# Comprehensive Network Security & Access Guide

This consolidated guide combines port security, STP security, VLAN security, DHCP snooping, zone-based firewall, ACL, AAA, and secure services configurations. Follow each section as a standalone task. Explanations are provided where available.  
**Remember, this not an official study material, I made it to help me with my study.**

# Switch & Router Security Configuration Guides

## Port Security

Lock down FastEthernet ports, set management SVI, limit MACs, learn sticky, restrict on violation, and shut unused ports.

### Management SVI (VLAN 1)

|  |  |
| --- | --- |
| Prompt | Command |
| Switch> | enable |
| Switch# | configure terminal |
| Switch(config)# | interface vlan 1 |
| Switch(config-if)# | ip address 10.10.10.2 255.255.255.0 |
| Switch(config-if)# | no shutdown |
| Switch(config-if)# | exit |
| Switch(config)# | exit |

### Port-Security on Fa0/1–2

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | interface range fastEthernet 0/1 – 0/2 |
| Switch(config-if-range)# | switchport mode access |
| Switch(config-if-range)# | switchport port-security |
| Switch(config-if-range)# | switchport port-security maximum 1 |
| Switch(config-if-range)# | switchport port-security violation restrict |
| Switch(config-if-range)# | switchport port-security mac-address sticky |
| Switch(config-if-range)# | exit |

### Shutdown Unused Ports

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | interface range fastEthernet 0/3 – 0/24 |
| Switch(config-if-range)# | shutdown |
| Switch(config-if-range)# | exit |
| Switch(config)# | exit |

### Verify Port-Security

|  |  |
| --- | --- |
| Prompt | Command |
| Switch# | show port-security interface fastEthernet 0/1 |
| Switch# | show port-security address |

## STP Security

Protect spanning-tree topology with root guard, BPDU guard, loop guard, and PortFast.

### Root Bridge Election

|  |  |
| --- | --- |
| Prompt | Command |
| Switch> | enable |
| Switch# | configure terminal |
| Switch(config)# | spanning-tree vlan 1 root primary |
| Switch(config)# | spanning-tree vlan 1 root secondary |
| Switch(config)# | exit |

### PortFast & BPDU Guard on Access Ports

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | interface range fastEthernet 0/1 – 0/22 |
| Switch(config-if-range)# | spanning-tree portfast |
| Switch(config-if-range)# | spanning-tree bpduguard enable |
| Switch(config-if-range)# | exit |

### Root Guard on Uplinks

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | interface range fastEthernet 0/23 – 0/24 |
| Switch(config-if-range)# | spanning-tree guard root |
| Switch(config-if-range)# | exit |

### Loop Guard

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | spanning-tree loopguard default |
| Switch(config)# | exit |

### Verify STP

|  |  |
| --- | --- |
| Prompt | Command |
| Switch# | show spanning-tree summary |
| Switch# | show spanning-tree interface gigabitEthernet 0/1 rootguard |

## Layer 2 VLAN Security

Lock down trunk negotiation, restrict VLANs, disable CDP, create management VLAN and SVI, configure router subinterface, and apply ACLs.

### Trunk Negotiation & VLANs

|  |  |
| --- | --- |
| Prompt | Command |
| Switch> | enable |
| Switch# | configure terminal |
| Switch(config)# | interface gigabitEthernet 0/1 |
| Switch(config-if)# | switchport mode trunk |
| Switch(config-if)# | switchport trunk native vlan 15 |
| Switch(config-if)# | switchport trunk allowed vlan 5,10,15 |
| Switch(config-if)# | switchport nonegotiate |
| Switch(config-if)# | exit |

### Disable CDP on Uplink

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | interface gigabitEthernet 0/1 |
| Switch(config-if)# | no cdp enable |
| Switch(config-if)# | exit |
| Switch(config)# | exit |

### Management VLAN & SVI

|  |  |
| --- | --- |
| Prompt | Command |
| Switch# | configure terminal |
| Switch(config)# | vlan 20 |
| Switch(config-vlan)# | name Management |
| Switch(config-vlan)# | exit |
| Switch(config)# | interface vlan 20 |
| Switch(config-if)# | ip address 192.168.20.1 255.255.255.0 |
| Switch(config-if)# | no shutdown |
| Switch(config-if)# | exit |
| Switch(config)# | exit |

