
```

Step 10: Save the Configuration

Save the running configuration to non-volatile memory.

```
do write
```

ASA Firewall (ASA-FW)

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the firewall hostname, domain name, enable password, and create a local user.

```
hostname ASA-FW
domain-name cisco.local
enable password cisco
username cisco password cisco
```

Generate RSA keys for SSH access.

```
crypto key generate rsa modulus 1024
yes
```

Enable SSH access from the INSIDE network using local authentication.

```
ssh 10.11.12.192 255.255.255.248 INSIDE
aaa authentication ssh console LOCAL
```

Step 3: Configure Firewall Interfaces

Configure all security zones with appropriate security levels and IP addressing.

OUTSIDE Interface

```
interface gigabitEthernet 1/1
nameif OUTSIDE
security-level 0
ip address 10.11.12.234 255.255.255.248
no shutdown
exit
```

INSIDE Interface

```
interface gigabitEthernet 1/2
nameif INSIDE
security-level 100
ip address 10.11.12.193 255.255.255.248
no shutdown
exit
```

DMZ Interface

```
interface gigabitEthernet 1/3
nameif DMZ
security-level 50
ip address 10.11.12.185 255.255.255.248
no shutdown
exit
```

Step 4: Enable Application Inspection

Allow stateful inspection for common protocols to permit return traffic.

```
policy-map global_policy
class inspection_default
inspect dns
no inspect icmp
no inspect ftp
no inspect tftp
no inspect http
exit
```

Step 5: Configure Default Route

Define a default route toward the upstream router on the OUTSIDE interface.

```
route OUTSIDE 0.0.0.0 0.0.0.0 10.11.12.233
```

Step 6: Configure Network Objects and NAT

Create network objects and configure static NAT for INSIDE and DMZ resources.

INSIDE Network Static NAT

```
object network INSIDE-Network
subnet 10.11.12.192 255.255.255.248
```

```
nat (INSIDE,OUTSIDE) static 10.11.12.237
exit
```

DMZ Network Object

```
object network DMZ-Network
subnet 10.11.12.184 255.255.255.248
exit
```

DMZ Server Static NAT

```
object network SERVER-DMZ-NET
host 10.11.12.187
nat (DMZ,OUTSIDE) static 10.11.12.235
exit
```

DMZ PC Static NAT

```
object network PC-DMZ-NET
host 10.11.12.188
nat (DMZ,OUTSIDE) static 10.11.12.236
exit
```

Step 7: Configure Access Control Lists (ACLs)

OUTSIDE Interface ACL

Allow external users to access specific services hosted in the DMZ.

```
access-list OUTSIDE_ACL extended permit tcp any host
10.11.12.235 eq 80
access-list OUTSIDE_ACL extended permit tcp any host
10.11.12.235 eq 443
access-list OUTSIDE_ACL extended permit tcp any host
10.11.12.235 eq 25
access-list OUTSIDE_ACL extended permit udp any host
10.11.12.235 eq 53
access-list OUTSIDE_ACL extended permit tcp any host
10.11.12.235 eq 21
access-list OUTSIDE_ACL extended permit tcp any host
10.11.12.235 eq 20
access-list OUTSIDE_ACL extended permit tcp host 10.11.12.235 eq
443 host 10.11.12.237
access-list OUTSIDE_ACL extended permit tcp host 10.11.12.235 eq
www host 10.11.12.237
access-list OUTSIDE_ACL extended permit icmp any any echo-reply
access-group OUTSIDE_ACL in interface OUTSIDE
```

DMZ Interface ACL

Allow INSIDE users to access DMZ services using management protocols.

```
access-list DMZ_ACL extended permit tcp object DMZ-Network
object INSIDE-Network eq 22
access-list DMZ_ACL extended permit tcp object DMZ-Network
object INSIDE-Network eq 23
access-list DMZ_ACL extended permit udp host 10.11.12.187 eq 53
any
access-group DMZ_ACL in interface DMZ
```

Step 8: Save the Configuration

Save the running configuration to non-volatile memory.

```
write memory
```

Switch S19

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.

```
enable
configure terminal
```

Step 2: Configure Basic Device Identity and Security

Assign the switch hostname, configure a security banner, and create a privileged local user.

```
hostname S19
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```

Enable password encryption.

```
service password-encryption
```

Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH.

```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```

Configure VTY lines for SSH-only access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```

Enable authentication on the console line.

```
line console 0
login local
exit
```

Configure a secure enable password.

```
enable secret cisco
```

Step 4: Create VLANs

Create a dedicated VLAN for unused ports.

```
vlan 500
name Unused-Ports
exit
```

Step 5: Configure Access Ports

Configure active user ports as access ports.

```
interface range fastEthernet 0/1-2
switchport mode access
exit
```

Step 6: Configure the Management VLAN Interface

Assign an IP address to the default VLAN interface for management access.

```
interface vlan 1
ip address 10.11.12.186 255.255.255.248
no shutdown
exit
```

Step 7: Configure Default Gateway

Define the default gateway for management traffic.

```
ip default-gateway 10.11.12.185
```

Step 8: Secure Unused Ports

Move all unused interfaces to a dedicated VLAN and administratively shut them down.

```
interface range fastEthernet 0/3-24, gigabitEthernet 0/2
switchport access vlan 500
shutdown
exit
```

Step 9: Enable Port Security on Access Ports

Restrict access ports to a single MAC address using sticky MAC learning.

```
interface range fastEthernet 0/1-2
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 10: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection.

```
ip dhcp snooping
ip arp inspection vlan 1
```

```
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```
Trust the uplink interface.
```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```
Apply rate limiting and spanning-tree protections on access ports.
```
interface range fastEthernet 0/1-2
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```
Step 11: Enable Logging

Enable timestamping for system logs.
```
service timestamps log datetime msec
```
Step 12: Save the Configuration

Save the running configuration to non-volatile memory.
```
do write
```
Switch S20

Step 1: Enter Privileged and Global Configuration Mode

Access privileged EXEC mode and enter global configuration.
```
enable
configure terminal
```
Step 2: Configure Basic Device Identity and Security

Assign the switch hostname, configure a security banner, and create a privileged local user.
```
hostname S20
banner motd &#### Authorized Access Only ####&
username cisco privilege 15 secret cisco
```
Enable password encryption.
```
service password-encryption
```
Step 3: Enable Secure Remote Access (SSH)

Configure the domain name and generate RSA keys required for SSH.
```
ip domain-name cisco.local
crypto key generate rsa general-keys modulus 1024
```
Configure VTY lines for SSH-only access using local authentication.

```
line vty 0 4
login local
transport input ssh
exit
```
Enable authentication on the console line.
```
line console 0
login local
exit
```
Configure a secure enable password.
```
enable secret cisco
```
Step 4: Create VLANs

Create a dedicated VLAN for unused ports.
```
vlan 510
name Unused-Ports
exit
```
Step 5: Configure Access Ports

Configure the active user port as an access port.
```
interface fastEthernet 0/1
switchport mode access
exit
```
Step 6: Configure the Management VLAN Interface

Assign an IP address to the default VLAN interface for management access.
```
interface vlan 1
ip address 10.11.12.194 255.255.255.248
no shutdown
exit
```
Step 7: Configure Default Gateway

Define the default gateway for management traffic.
```
ip default-gateway 10.11.12.193
```
Step 8: Secure Unused Ports

Move all unused interfaces to a dedicated VLAN and administratively shut them down.
```
interface range fastEthernet 0/2-24, gigabitEthernet 0/2
switchport access vlan 510
shutdown
exit
```
Step 9: Enable Port Security on Access Ports

Restrict the access port to a single MAC address using sticky MAC learning.
```
interface fastEthernet 0/1
```

```
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation restrict
exit
```

Step 10: Enable Layer 2 Security Features

Enable DHCP Snooping and Dynamic ARP Inspection.

```
ip dhcp snooping
ip arp inspection vlan 1
ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip
```

Trust the uplink interface.

```
interface gigabitEthernet 0/1
ip dhcp snooping trust
ip arp inspection trust
exit
```

Apply rate limiting and spanning-tree protections on the access port.

```
interface fastEthernet 0/1
ip dhcp snooping limit rate 6
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

Step 11: Enable Logging

Enable timestamping for system logs.

