CCNA 200-301 v1.1

MODULE 5 — Security Fundamentals

Complete Hands-on Training Labs

Topology • Sequential Device Configuration • Verification Output • Troubleshooting

NETWORK GUIDE ACADEMY

Instructor / Student Lab Guide

Scope: This workbook follows a single forward configuration sequence. Each device is configured once for the base lab. Later commands are only verification, controlled attack/failure tests, or deliberate security-policy changes.

Module 5 lab map

Lesson	Lab focus	Hands-on outcome
5.1	Security concepts: threats, vulnerabilities, exploits and mitigation	Guided security assessment
5.2	Security program elements: awareness, training and physical access	Security-control audit
5.3	Device access control using local passwords	Router + switch hardening
5.4	Password policy, complexity and alternatives	Policy + login lockout
5.5	IPsec remote access and site-to-site VPNs	Site-to-site IPsec demonstration
5.6	Access control lists	Standard + extended IPv4 ACLs
5.7	Layer 2 security	Port security + DHCP snooping + DAI
5.8	Authentication, authorization and accounting	TACACS+ with local fallback
5.9	Wireless security protocols	WPA/WPA2/WPA3 interpretation
5.10	WLAN with WPA2 PSK	WLC GUI + client verification

How to use this workbook

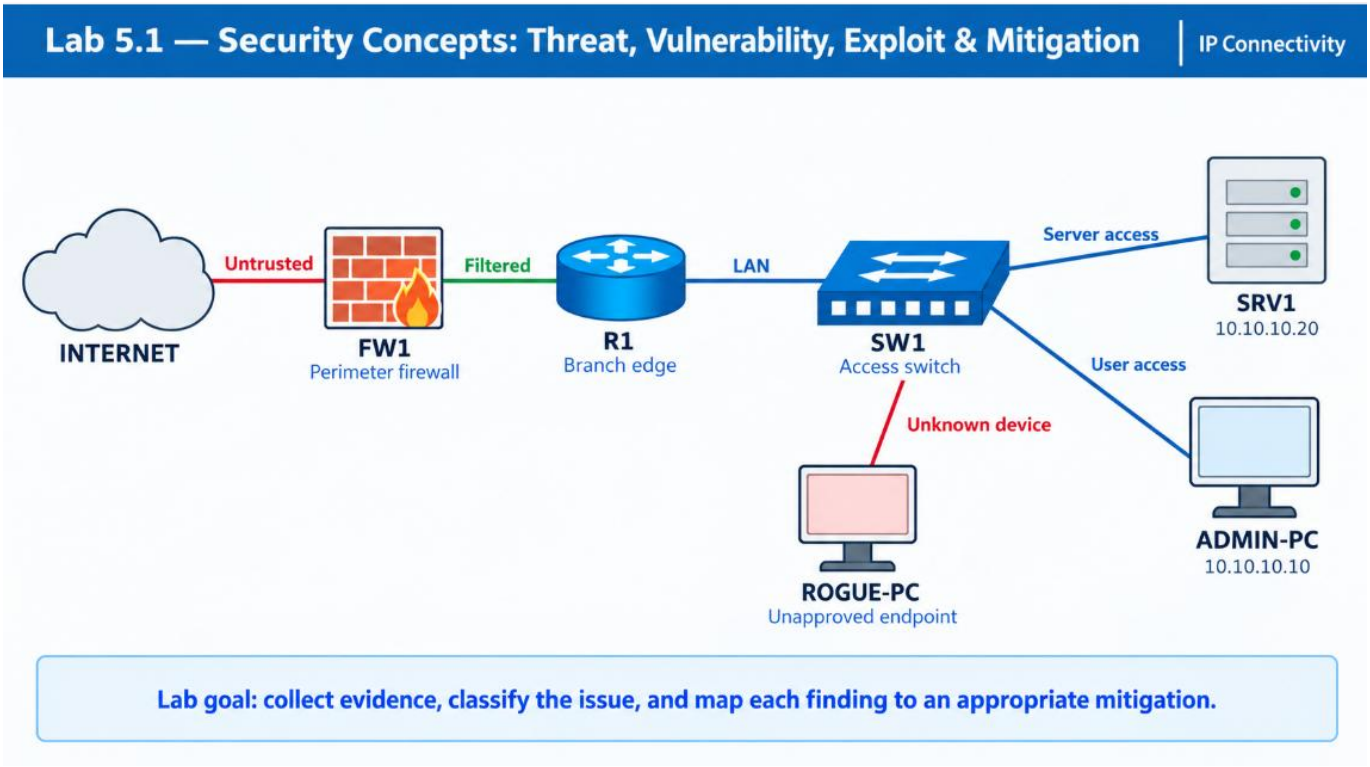
1. Build the topology exactly as shown and apply the addressing plan.
2. Configure devices in the order presented. Do not repeat an earlier configuration block.
3. Run each verification command immediately after its related configuration.
4. Compare your output with the sample output and read the “What to verify” bullets.
5. Run the end-to-end test, then perform the controlled security/failure exercise where provided.

Exam alignment: Cisco CCNA 200-301 v1.1 lists Security Fundamentals objectives 5.1 through 5.10. Concept-only objectives are implemented as guided scenario/interpretation labs; configuration objectives include full device-by-device CLI or GUI steps.

Lab 5.1 — Security Concepts: Threat, Vulnerability, Exploit and Mitigation

Perform a security assessment of an intentionally weak branch network. The goal is to distinguish a threat from a vulnerability and an exploit, then select a realistic mitigation.

Lab topology



Addressing / device plan

Device	Interface / role	Address / state
R1	LAN gateway	10.10.10.1/24
SW1	Access switch	10.10.10.2/24 management
ADMIN-PC	Approved endpoint	10.10.10.10/24
SRV1	Application server	10.10.10.20/24
ROGUE-PC	Unapproved endpoint	10.10.10.99/24

Lab objectives

- Collect evidence without changing the network.
- Classify findings as threat, vulnerability, exploit or mitigation.
- Identify weak management access, unused-access-port exposure and unauthorized endpoints.
- Create a mitigation plan that will be implemented in later Module 5 labs.