### Router Subinterface for VLAN 20

|  |  |
| --- | --- |
| Prompt | Command |
| Router> | enable |
| Router# | configure terminal |
| Router(config)# | interface g0/0.20 |
| Router(config-subif)# | encapsulation dot1q 20 |
| Router(config-subif)# | ip address 192.168.20.254 255.255.255.0 |
| Router(config-subif)# | exit |
| Router(config)# | exit |

### ACL Configuration

|  |  |
| --- | --- |
| Prompt | Command |
| Router> | enable |
| Router# | configure terminal |
| Router(config)# | access-list 101 deny ip any 192.168.20.0 0.0.0.255 |
| Router(config)# | access-list 101 permit ip any any |
| Router(config)# | access-list 102 permit ip host 192.168.20.50 any |
| Router(config)# | exit |
| Router(config)# | line vty 0 4 |
| Router(config-line)# | access-class 102 in |
| Router(config-line)# | exit |
| Router(config)# | exit |

## DHCP Snooping

Enable DHCP snooping globally and per VLAN, trust uplinks, rate-limit untrusted ports, and verify.

### Secure Trunks

|  |  |
| --- | --- |
| Prompt | Command |
| Switch> | enable |
| Switch# | configure terminal |
| Switch(config)# | interface range gigabitEthernet 0/1 – 0/2 |
| Switch(config-if-range)# | switchport mode trunk |
| Switch(config-if-range)# | switchport trunk native vlan 100 |
| Switch(config-if-range)# | switchport nonegotiate |
| Switch(config-if-range)# | exit |

### Enable DHCP Snooping

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | ip dhcp snooping |
| Switch(config)# | ip dhcp snooping vlan 10,20,99 |
| Switch(config)# | exit |

### Trust & Rate-Limit

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | interface gigabitEthernet 0/1 |
| Switch(config-if)# | ip dhcp snooping trust |
| Switch(config-if)# | exit |
| Switch(config)# | interface range fastEthernet 0/3 – 0/24 |
| Switch(config-if-range)# | ip dhcp snooping limit rate 5 |
| Switch(config-if-range)# | exit |
| Switch(config)# | exit |

### Verify DHCP Snooping

|  |  |
| --- | --- |
| Prompt | Command |
| Switch# | show ip dhcp snooping |
| Switch# | show ip dhcp snooping binding |

## Zone-Based Policy Firewall (ZPF)

Define security zones, assign interfaces and IPs, configure class-maps and policy-maps, apply service policy, and verify.

### Define Security Zones

|  |  |
| --- | --- |
| Prompt | Command |
| Router> | enable |
| Router# | configure terminal |
| Router(config)# | zone security IN-ZONE |
| Router(config)# | zone security OUT-ZONE |
| Router(config)# | exit |

### Assign Interfaces & IP Addresses

|  |  |
| --- | --- |
| Prompt | Command |
| Router(config)# | interface gigabitEthernet 0/1 |
| Router(config-if)# | ip address 192.168.3.1 255.255.255.0 |
| Router(config-if)# | zone-member security IN-ZONE |
| Router(config-if)# | exit |
| Router(config)# | interface serial0/0/1 |
| Router(config-if)# | ip address 10.2.2.1 255.255.255.252 |
| Router(config-if)# | zone-member security OUT-ZONE |
| Router(config-if)# | exit |
| Router(config)# | exit |

### Class-Map & Policy-Map

|  |  |
| --- | --- |
| Prompt | Command |
| Router(config)# | access-list 101 permit ip 192.168.3.0 0.0.0.255 any |
| Router(config)# | class-map type inspect match-all IN-NET-CLASS |
| Router(config-cmap)# | match access-group 101 |
| Router(config-cmap)# | exit |
| Router(config)# | policy-map type inspect IN-2-OUT-PMAP |
| Router(config-pmap)# | class type inspect IN-NET-CLASS |
| Router(config-pmap-c)# | inspect |
| Router(config-pmap-c)# | exit |
| Router(config-pmap)# | exit |
| Router(config)# | exit |