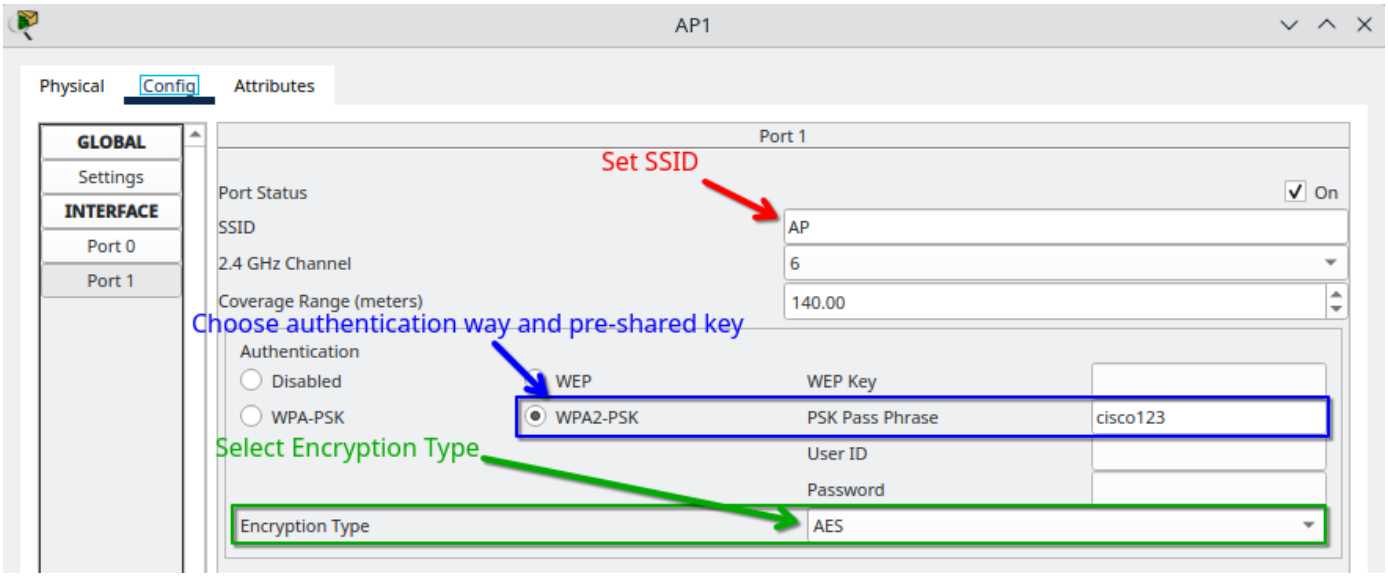
```
service timestamps log datetime msec
```

Step 12: Save the Configuration

Save the running configuration to non-volatile memory.