Step 1 — Inspect R1 without making changes

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.10.10.1      YES manual up                    up

R1# show running-config | section line vty
line vty 0 4
 password cisco
 login
 transport input telnet ssh

R1# show running-config | include enable password|enable secret|username|service password
enable password cisco
service password-encryption

R1# show logging | include LOGIN|SECURITY
<no security-login messages>
```

What to verify

- VTY access accepts Telnet, which exposes credentials and management traffic in clear text.
- The router uses a weak enable password rather than an enable secret.
- No named local administrator is present.
- The absence of security-login events does not prove the device is secure; it only shows that no login-control feature is generating those events.

Step 2 — Inspect SW1

```
SW1# show interfaces status
Port      Name               Status       Vlan
Gi0/1                        connected    10
Gi0/2                        connected    10
Gi0/3                        notconnect   1
Gi0/4                        notconnect   1

SW1# show mac address-table dynamic
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
10      00aa.aaaa.0010    DYNAMIC     Gi0/1
10      00bb.bbbb.0099    DYNAMIC     Gi0/2

SW1# show running-config | include port-security|bpduguard|shutdown
<no matching lines>
```

What to verify

- An unexpected MAC address is learned on an access port, representing an unauthorized endpoint threat.
- Unused ports are in VLAN 1 and are not administratively shut down.
- No port-security or BPDU Guard control is present on access interfaces.

Step 3 — Classify the findings

Observation	Classification	Why it matters	Recommended mitigation
Telnet permitted on VTY	Vulnerability	Credentials can be captured in transit	SSH only; local/AAA authentication

Weak enable password	Vulnerability	Easy credential guessing / offline recovery	Use enable secret and strong password policy
Rogue endpoint attached	Threat / possible exploit path	Unauthorized host can probe the LAN	Port security, 802.1X where available, shut unused ports
Unused access ports active	Vulnerability	Provides physical entry point	Move to unused VLAN and shutdown
ARP/DHCP protections absent	Vulnerability	Enables spoofing or rogue DHCP attacks	DHCP snooping + DAI

End-of-lab verification

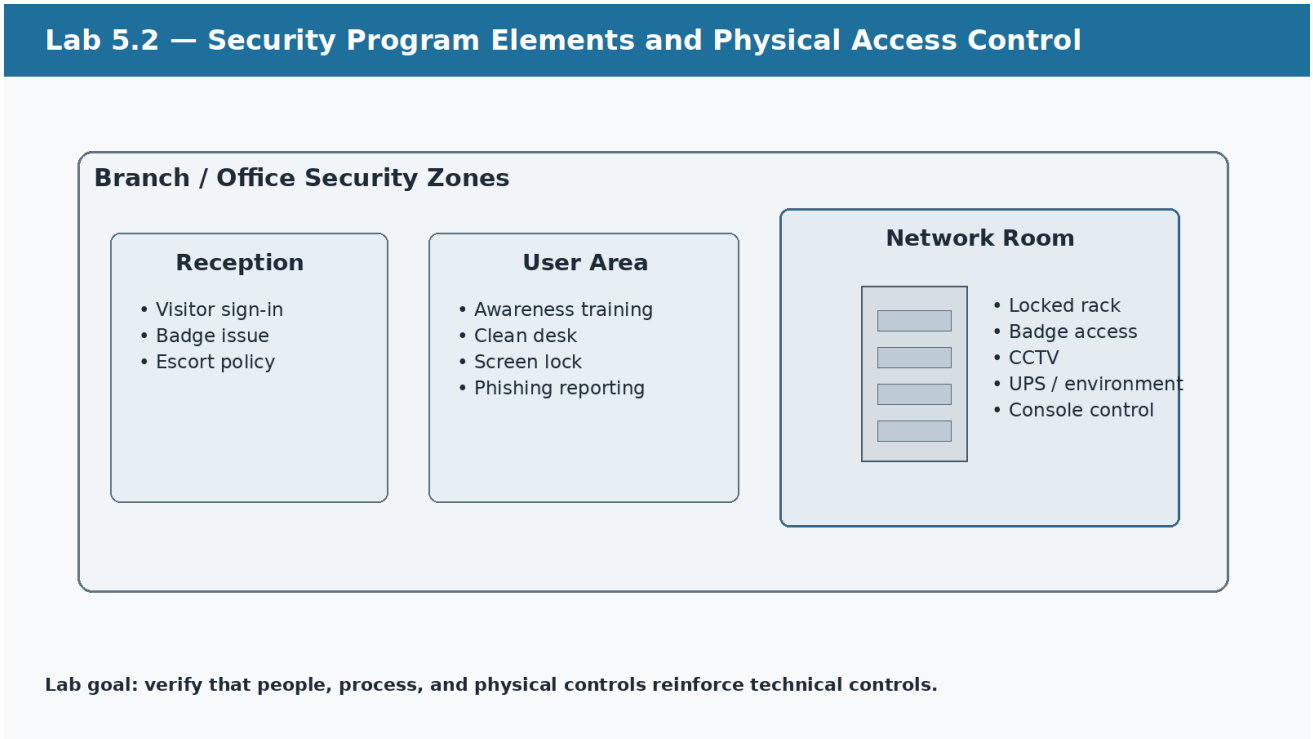
What to verify

- You can explain the difference between a threat (potential cause of harm), vulnerability (weakness), exploit (method used to abuse the weakness), and mitigation (control that reduces likelihood or impact).
- Every observed weakness has a specific mitigation that can be validated in a later lab.

Lab 5.2 Optional — Security Program Elements: Awareness, Training and Physical Access

Audit a small branch from the perspective of people, process and physical controls. This lab intentionally has no IOS configuration because the objective is to validate the security program around the network.

Lab topology / facility view



Lab objectives

- Verify user-awareness and recurring training controls.
- Verify visitor, badge and restricted-room controls.
- Verify physical safeguards for network equipment and console access.
- Document evidence rather than relying on assumed policy.

Step 1 — User awareness and training audit

Control	Evidence to collect	Pass condition
Security awareness	Training completion report	All in-scope users completed required training
Phishing awareness	Simulation/reporting record	Users know how and where to report suspicious messages
Password/MFA guidance	Published standard	Users receive current password and MFA guidance
Incident reporting	Help desk / SOC process	Users can identify the correct reporting channel

Step 2 — Physical access audit

Control	Verification action	Expected result
Visitor management	Attempt entry without sign-in	Visitor is stopped and registered

Network-room access	Review badge group membership	Only authorized operations staff have access
Rack security	Inspect rack doors and keys	Racks are locked; keys are controlled
Console access	Inspect console cables / terminal server	Access is restricted and auditable
Environmental resilience	Inspect UPS / temperature monitoring	Power and environmental controls are operational

Step 3 — Record findings