### Apply Zone-Pair & Service-Policy

|  |  |
| --- | --- |
| Prompt | Command |
| Router(config)# | zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE |
| Router(config-sec-zone-pair)# | service-policy type inspect IN-2-OUT-PMAP |
| Router(config-sec-zone-pair)# | exit |
| Router(config)# | exit |

### Verify Firewall & Sessions

|  |  |
| --- | --- |
| Prompt | Command |
| Router# | show zone security |
| Router# | show policy-map type inspect zone-pair |
| Router# | show policy-map type inspect zone-pair sessions |

# ACL & AAA Configuration Guides

## ACL Demonstration

Observe ACL impact: view ACLs, remove ACL, and verify access.

### View Current ACL Configuration

|  |  |
| --- | --- |
| Prompt | Command |
| R1# | show access-lists |
| R1# | show run | include interface|access |

### Remove ACL from Interface

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface Serial0/0/0 |
| R1(config-if)# | no ip access-group 11 out |
| R1(config-if)# | exit |

### Delete ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | no access-list 11 |

### Verify Access Restoration

|  |  |
| --- | --- |
| Prompt | Command |
| PC1> | ping 192.168.30.12 |
| PC1> | ping 192.168.31.12 |

## Numbered Standard IPv4 ACLs

Restrict specific source networks with numbered standard ACLs on R2 and R3.

### Configure and Apply ACL on R2

|  |  |
| --- | --- |
| Prompt | Command |
| R2(config)# | access-list 1 deny 192.168.11.0 0.0.0.255 |
| R2(config)# | access-list 1 permit any |
| R2(config)# | interface GigabitEthernet0/0 |
| R2(config-if)# | ip access-group 1 out |

### Configure and Apply ACL on R3

|  |  |
| --- | --- |
| Prompt | Command |
| R3(config)# | access-list 1 deny 192.168.10.0 0.0.0.255 |
| R3(config)# | access-list 1 permit any |
| R3(config)# | interface GigabitEthernet0/0 |
| R3(config-if)# | ip access-group 1 out |

### Verify ACLs

|  |  |
| --- | --- |
| Prompt | Command |
| R2# | show access-lists |
| R3# | show access-lists |

## Named Standard IPv4 ACLs

Create and apply a named standard ACL to protect a file server.

### Configure Named ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ip access-list standard File\_Server\_Restrictions |
| R1(config-std-nacl)# | permit host 192.168.20.4 |
| R1(config-std-nacl)# | permit host 192.168.100.100 |
| R1(config-std-nacl)# | deny any |

### Apply Named ACL to Interface

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface FastEthernet0/1 |
| R1(config-if)# | ip access-group File\_Server\_Restrictions out |

### Verify Named ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1# | show access-lists |
| R1# | show ip interface FastEthernet0/1 |

## Extended ACLs (Scenario 1)

Permit specific FTP and HTTP/ICMP traffic using extended ACLs.

### Configure Extended Numbered ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp |
| R1(config)# | access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62 |

### Apply Numbered ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface GigabitEthernet0/0 |
| R1(config-if)# | ip access-group 100 in |

### Configure Extended Named ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ip access-list extended HTTP\_ONLY |
| R1(config-ext-nacl)# | permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www |
| R1(config-ext-nacl)# | permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62 |

### Apply Named ACL

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface GigabitEthernet0/1 |
| R1(config-if)# | ip access-group HTTP\_ONLY in |

## IP ACLs to Mitigate Attacks

Use ACLs to restrict management and service access on edge routers.