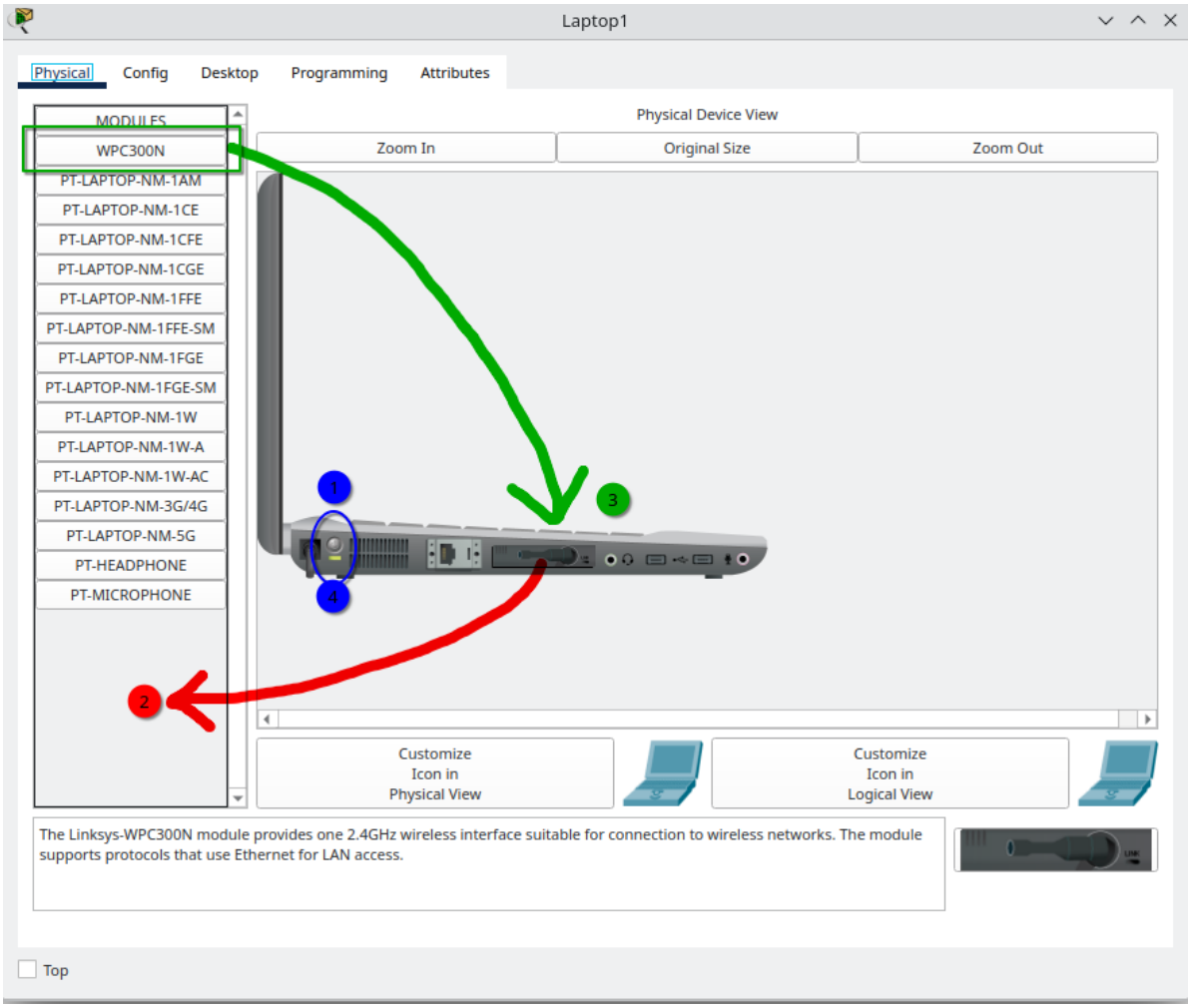
```
do write
```

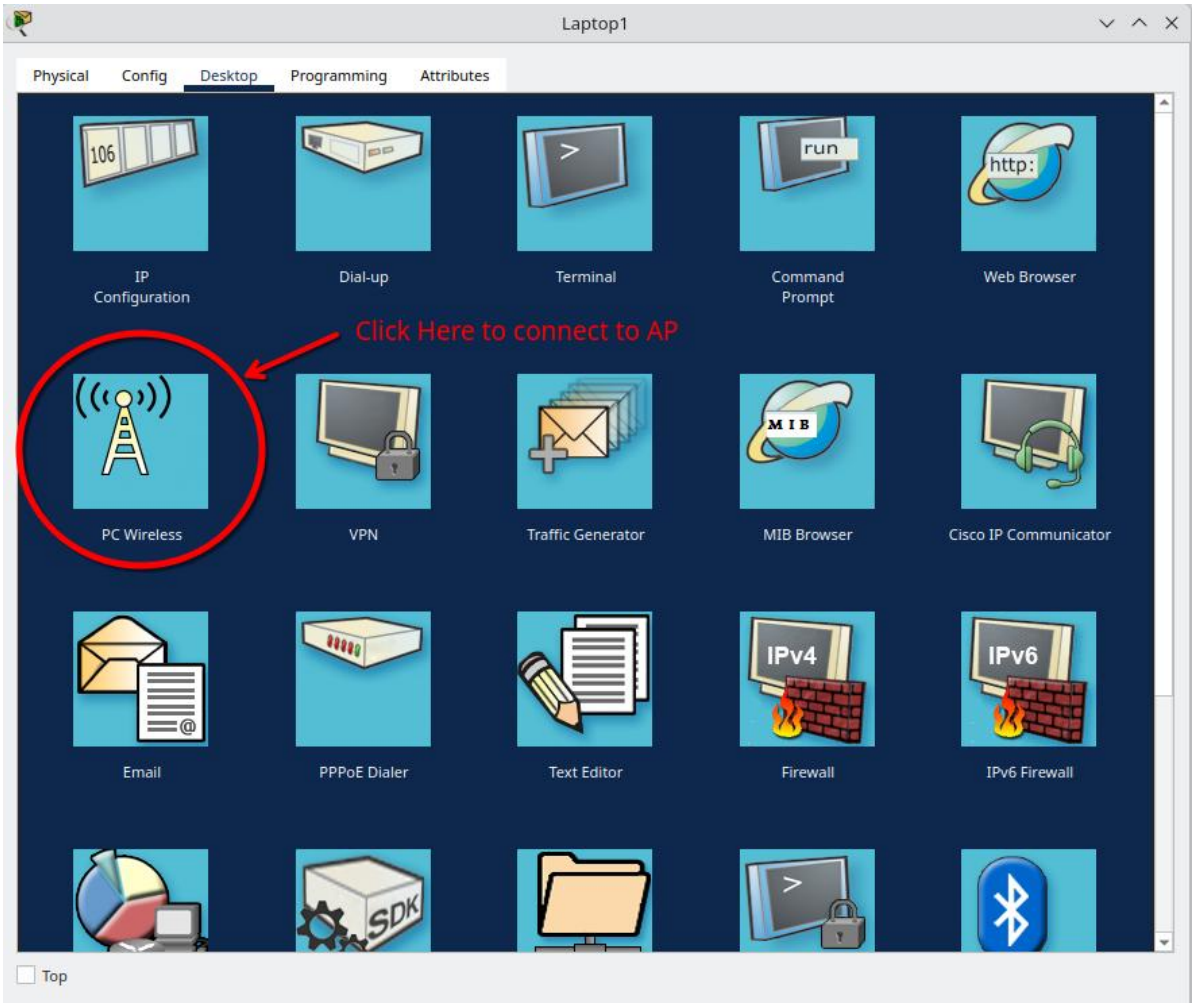
Access Point

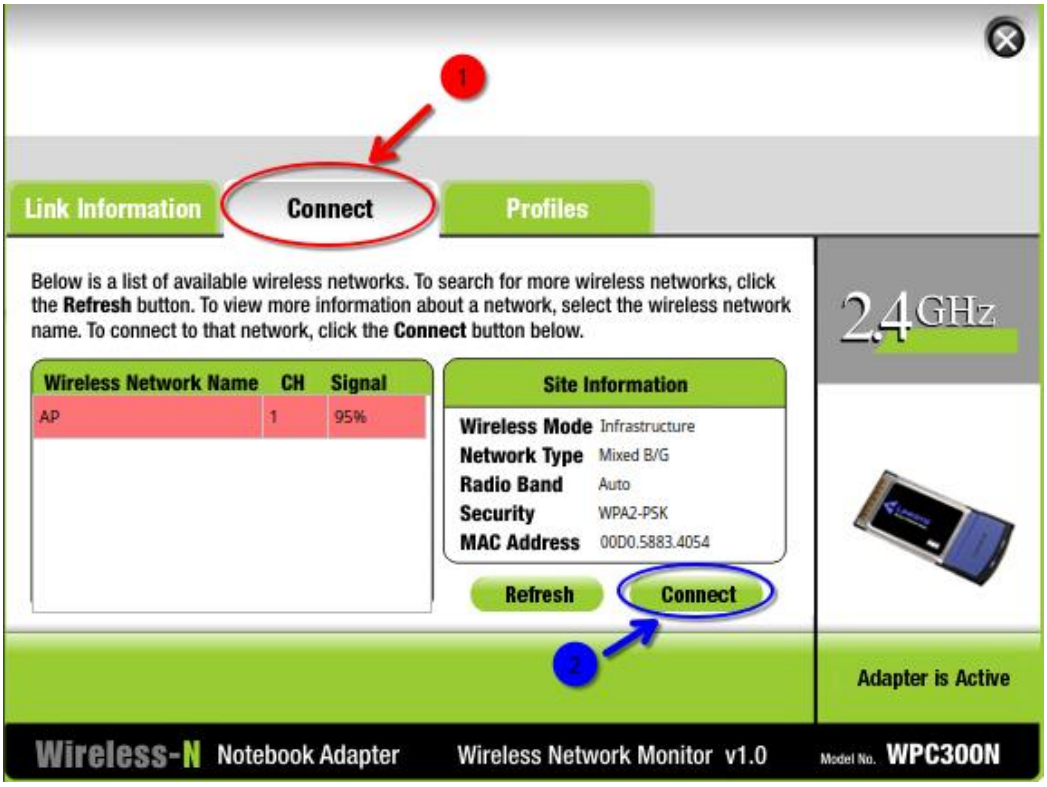


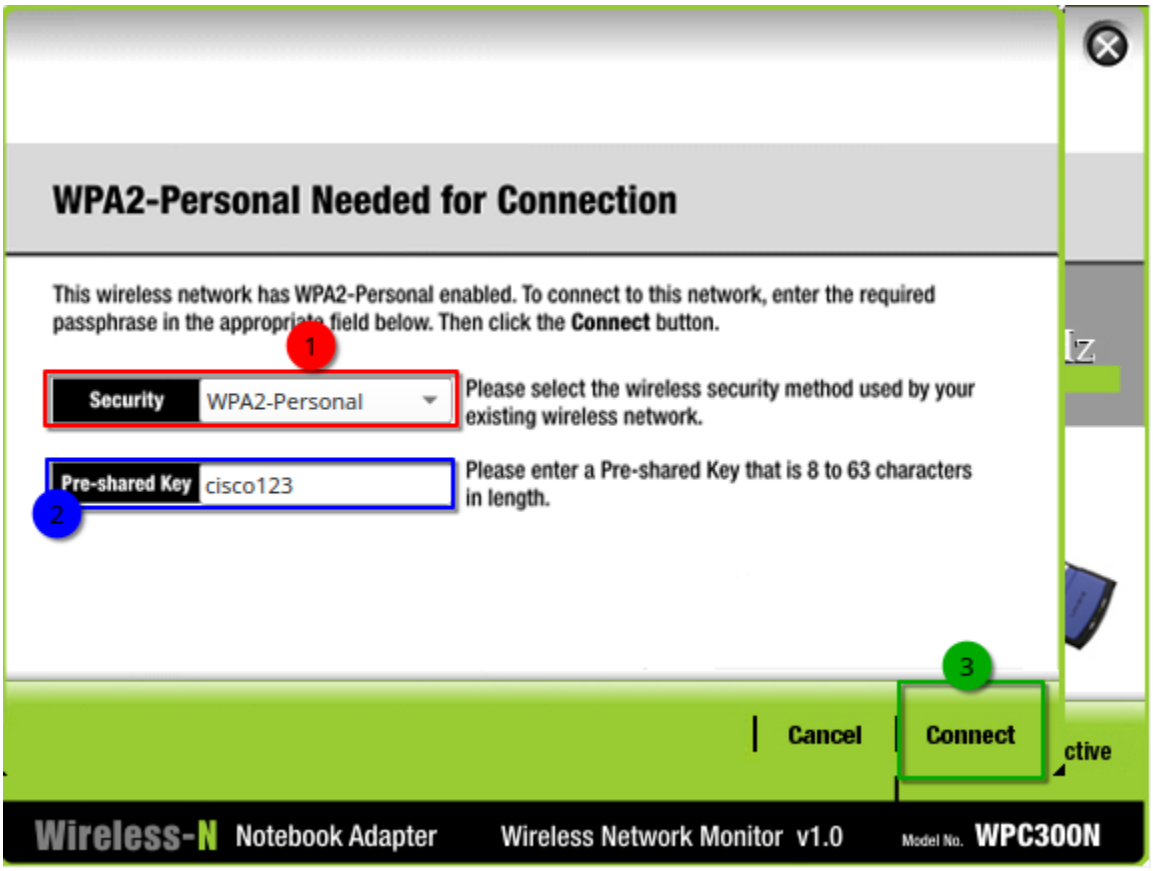
Laptop

1. Power OFF the laptop.
2. Add Wireless Card (WPC300N).
3. Power ON the laptop.

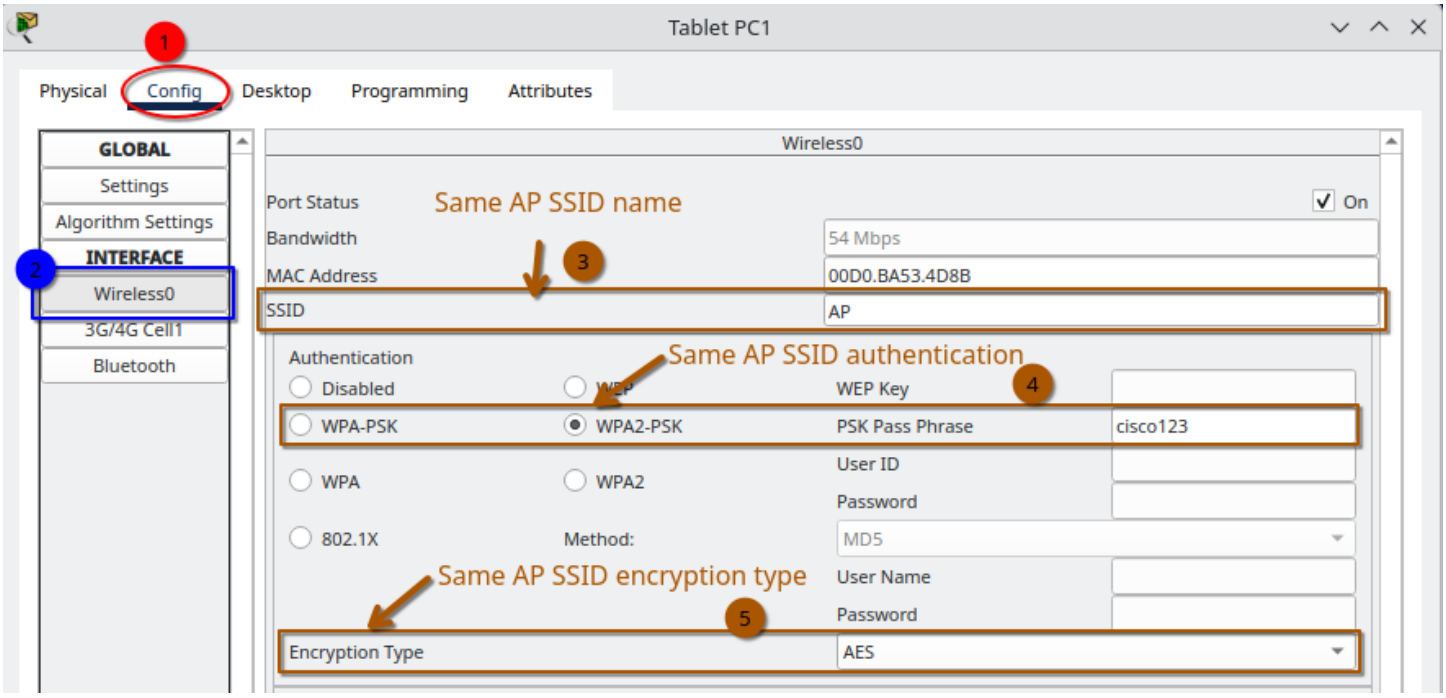


4. 
Laptop1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Dial-up
Terminal
Command Prompt
Web Browser
Click Here to connect to AP
PC Wireless
VPN
Traffic Generator
MIB Browser
Cisco IP Communicator
Email
PPPoE Dialer
Text Editor
Firewall
IPv6 Firewall
Top