```
SECURITY PROGRAM AUDIT RESULT
User awareness training:      PASS / FAIL
Phishing reporting process:   PASS / FAIL
Visitor sign-in / escort:     PASS / FAIL
Network-room badge control:   PASS / FAIL
Rack locking:                 PASS / FAIL
Console access control:       PASS / FAIL
UPS/environment monitoring:   PASS / FAIL

Open findings:
1. _____
2. _____
3. _____
```

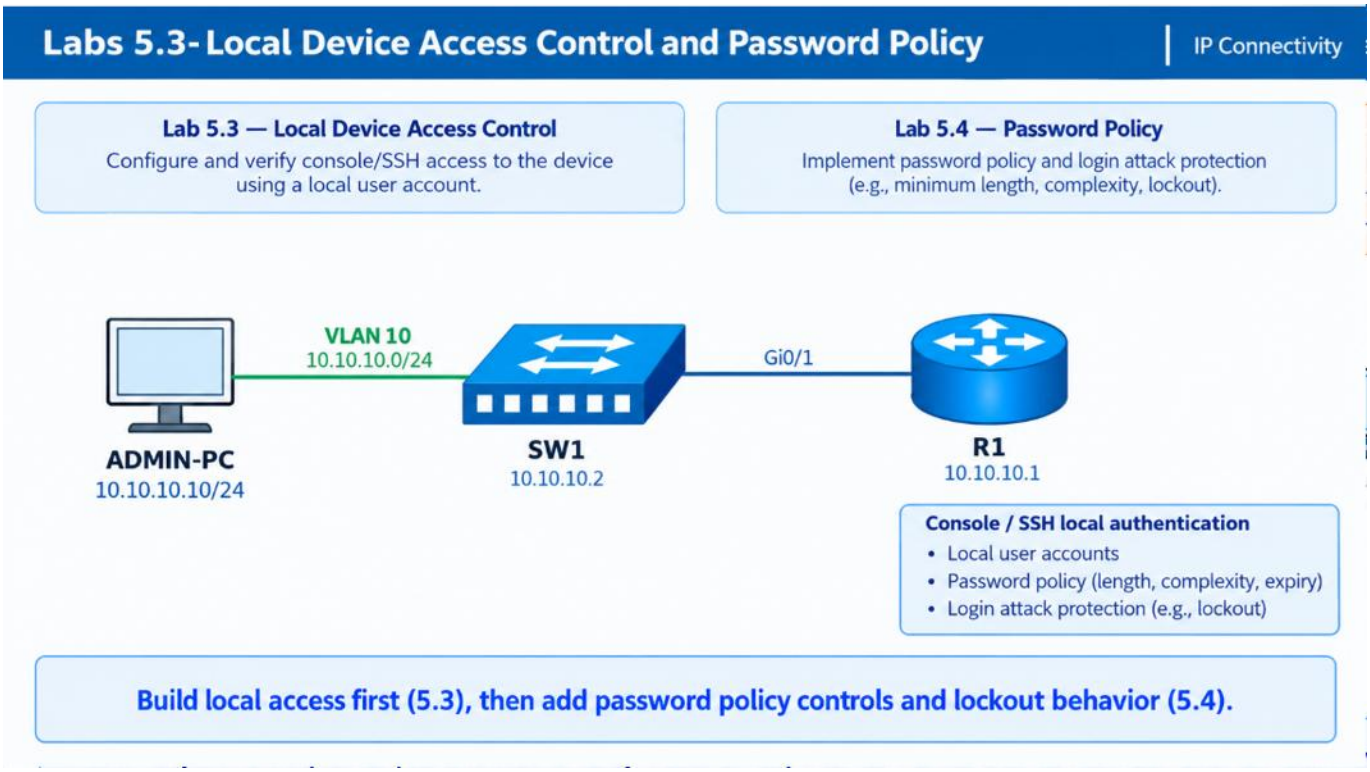
What to verify

- Each control has evidence, an owner and a pass/fail decision.
- Physical controls protect the devices that logical controls depend on.
- Security awareness and training are treated as recurring controls, not one-time events.

Lab 5.3 — Configure and Verify Local Device Access Control

Harden one router and one switch with local named accounts, enable secret, console authentication and SSH-only VTY access.

Lab topology



Addressing / device plan

Device	Interface	IPv4
R1	Gi0/0	10.10.10.1/24
SW1	SVI VLAN 10	10.10.10.2/24
ADMIN-PC	NIC	10.10.10.10/24; GW 10.10.10.1

Step 1 — Configure SW1 Layer 2 and management access

```
enable
configure terminal
hostname SW1
!
vlan 10
 name MANAGEMENT
!
interface GigabitEthernet0/1
 description TO_R1
 switchport mode access
 switchport access vlan 10
 no shutdown
!
interface GigabitEthernet0/2
 description ADMIN_PC
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 no shutdown
!
interface Vlan10
 ip address 10.10.10.2 255.255.255.0
 no shutdown
!
ip default-gateway 10.10.10.1
!
enable secret CcnaEnable!2026
username netadmin privilege 15 secret LocalAdmin!2026
service password-encryption
ip domain-name nga.lab
crypto key generate rsa modulus 2048
ip ssh version 2
!
line console 0
 login local
 exec-timeout 5 0
!
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0
end
write memory
```

SW1 verification