### Create Numbered IP ACL 120 on R1

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | access-list 120 permit udp any host 192.168.1.3 eq 53 |
| R1(config)# | access-list 120 permit tcp any host 192.168.1.3 eq smtp |
| R1(config)# | access-list 120 permit tcp any host 192.168.1.3 eq ftp |
| R1(config)# | access-list 120 deny tcp any host 192.168.1.3 eq 443 |
| R1(config)# | access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22 |

### Apply ACL 120 on R1

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface Serial0/0/0 |
| R1(config-if)# | ip access-group 120 in |
| R1(config-if)# | exit |

### Modify ACL 120 for ICMP

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ip access-list extended 120 |
| R1(config-ext-nacl)# | permit icmp any any echo-reply |
| R1(config-ext-nacl)# | permit icmp any any unreachable |
| R1(config-ext-nacl)# | deny icmp any any |
| R1(config-ext-nacl)# | permit ip any any |

### Secure R3 Edge Router

|  |  |
| --- | --- |
| Prompt | Command |
| R3(config)# | access-list 110 permit ip any any |

## Local AAA for Console and VTY Access

Configure local AAA authentication for console and SSH on R1.

### Configure Local User

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | username Admin1 secret admin1pa55 |

### Enable AAA for Console

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | aaa new-model |
| R1(config)# | aaa authentication login default local |
| R1(config)# | line console 0 |
| R1(config-line)# | login authentication default |

### Configure SSH Authentication

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ip domain-name netsec.com |
| R1(config)# | crypto key generate rsa modulus 1024 |
| R1(config)# | aaa authentication login SSH-LOGIN local |
| R1(config)# | line vty 0 4 |
| R1(config-line)# | login authentication SSH-LOGIN |
| R1(config-line)# | transport input ssh |

## Server-Based AAA with TACACS+ and RADIUS

Configure TACACS+ on R2 and RADIUS on R3 with backup local accounts.

### Backup Local Users

|  |  |
| --- | --- |
| Prompt | Command |
| R2(config)# | username Admin2 secret admin2pa55 |
| R3(config)# | username Admin3 secret admin3pa55 |

### Configure TACACS+ on R2

|  |  |
| --- | --- |
| Prompt | Command |
| R2(config)# | tacacs-server host 192.168.2.2 |
| R2(config)# | tacacs-server key tacacspa55 |
| R2(config)# | aaa new-model |
| R2(config)# | aaa authentication login default group tacacs+ local |
| R2(config)# | line console 0 |
| R2(config-line)# | login authentication default |

### Configure RADIUS on R3

|  |  |
| --- | --- |
| Prompt | Command |
| R3(config)# | radius-server host 192.168.3.2 |
| R3(config)# | radius-server key radiuspa55 |
| R3(config)# | aaa new-model |
| R3(config)# | aaa authentication login default group radius local |
| R3(config)# | line console 0 |
| R3(config-line)# | login authentication default |

# Secure Services Configuration Guides

## Configure Secure Passwords and SSH

Enable password encryption, strong secrets, RSA key generation, login blocking, and SSH on RTA and SW1.

### RTA Basic Security & SSH

|  |  |
| --- | --- |
| Prompt | Command |
| RTA(config)# | service password-encryption |
| RTA(config)# | security passwords min-length 10 |
| RTA(config)# | enable secret <your\_secret> |
| RTA(config)# | no ip domain-lookup |
| RTA(config)# | ip domain-name netsec.com |
| RTA(config)# | username admin secret <admin\_password> |
| RTA(config)# | crypto key generate rsa modulus 1024 |
| RTA(config)# | login block-for 180 attempts 4 within 120 |
| RTA(config)# | line vty 0 4 |
| RTA(config-line)# | transport input ssh |
| RTA(config-line)# | login local |
| RTA(config-line)# | exec-timeout 6 |
| RTA# | copy running-config startup-config |

### SW1 Basic Security & SSH

|  |  |
| --- | --- |
| Prompt | Command |
| SW1(config)# | service password-encryption |
| SW1(config)# | security passwords min-length 10 |
| SW1(config)# | enable secret <your\_secret> |
| SW1(config)# | no ip domain-lookup |
| SW1(config)# | ip domain-name netsec.com |
| SW1(config)# | username admin secret <admin\_password> |
| SW1(config)# | crypto key generate rsa modulus 1024 |
| SW1(config)# | interface vlan 1 |
| SW1(config-if)# | ip address 172.16.1.2 255.255.255.0 |
| SW1(config-if)# | no shutdown |
| SW1(config)# | ip default-gateway 172.16.1.1 |
| SW1(config)# | interface range Fa0/2-24, G0/2 |
| SW1(config-if-range)# | shutdown |
| SW1(config)# | line vty 0 4 |
| SW1(config-line)# | transport input ssh |
| SW1(config-line)# | login local |
| SW1(config-line)# | exec-timeout 6 |
| SW1# | copy running-config startup-config |

## Configure OSPF Authentication

Enable MD5 authentication for OSPF area 0 on all routers.

