# Switch & Router Security Configuration Guides

## 1. 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 |

## 2. 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 |

## 3. 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 |

## 4. 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 |

## 5. 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 |