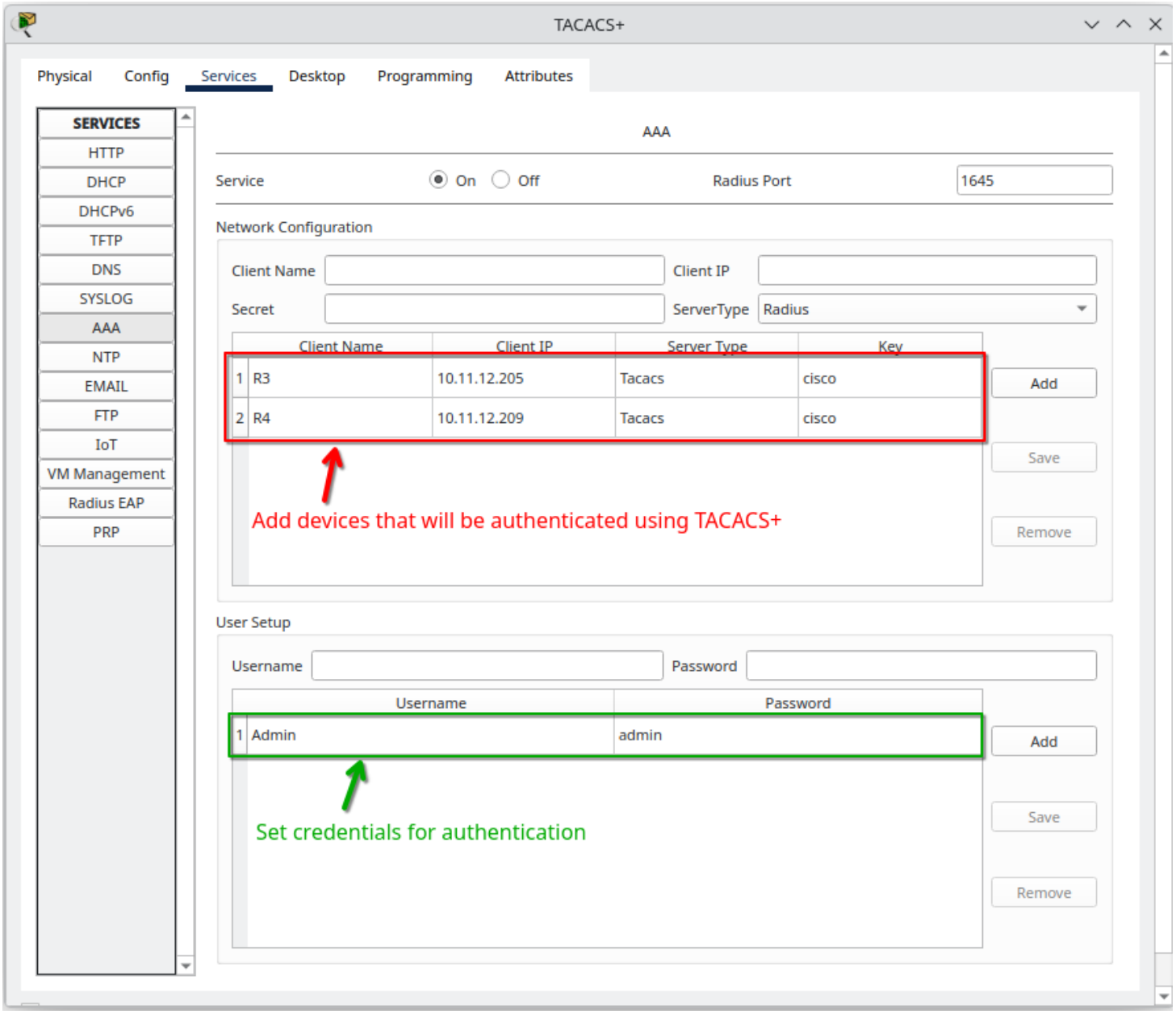
5. 
1
Link Information
Connect
Profiles
Below is a list of available wireless networks. To search for more wireless networks, click the Refresh button. To view more information about a network, select the wireless network name. To connect to that network, click the Connect button below.
Wireless Network Name
CH
Signal
AP
1
95%
Site Information
Wireless Mode Infrastructure
Network Type Mixed B/G
Radio Band Auto
Security WPA2-PSK
MAC Address 00D0.5883.4054
2.4GHz
Refresh
Connect
2
Adapter is Active
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No. WPC300N

6. 
WPA2-Personal Needed for Connection
This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the Connect button.
1
Security
WPA2-Personal
Please select the wireless security method used by your existing wireless network.
Pre-shared Key
cisco123
2
Please enter a Pre-shared Key that is 8 to 63 characters in length.
3
Cancel
Connect
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No. WPC300N

