# Network Security and Access Configuration Guide

This guide provides step-by-step instructions for securing network devices, configuring access control, and enabling essential services. Designed for beginners, each section includes a plain-language explanation followed by command tables.

## 1. Port Security

Port Security limits which devices can connect to switch ports by controlling MAC addresses and shutting down unused ports. Use this to prevent unauthorized devices on your network.

### Configure Management IP

Assign an IP to VLAN 1 on the switch so you can manage it remotely. Example: 10.10.10.2/24.

|  |  |
| --- | --- |
| 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 |

### Enable Port Security on Access Ports

Restrict ports Fa0/1-2 to one MAC address, learn it automatically (sticky), and shut down if violated.

|  |  |
| --- | --- |
| Prompt | Command |
| Switch(config)# | interface range fastEthernet 0/1-2 |
| 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

Disable all other FastEthernet ports (0/3-0/24) to reduce open vulnerability points.

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

### Verify Port Security

Check the status and learned MAC addresses on port Fa0/1.

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

## 2. ACL Demonstration

Access Control Lists (ACLs) filter traffic by IP addresses or protocols. First, observe existing ACLs, then remove and delete an ACL to restore access.

### View Current ACLs

See all ACL entries and where they are applied.

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

### Remove ACL from Interface

Take off ACL 11 from Serial0/0/0 to allow all traffic again.

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

### Delete ACL

Permanently remove ACL 11 from the router.

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

### Verify Access Restoration

Ping two IPs from PC1 to confirm connectivity is back.

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

## 3. Configure Secure Passwords and SSH

Protect device access by encrypting passwords, setting minimum length, and enabling secure SSH login.

### RTA Security & SSH Setup

On router RTA: encrypt passwords, set a strong secret, disable DNS lookup, create a user, generate RSA keys, and require SSH.

|  |  |
| --- | --- |
| Prompt | Command |
| RTA(config)# | service password-encryption |
| RTA(config)# | security passwords min-length 10 |
| RTA(config)# | enable secret myEnableSecret |
| RTA(config)# | no ip domain-lookup |
| RTA(config)# | ip domain-name netsec.com |
| RTA(config)# | username admin secret AdminPa55! |
| 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 |