### Test Connectivity

|  |  |
| --- | --- |
| Prompt | Command |
| Router# | ping 10.1.1.2 |
| Router# | ping 10.2.2.1 |
| Router# | ping 192.168.3.1 |

### Enable OSPF MD5 Authentication

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | router ospf 1 |
| R1(config-router)# | area 0 authentication message-digest |
| R2(config)# | router ospf 1 |
| R2(config-router)# | area 0 authentication message-digest |
| R3(config)# | router ospf 1 |
| R3(config-router)# | area 0 authentication message-digest |

### Configure OSPF Keys on Interfaces

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | interface g0/0/0 |
| R1(config-if)# | ip ospf message-digest-key 1 md5 MD5pa55 |
| R2(config)# | interface g0/0/0 |
| R2(config-if)# | ip ospf message-digest-key 1 md5 MD5pa55 |
| R3(config)# | interface g0/0/0 |
| R3(config-if)# | ip ospf message-digest-key 1 md5 MD5pa55 |

### Verify OSPF Authentication

|  |  |
| --- | --- |
| Prompt | Command |
| Router# | show ip ospf interface |
| Router# | show ip ospf neighbor |

## Configure and Verify Secure NTP

Set up NTP client authentication and synchronization on R1 and R2.

### Verify Server & Connectivity

|  |  |
| --- | --- |
| Prompt | Command |
| R1# | show ntp status |
| R1# | ping 209.165.200.225 |
| R2# | ping 209.165.200.225 |

### Configure NTP Client

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ntp server 209.165.200.225 |
| R2(config)# | ntp server 209.165.200.225 |

### Enable NTP Authentication

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ntp authenticate |
| R1(config)# | ntp trusted-key 1 |
| R1(config)# | ntp authentication-key 1 md5 NTPpa55 |
| R2(config)# | ntp authenticate |
| R2(config)# | ntp trusted-key 1 |
| R2(config)# | ntp authentication-key 1 md5 NTPpa55 |

### Verify NTP Configuration

|  |  |
| --- | --- |
| Prompt | Command |
| R1# | show clock detail |
| R1# | show ntp status |
| R1# | show ntp associations |

## Syslog, NTP & SSH Operations

Configure remote SSH access, syslog servers, switch timestamps, and NTP synchronization.

### Secure Remote SSH on R1

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | enable secret cisco12345 |
| R1(config)# | no ip domain-lookup |
| R1(config)# | ip domain-name example.com |
| R1(config)# | username SSHuser secret SSHuserpass |
| R1(config)# | crypto key generate rsa modulus 1024 |
| R1(config)# | login block-for 300 attempts 4 within 120 |
| R1(config)# | line vty 0 4 |
| R1(config-line)# | transport input ssh |
| R1(config-line)# | login local |
| R1(config-line)# | exec-timeout 5 |

### Configure Syslog

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | logging 10.0.1.254 |
| S1(config)# | logging 10.0.1.254 |
| S2(config)# | logging 10.0.1.254 |

### Enable Switch Timestamps

|  |  |
| --- | --- |
| Prompt | Command |
| S1(config)# | service timestamps log datetime msec |
| S2(config)# | service timestamps log datetime msec |

### Configure NTP on R1

|  |  |
| --- | --- |
| Prompt | Command |
| R1(config)# | ntp server 64.103.224.2 |

### Verify Operations

|  |  |
| --- | --- |
| Prompt | Command |
| R1# | show logging |
| S1# | show clock |
| R1# | show ntp status |