```
SW1# show ip interface brief | include Vlan10
Vlan10                 10.10.10.2     YES manual up                    up

SW1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3

SW1# show running-config | include enable secret|username netadmin|service password
enable secret 9 <hash>
username netadmin privilege 15 secret 9 <hash>
service password-encryption
```

What to verify

- SVI VLAN 10 is up/up and reachable from ADMIN-PC.
- SSH version 2 is enabled.
- Secrets are stored as hashes rather than visible plaintext.
- Console and VTY lines authenticate against the local username database.

Step 2 — Configure R1 local access control

```
enable
configure terminal
hostname R1
!
interface GigabitEthernet0/0
 description TO_SW1
 ip address 10.10.10.1 255.255.255.0
 no shutdown
!
enable secret CcnaEnable!2026
username netadmin privilege 15 secret LocalAdmin!2026
service password-encryption
ip domain-name nga.lab
crypto key generate rsa modulus 2048
ip ssh version 2
!
line console 0
 login local
 exec-timeout 5 0
!
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0
end
write memory
```

R1 verification

```
R1# show ip ssh
SSH Enabled - version 2.0

R1# show running-config | section line vty
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0

R1# show users
    Line       User       Host(s)              Idle       Location
*  0 con 0     netadmin   idle                 00:00:00
```

What to verify

- VTY allows SSH only; Telnet is not accepted.
- “login local” points line authentication to the local username database.
- The privileged local administrator exists on both devices.

Step 3 — Verify from ADMIN-PC

```
ADMIN-PC> ping 10.10.10.1
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255

ADMIN-PC> ssh -l netadmin 10.10.10.1
Password:
R1#

ADMIN-PC> ssh -l netadmin 10.10.10.2
Password:
SW1#
```

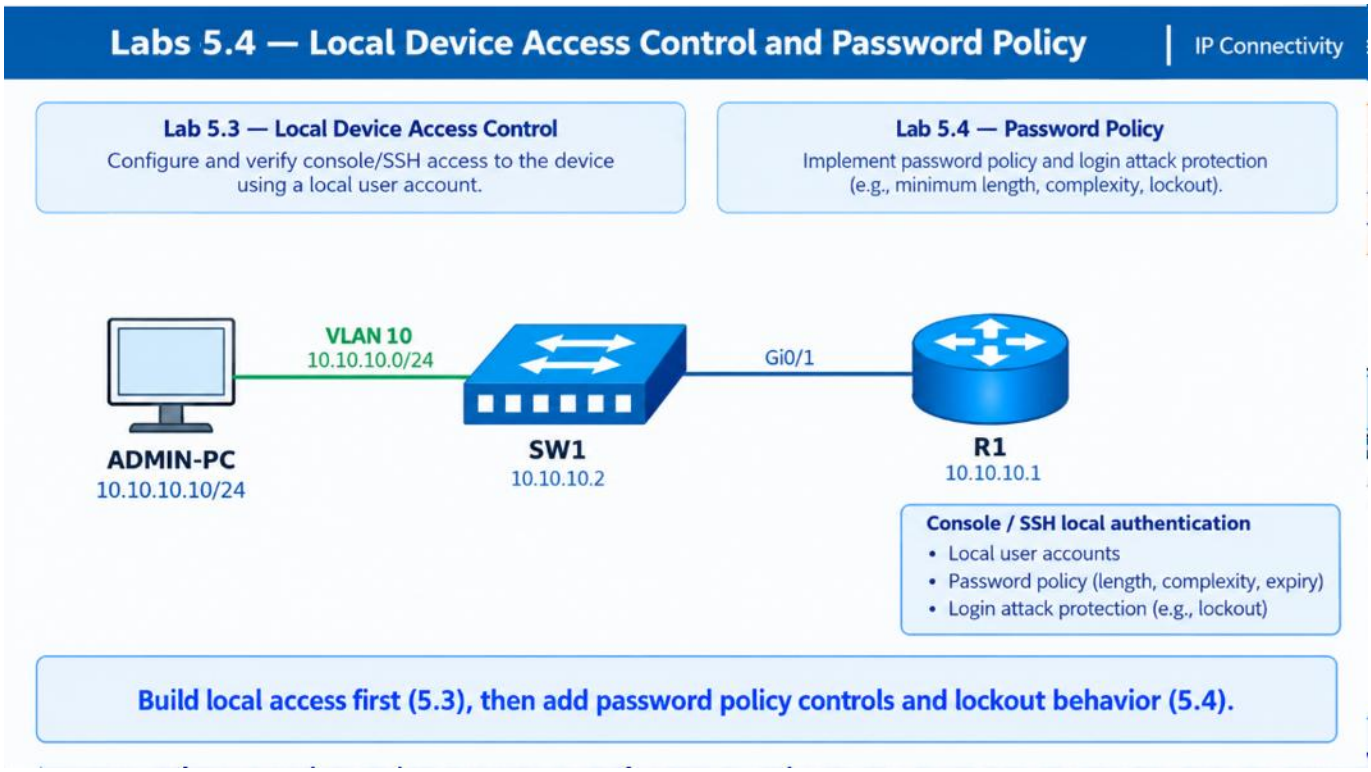
What to verify

- ADMIN-PC can reach both management addresses.
- The named “netadmin” account successfully authenticates to both devices.
- Successful login lands at the expected privilege level.

Lab 5.4 — Password Policy, Complexity and Authentication Alternatives

Build on the locally secured R1 by enforcing minimum password length and login-attack protection. Then compare passwords with MFA, certificates and biometrics.

Lab topology



Step 1 — Add password and login policy to R1

```
R1# configure terminal
R1(config)# security passwords min-length 10
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# login delay 2
R1(config)# banner motd ^C
Unauthorized access is prohibited. Activity may be monitored.
^C
R1(config)# end
R1# write memory
```

Policy verification

```
R1# show login
    A login delay of 2 seconds is applied.
    Router enabled to watch for login attacks.
    If more than 3 login failures occur in 60 seconds or less,
    logins will be disabled for 120 seconds.