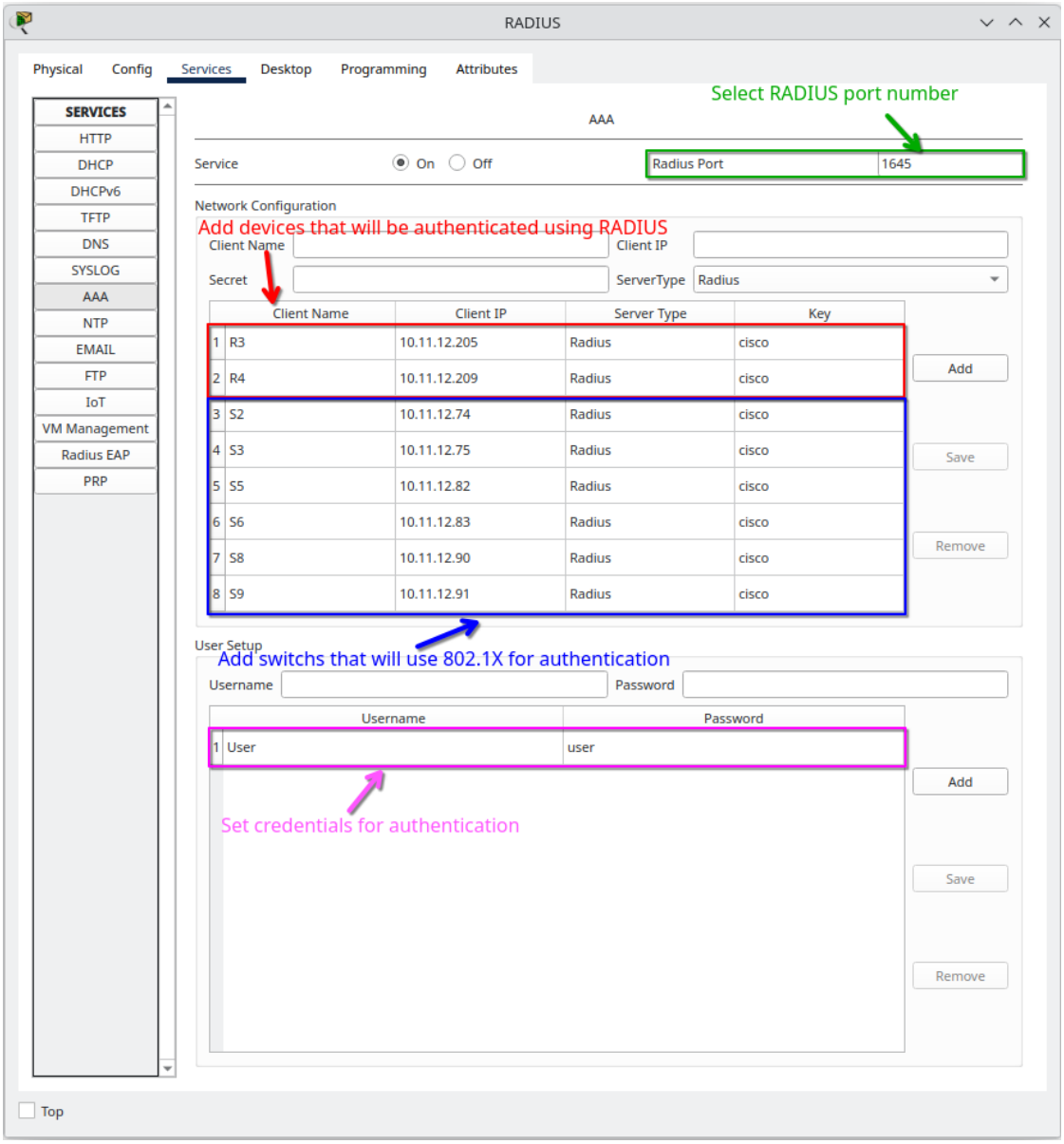
Tablet

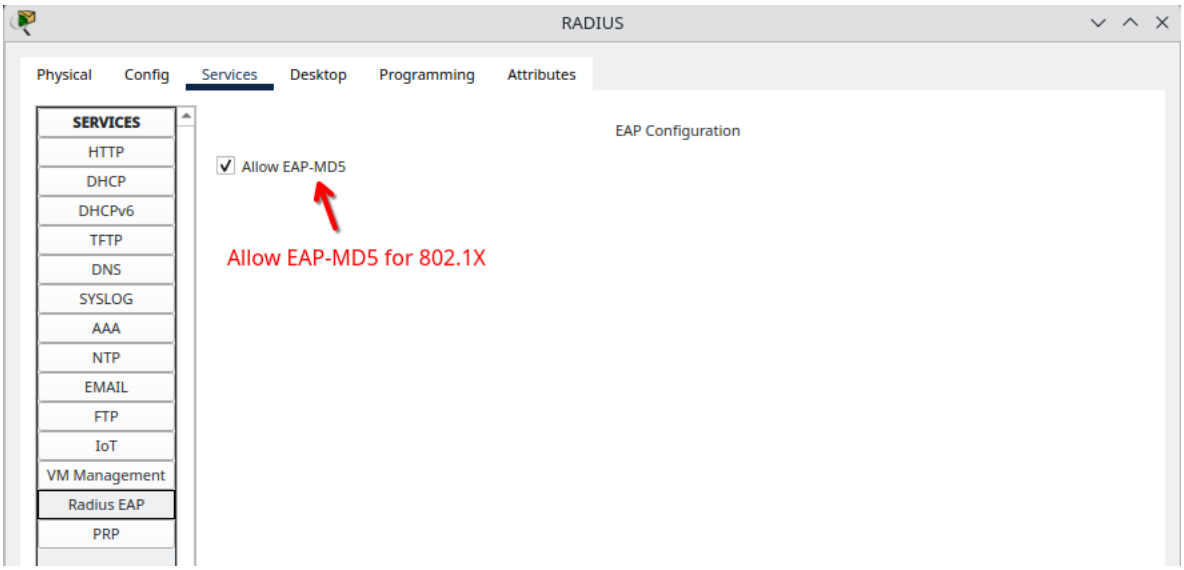

Tablet PC1
1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
2
Wireless0
3G/4G Cell1
Bluetooth
Wireless0
Port Status
Same AP SSID name
On
Bandwidth
54 Mbps
MAC Address
00D0.BA53.4D8B
3
SSID
AP
Authentication
Same AP SSID authentication
Disabled
WEP
WEP Key
4
WPA-PSK
WPA2-PSK
PSK Pass Phrase
cisco123
User ID
WPA
WPA2
Password
802.1X
Method:
MD5
Same AP SSID encryption type
User Name
5
Password
Encryption Type
AES