R1# show running-config | include security passwords|login block-for|login delay
security passwords min-length 10
login block-for 120 attempts 3 within 60
login delay 2
```

What to verify

- The minimum password-length policy is present.
- The router monitors failed attempts within a time window.
- Excessive failures trigger a temporary quiet/blocked state.
- A login delay slows repeated guessing attempts.

Step 2 — Controlled failed-login test

```
ADMIN-PC> ssh -l wronguser 10.10.10.1
Password: wrong
% Authentication failed

(repeat until three failures occur within 60 seconds)

R1# show login
    Router presently in Quiet-Mode.
    Quiet-Mode remaining time: 0:01:47

R1# show logging | include LOGIN_FAILED|QUIET_MODE
%SEC_LOGIN-4-LOGIN_FAILED: Login failed ...
%SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 0 secs...
```

What to verify

- Repeated failures are logged.
- The router enters the configured temporary blocked state after the threshold is reached.
- Legitimate access recovers after the quiet-mode timer expires.

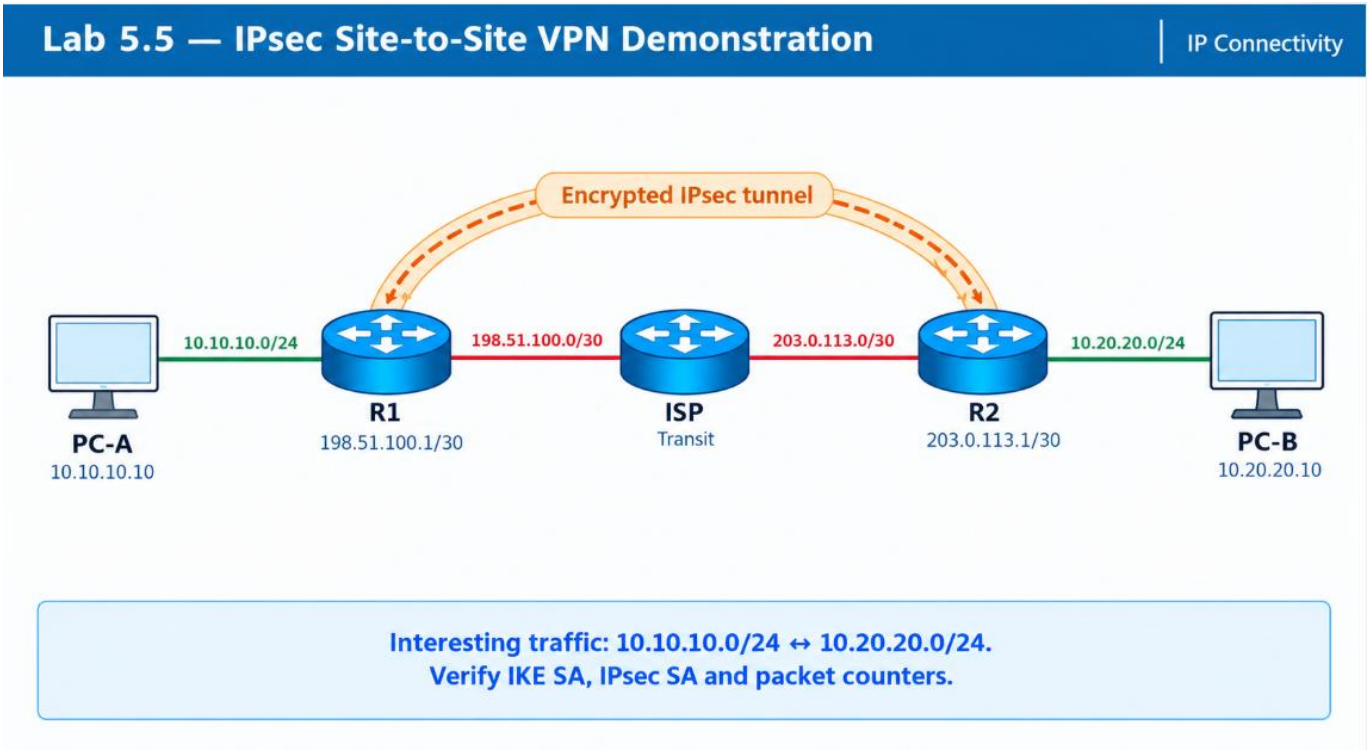
Password alternatives — what to verify conceptually

Control	What it proves	Security value
Multi-factor authentication	User presents two or more independent factors	Reduces impact of a stolen password
Digital certificate	Client/server proves possession of a private key bound to a trusted certificate	Strong machine/user identity and scalable trust
Biometric	User provides an inherence factor	Adds identity assurance but requires privacy and fallback controls

Lab 5.5 — IPsec Remote Access and Site-to-Site VPNs

Configure a demonstration site-to-site IPsec VPN between two branch routers and use it to understand the building blocks also used by secure remote-access VPNs.

Lab topology



Addressing / device plan

Device	Interface	IPv4
R1	Gi0/0 LAN	10.10.10.1/24
R1	Gi0/1 WAN	198.51.100.1/30
ISP	Gi0/0 / Gi0/1	198.51.100.2/30 / 203.0.113.2/30
R2	Gi0/1 WAN	203.0.113.1/30
R2	Gi0/0 LAN	10.20.20.1/24
PC-A	NIC	10.10.10.10/24; GW 10.10.10.1
PC-B	NIC	10.20.20.10/24; GW 10.20.20.1

Platform note: classic IOS/Packet Tracer IPsec syntax can vary. The sequence below uses a traditional IKEv1 crypto-map workflow because it makes each VPN phase visible for training.

Step 1 — Configure ISP transit router

```
enable
configure terminal
hostname ISP
interface GigabitEthernet0/0
 description TO_R1
 ip address 198.51.100.2 255.255.255.252
 no shutdown
interface GigabitEthernet0/1
 description TO_R2
 ip address 203.0.113.2 255.255.255.252
 no shutdown
end
```

ISP verification

```
ISP# show ip interface brief
GigabitEthernet0/0  198.51.100.2  YES manual up  up
GigabitEthernet0/1  203.0.113.2   YES manual up  up
```

What to verify

- Both public transit interfaces are up/up.

Step 2 — Configure R1 and IPsec policy

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 description LAN_A
 ip address 10.10.10.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/1
 description TO_ISP
 ip address 198.51.100.1 255.255.255.252
 no shutdown
ip route 0.0.0.0 0.0.0.0 198.51.100.2
!
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 14
crypto isakmp key CCNA-VPN-2026 address 203.0.113.1
!
ip access-list extended VPN-TRAFFIC
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
!
crypto ipsec transform-set CCNA-SET esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CCNA-MAP 10 ipsec-isakmp
 set peer 203.0.113.1
 set transform-set CCNA-SET
 match address VPN-TRAFFIC
!
interface GigabitEthernet0/1
 crypto map CCNA-MAP
end
```

Step 3 — Configure R2 and mirrored IPsec policy

```
enable
configure terminal
hostname R2
interface GigabitEthernet0/0
 description LAN_B
 ip address 10.20.20.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/1
 description TO_ISP
 ip address 203.0.113.1 255.255.255.252
 no shutdown
ip route 0.0.0.0 0.0.0.0 203.0.113.2
!
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 14
crypto isakmp key CCNA-VPN-2026 address 198.51.100.1
!
ip access-list extended VPN-TRAFFIC
 permit ip 10.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255
!
crypto ipsec transform-set CCNA-SET esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CCNA-MAP 10 ipsec-isakmp
 set peer 198.51.100.1
 set transform-set CCNA-SET
 match address VPN-TRAFFIC
!
interface GigabitEthernet0/1
 crypto map CCNA-MAP
end
```

Step 4 — Verify before interesting traffic

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
<no active SA>

R1# show crypto ipsec sa | include pkts encaps|pkts decaps
#pkts encaps: 0, #pkts encrypt: 0
#pkts decaps: 0, #pkts decrypt: 0
```

What to verify

- No tunnel is built until traffic matches the crypto ACL.
- Packet counters are zero before interesting traffic.

Step 5 — Generate interesting traffic and verify

```
PC-A> ping 10.20.20.10
Reply from 10.20.20.10: bytes=32 time=10ms TTL=126

R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
203.0.113.1     198.51.100.1    QM_IDLE        1001    ACTIVE

R1# show crypto ipsec sa | include local ident|remote ident|pkts encaps|pkts decaps
local  ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
#pkts encaps: 5, #pkts encrypt: 5
#pkts decaps: 4, #pkts decrypt: 4
```

What to verify

- IKE reaches an established state (`QM_IDLE` in this IKEv1 example).
- Local and remote protected subnets match the VPN ACL.
- Encapsulation/encryption and decapsulation/decryption counters increase.
- PC-A reaches PC-B through the encrypted tunnel.

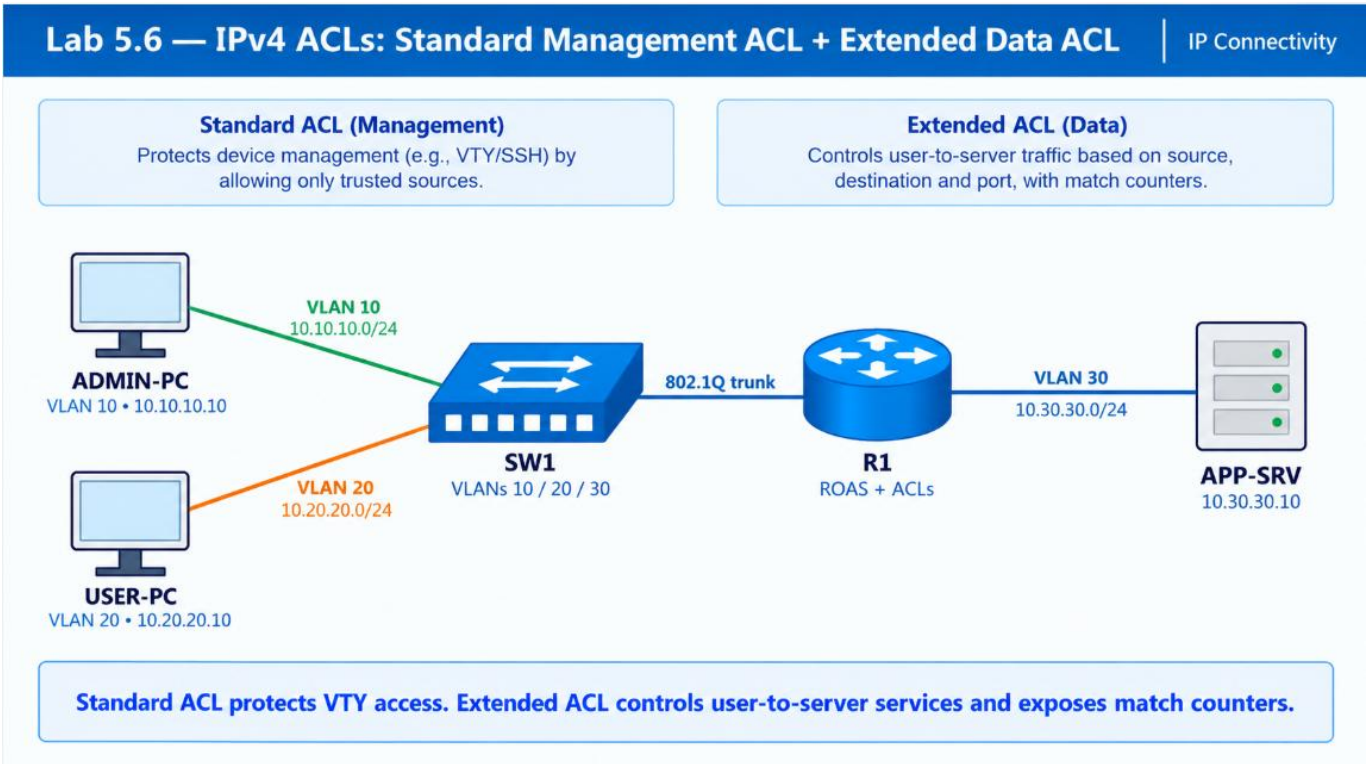
Remote-access vs site-to-site interpretation

Characteristic	Remote-access VPN	Site-to-site VPN
Typical endpoint	User device / VPN client	VPN gateway/router/firewall
Purpose	Secure individual user access	Secure network-to-network connectivity
Authentication	User/device identity, often MFA/certificates	Gateway identity, PSK or certificates
Traffic scope	Selected user/device traffic	Defined protected subnets

Lab 5.6 — Configure and Verify IPv4 Access Control Lists

Use one router-on-a-stick topology to build a standard management ACL and an extended data-plane ACL without reconfiguring the base interfaces twice.

Lab topology



Addressing / device plan

Segment	Subnet	Endpoint
VLAN 10 ADMIN	10.10.10.0/24	ADMIN-PC 10.10.10.10
VLAN 20 USERS	10.20.20.0/24	USER-PC 10.20.20.10
VLAN 30 SERVER	10.30.30.0/24	APP-SRV 10.30.30.10

Step 1 — Configure SW1 VLANs and trunk