TACACS+ Server

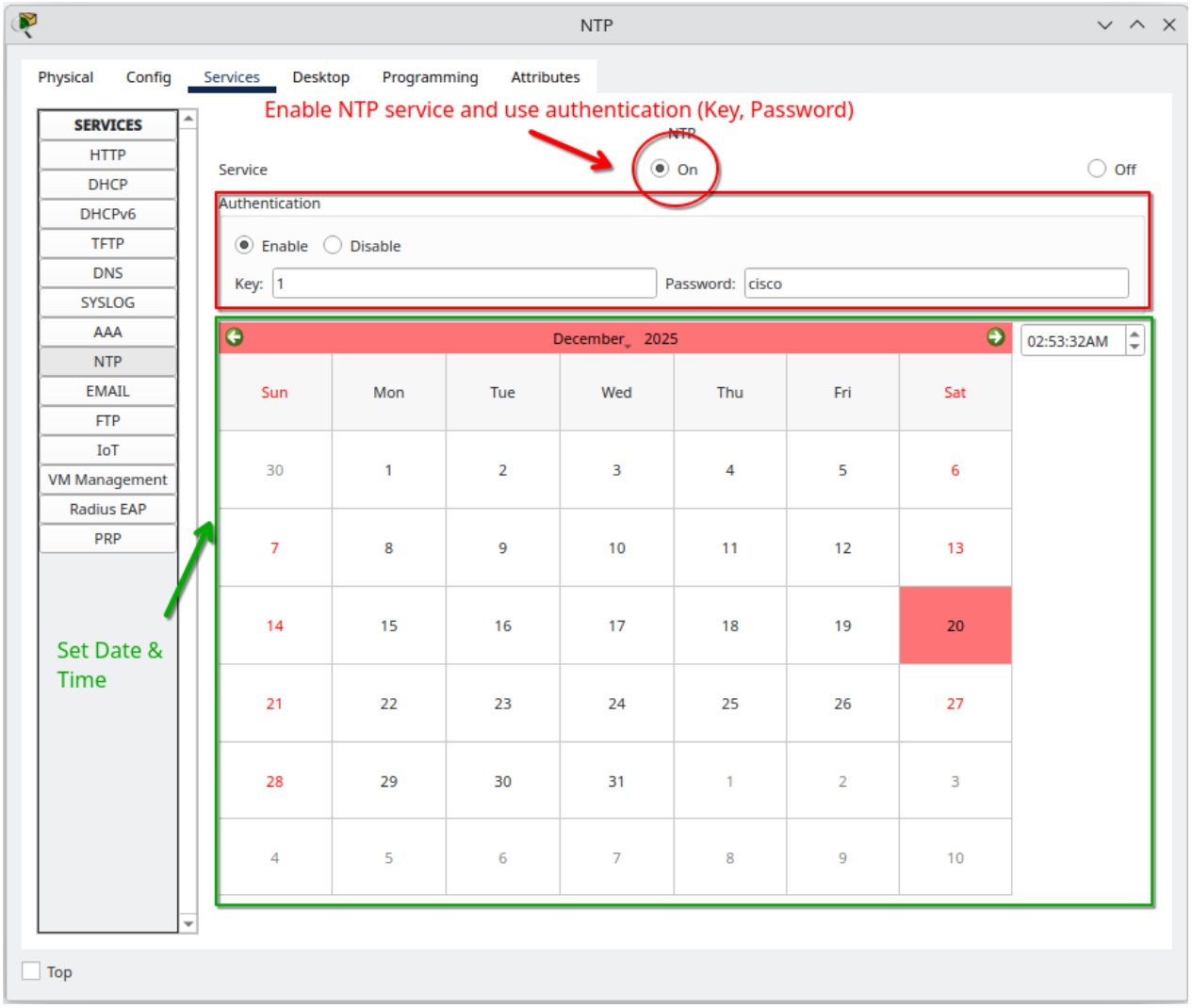


RADIUS Server

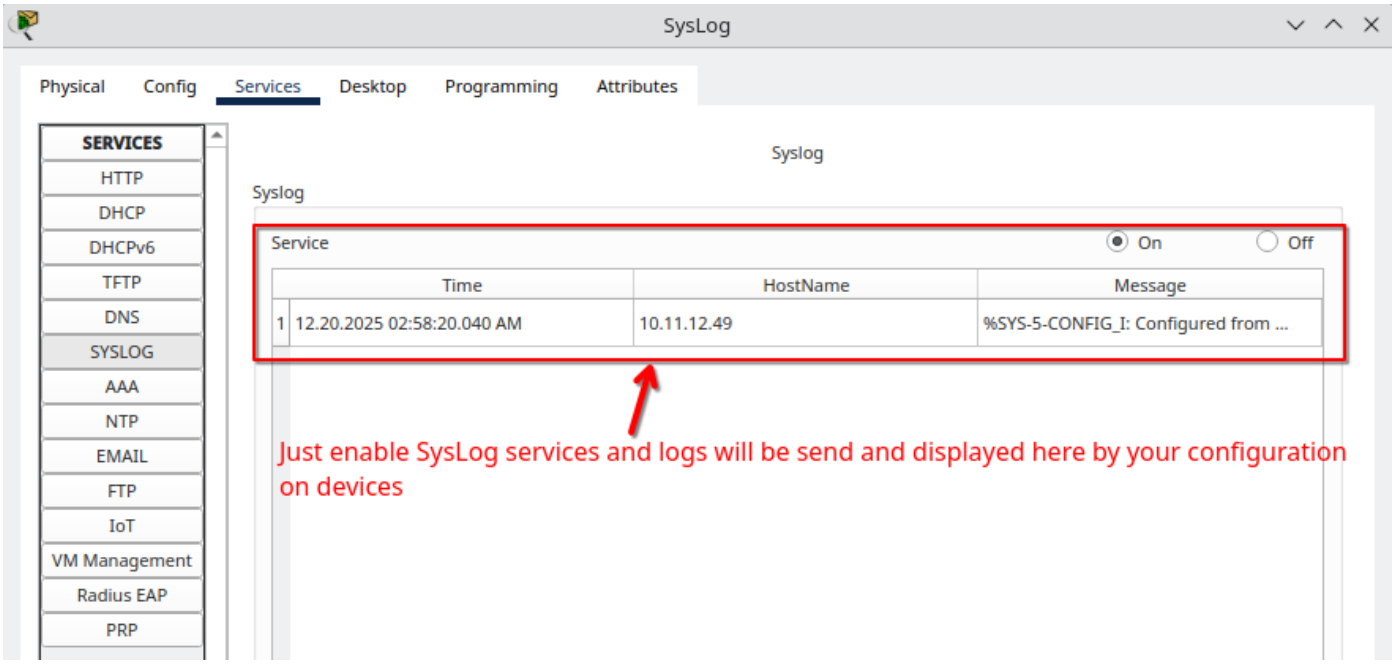




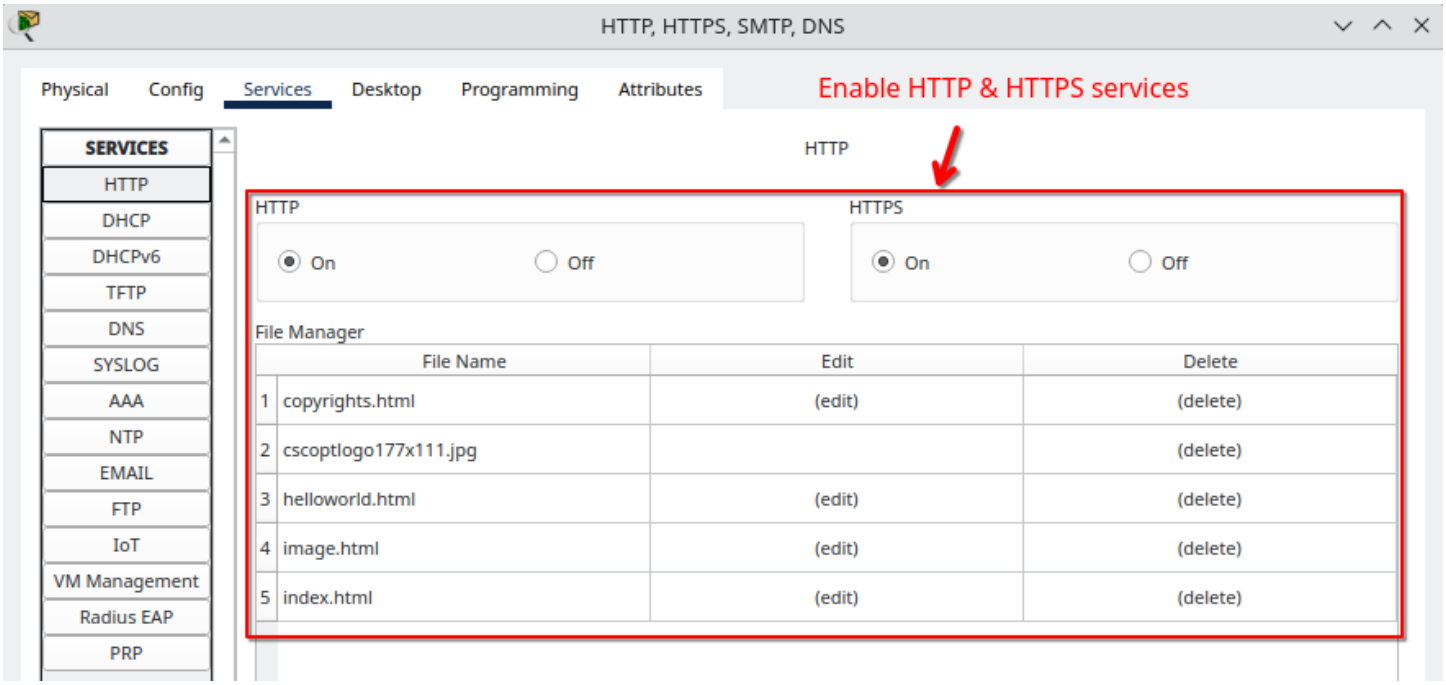
NTP Server

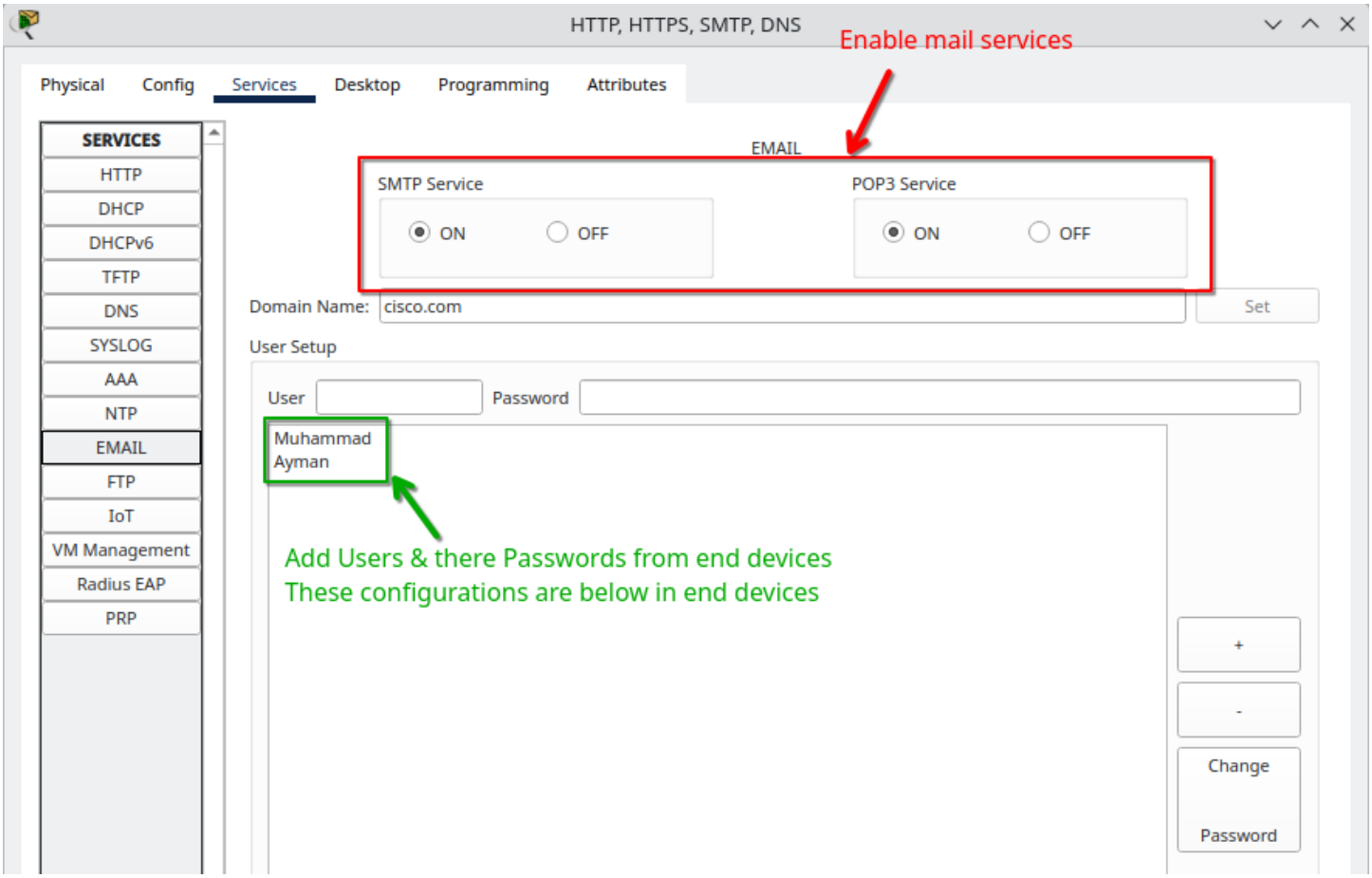


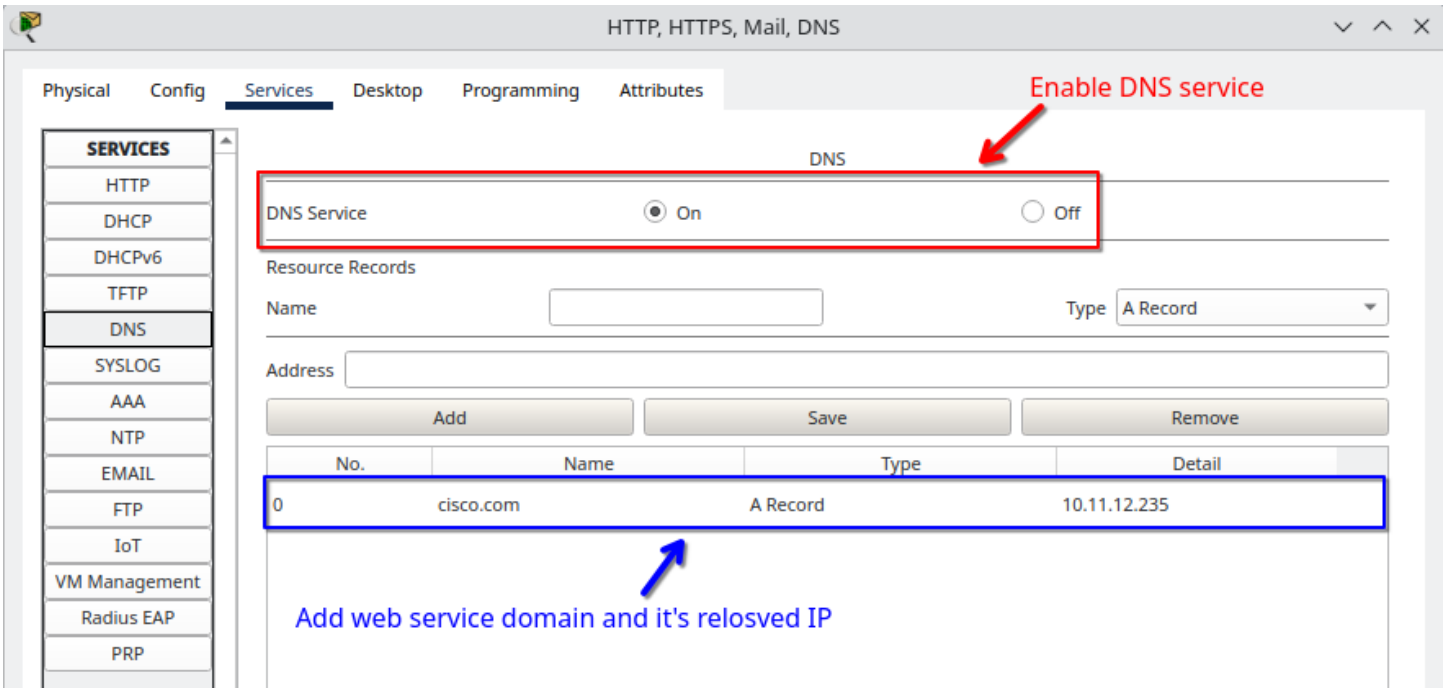
SysLog Server

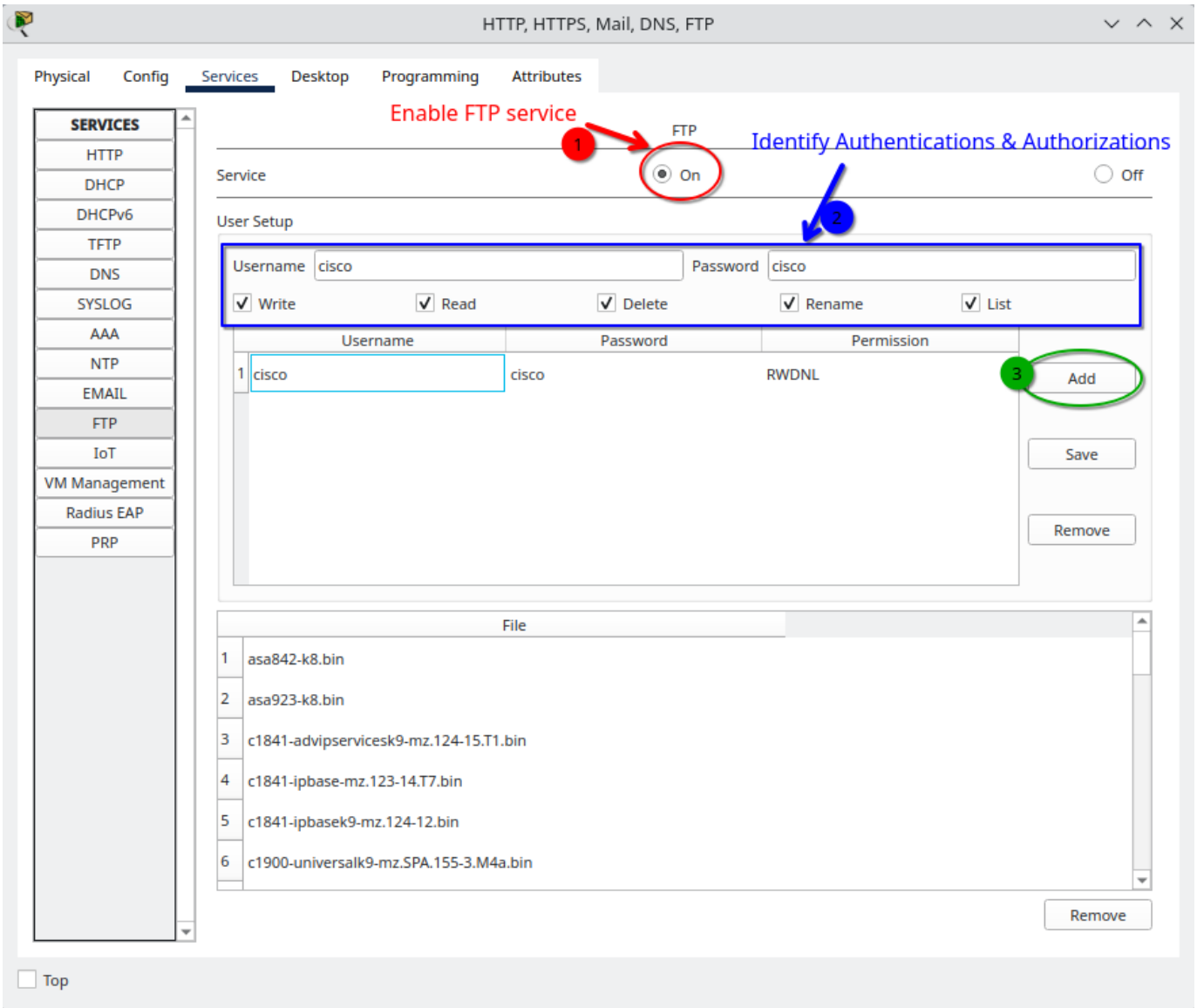


DMZ Server

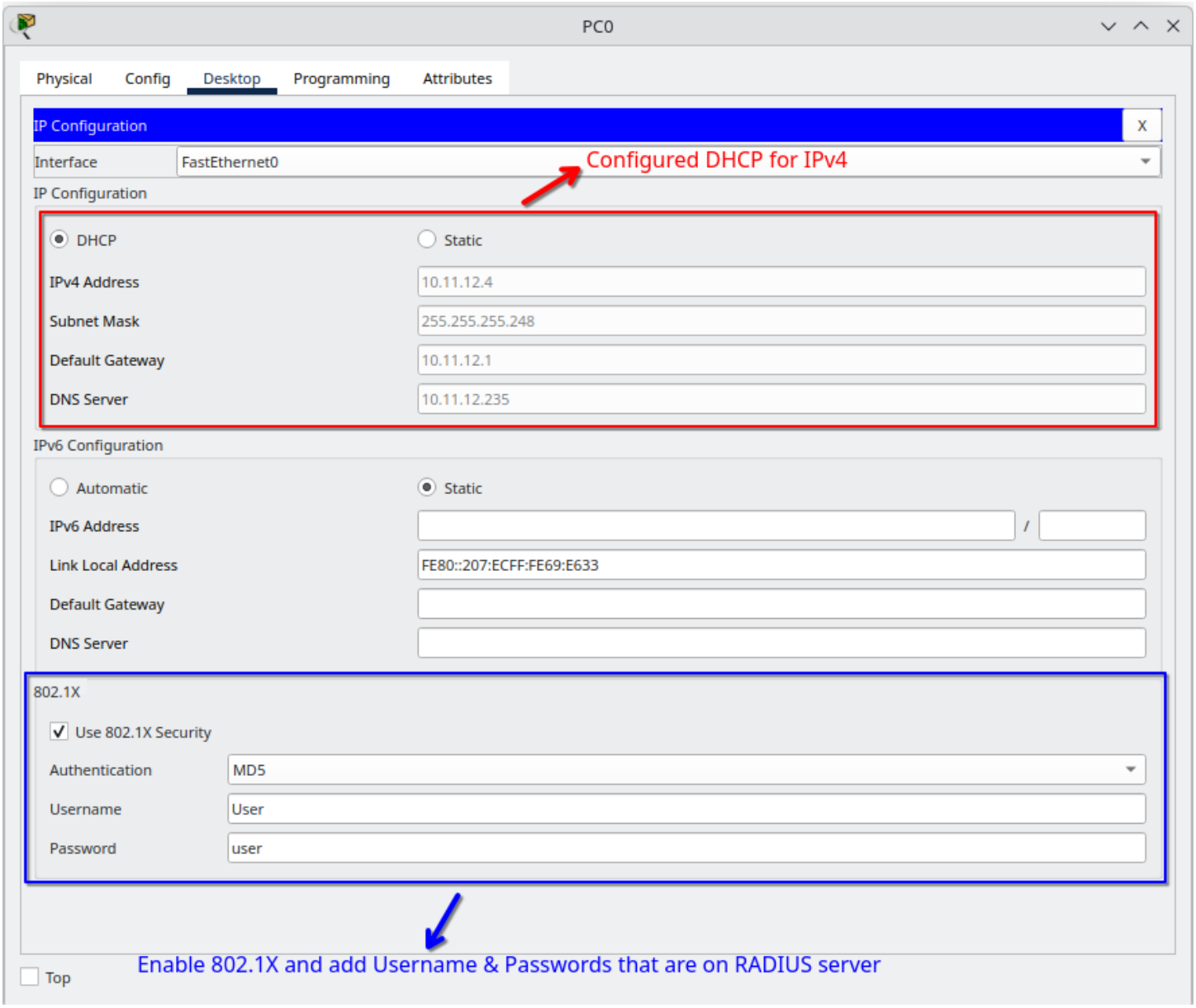

HTTP, HTTPS, SMTP, DNS
Physical
Config
Services
Desktop
Programming
Attributes
Enable HTTP & HTTPS services
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
PRP
HTTP
HTTP
On
Off
HTTPS
On
Off
File Manager
File Name
Edit
Delete
1 copyrights.html (edit) (delete)
2 cscoptlogo177x111.jpg (delete)
3 helloworld.html (edit) (delete)
4 image.html (edit) (delete)
5 index.html (edit) (delete)


HTTP, HTTPS, SMTP, DNS
Enable mail services
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
PRP
EMAIL
SMTP Service
ON
OFF
POP3 Service
ON
OFF
Domain Name:
cisco.com
Set
User Setup
User
Password
Muhammad Ayman
Add Users & there Passwords from end devices
These configurations are below in end devices
+
-
Change Password