```
enable
configure terminal
hostname SW1
vlan 10
 name ADMIN
vlan 20
 name USERS
vlan 30
 name SERVER
!
interface GigabitEthernet0/1
 description TO_R1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30
 no shutdown
!
interface GigabitEthernet0/2
 description ADMIN_PC
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
!
interface GigabitEthernet0/3
 description USER_PC
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
!
interface GigabitEthernet0/4
 description APP_SERVER
 switchport mode access
 switchport access vlan 30
 spanning-tree portfast
end
```

SW1 verification

```
SW1# show interfaces trunk
Port      Mode  Encapsulation  Status    Native vlan
Gi0/1     on    802.1q         trunking  1

Port      Vlans allowed on trunk
Gi0/1     10,20,30
```

What to verify

- Gi0/1 trunks VLANs 10, 20 and 30 to R1.

Step 2 — Configure R1 base routing and secure VTY

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 no shutdown
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.20.20.1 255.255.255.0
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.30.30.1 255.255.255.0
!
username netadmin privilege 15 secret LocalAdmin!2026
ip domain-name nga.lab
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
end
```

Step 3 — Apply standard ACL to management access

```
R1# configure terminal
R1(config)# ip access-list standard MGMT_ONLY
R1(config-std-nacl)# permit 10.10.10.0 0.0.0.255
R1(config-std-nacl)# deny any log
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# access-class MGMT_ONLY in
R1(config-line)# end
```

Standard ACL verification

```
R1# show access-lists MGMT_ONLY
Standard IP access list MGMT_ONLY
    10 permit 10.10.10.0, wildcard bits 0.0.0.255
    20 deny any log

ADMIN-PC> ssh -l netadmin 10.10.10.1
R1#

USER-PC> ssh -l netadmin 10.20.20.1
% Connection refused / access denied
```

What to verify

- Only the ADMIN subnet can open an inbound VTY session.
- The ACL is applied with `access-class`, not to a routed data interface.
- Denied attempts increment the deny entry counter after testing.

Step 4 — Add extended ACL for user-to-server traffic

```
R1# configure terminal
R1(config)# ip access-list extended USER_TO_SERVER
R1(config-ext-nacl)# deny tcp 10.20.20.0 0.0.0.255 host 10.30.30.10 eq 22 log
R1(config-ext-nacl)# permit tcp 10.20.20.0 0.0.0.255 host 10.30.30.10 eq 80
R1(config-ext-nacl)# permit tcp 10.20.20.0 0.0.0.255 host 10.30.30.10 eq 443
R1(config-ext-nacl)# permit icmp 10.20.20.0 0.0.0.255 host 10.30.30.10 echo
R1(config-ext-nacl)# deny ip 10.20.20.0 0.0.0.255 10.30.30.0 0.0.0.255 log
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
R1(config)# interface GigabitEthernet0/0.20
R1(config-subif)# ip access-group USER_TO_SERVER in
R1(config-subif)# end
```

Extended ACL verification

```
USER-PC> ping 10.30.30.10
Reply from 10.30.30.10: bytes=32 time<1ms TTL=127

USER-PC> ssh -l serveradmin 10.30.30.10
Connection timed out / denied

R1# show access-lists USER_TO_SERVER
Extended IP access list USER_TO_SERVER
    10 deny tcp 10.20.20.0 0.0.0.255 host 10.30.30.10 eq 22 (4 matches)
    20 permit tcp 10.20.20.0 0.0.0.255 host 10.30.30.10 eq www (6 matches)
    30 permit tcp 10.20.20.0 0.0.0.255 host 10.30.30.10 eq 443
    40 permit icmp 10.20.20.0 0.0.0.255 host 10.30.30.10 echo (5 matches)
    50 deny ip 10.20.20.0 0.0.0.255 10.30.30.0 0.0.0.255
    60 permit ip any any
```