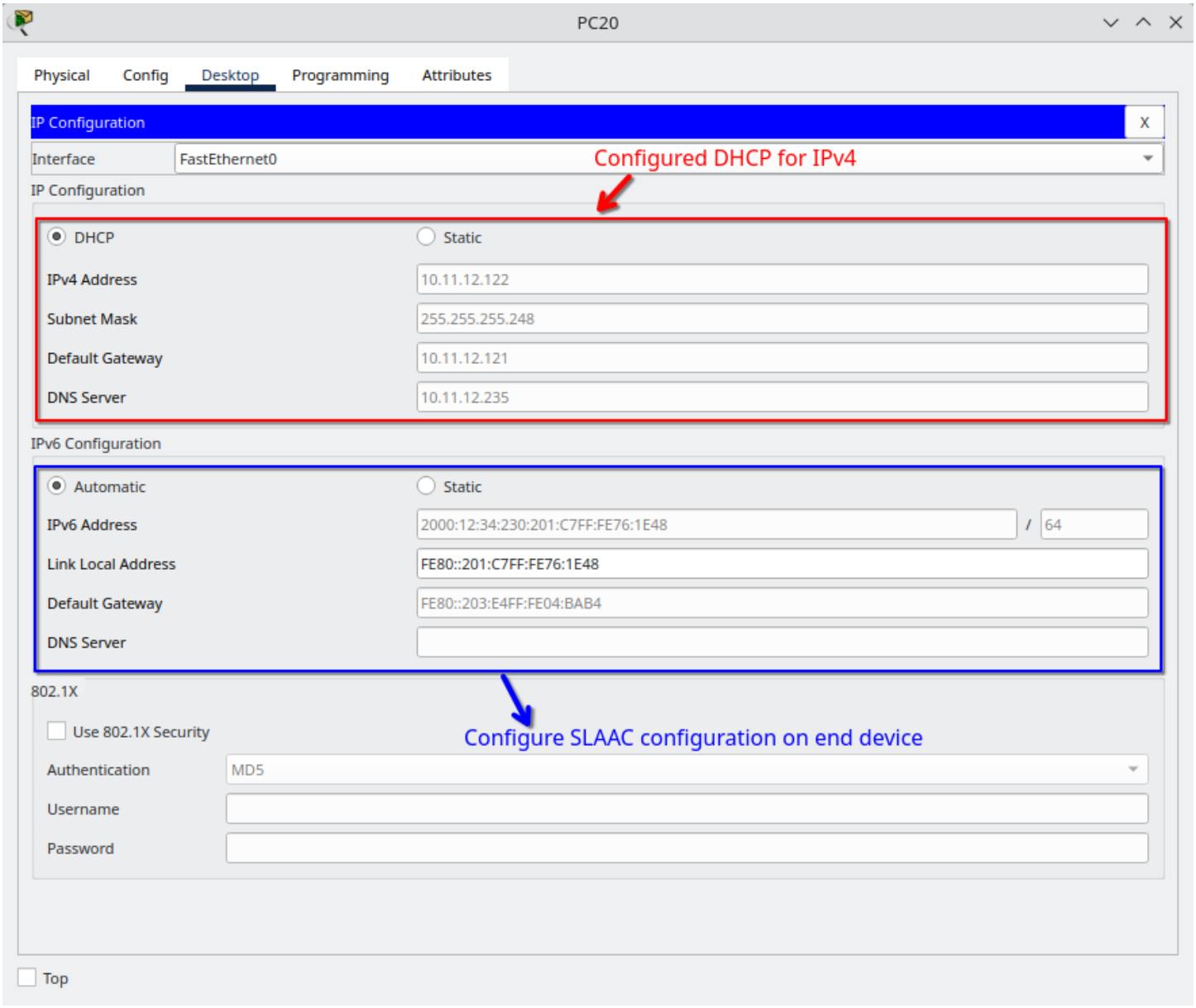

HTTP, HTTPS, Mail, DNS
Physical
Config
Services
Desktop
Programming
Attributes
Enable DNS service
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
PRP
DNS
DNS Service
On
Off
Resource Records
Name
Type
A Record
Address
Add
Save
Remove
No.
Name
Type
Detail
0
cisco.com
A Record
10.11.12.235
Add web service domain and it's relosved IP


HTTP, HTTPS, Mail, DNS, FTP
Physical
Config
Services
Desktop
Programming
Attributes
Enable FTP service
Identify Authentications & Authorizations
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
PRP
FTP
Service
On
Off
User Setup
Username
cisco
Password
cisco
Write
Read
Delete
Rename
List
Username
Password
Permission
1
cisco
cisco
RWDNL
Add
Save
Remove
File
1
asa842-k8.bin
2
asa923-k8.bin
3
c1841-advipservicesk9-mz.124-15.T1.bin
4
c1841-ipbase-mz.123-14.T7.bin
5
c1841-ipbasek9-mz.124-12.bin
6
c1900-universalk9-mz.SPA.155-3.M4a.bin
Remove
Top

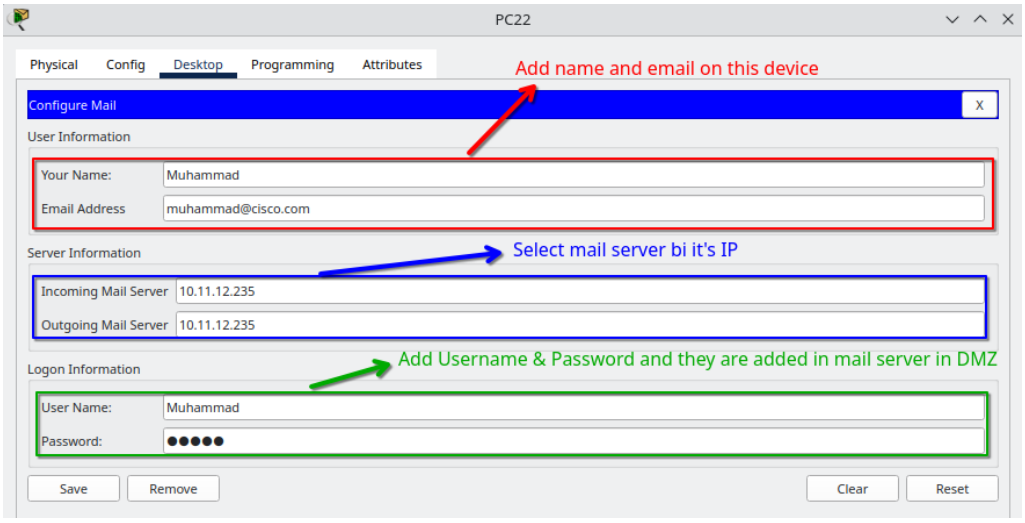
Others End Devices in Left-Side (PCs, Laptop, Tablet)



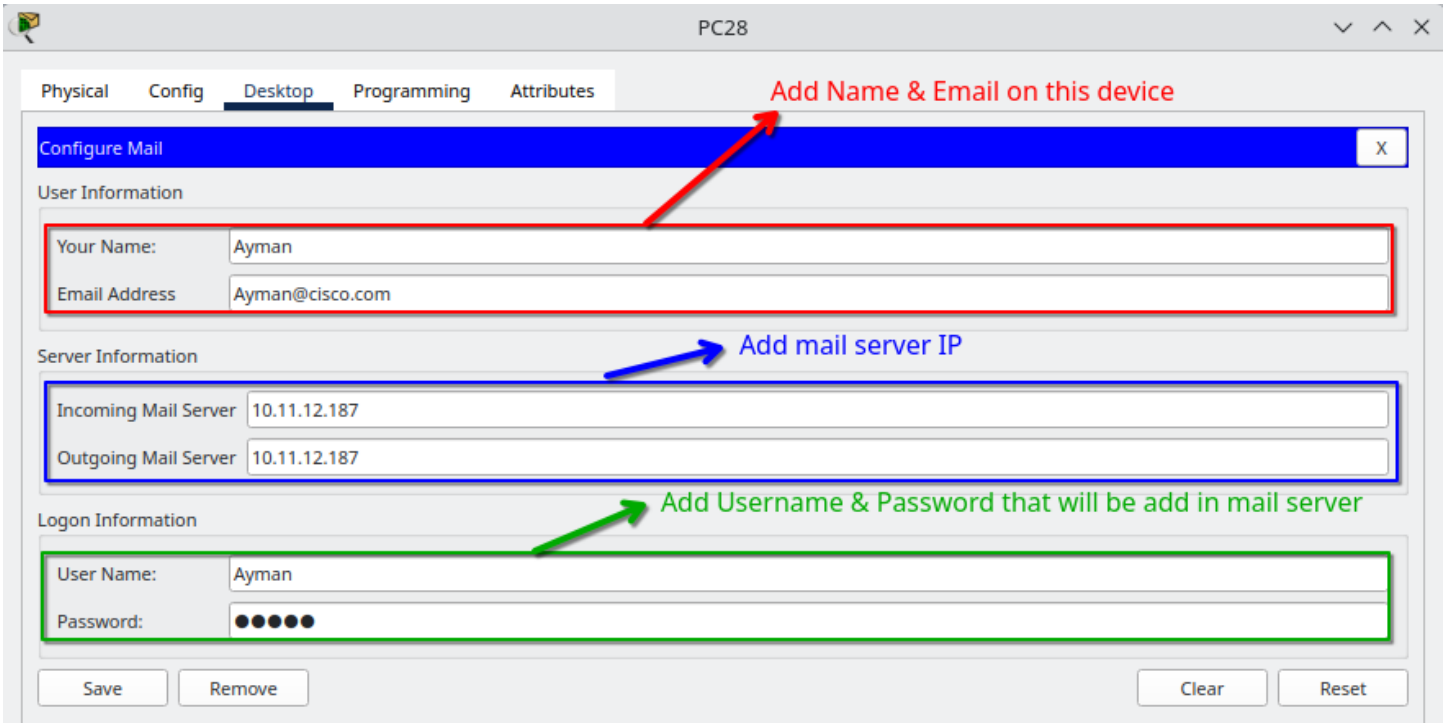
Others End Devices in Right-Side (PCs)



PC22 (Mail Settings)



PC28 (Mail Settings)



Notes

- All Servers have **static** IPs.
- Hardening All servers.
- DMZ and INSIDE zones have **static** IPs.
- When INSIDE wants to reach web server in DMZ, they reach it from OUTSIDE not directly from INSIDE to DMZ.

Check out the full project on GitHub

https://github.com/M0oham6d/Enterprise-Network-Design-and-Security-Implementation.git

Thanks 💙