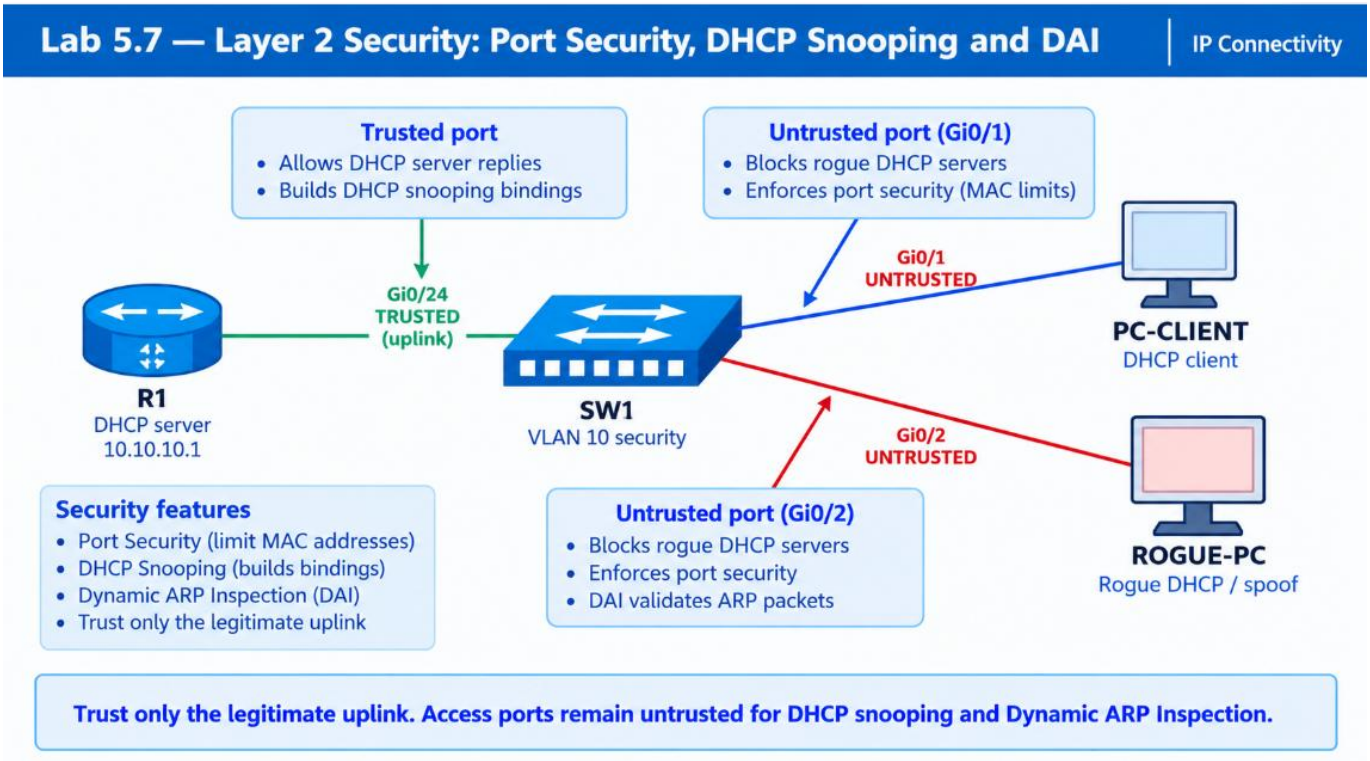
What to verify

- SSH from USERS to APP-SRV is denied while allowed services continue to work.
- ACL match counters prove which ACE handled the test traffic.
- The extended ACL is placed close to the source, inbound on the USERS subinterface.
- The final permit prevents unrelated traffic from being unintentionally blocked by the implicit deny.

Lab 5.7 — Layer 2 Security: Port Security, DHCP Snooping and Dynamic ARP Inspection

Secure VLAN 10 at the access layer. The legitimate router uplink is trusted; endpoint ports remain untrusted and enforce DHCP, ARP and source-MAC controls.

Lab topology



Addressing / device plan

Device	Role	Addressing
R1	DHCP server / gateway	10.10.10.1/24
SW1 Gi0/24	Trusted uplink	Access VLAN 10
PC-CLIENT	Legitimate endpoint	DHCP
ROGUE-PC	Attack simulation	DHCP / spoof source

Step 1 — Configure R1 DHCP service

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
 no shutdown
!
ip dhcp excluded-address 10.10.10.1 10.10.10.20
ip dhcp pool USERS
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 dns-server 8.8.8.8
end
```

Step 2 — Configure SW1 Layer 2 security

```
enable
configure terminal
hostname SW1
vlan 10
 name USERS
!
ip dhcp snooping
ip dhcp snooping vlan 10
no ip dhcp snooping information option
ip arp inspection vlan 10
!
interface GigabitEthernet0/24
 description TRUSTED_UPLINK_TO_R1
 switchport mode access
 switchport access vlan 10
 ip dhcp snooping trust
 ip arp inspection trust
 no shutdown
!
interface GigabitEthernet0/1
 description PC_CLIENT
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 ip dhcp snooping limit rate 15
 no shutdown
!
interface GigabitEthernet0/2
 description ROGUE_PC
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 ip dhcp snooping limit rate 15
 no shutdown
end
```

Step 3 — Obtain a legitimate DHCP lease and verify bindings

```
PC-CLIENT> ipconfig /renew
IPv4 Address.............: 10.10.10.21
Default Gateway.........: 10.10.10.1

SW1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Interface                  Trusted    Rate limit (pps)
Gi0/24                     yes        unlimited
Gi0/1                      no         15
Gi0/2                      no         15

SW1# show ip dhcp snooping binding
MacAddress          IpAddress      Lease(sec) Type          VLAN Interface
00:11:22:33:44:55   10.10.10.21   86320      dhcp-snooping 10   Gi0/1
```

What to verify

- Only Gi0/24 is trusted for DHCP server messages.
- PC-CLIENT receives a lease through the legitimate DHCP server.
- The snooping binding ties client MAC, IP, VLAN and interface together.

Step 4 — Verify DAI and port security

```
SW1# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
 Vlan     Configuration    Operation   ACL Match  Static ACL
 ----     -------------    ---------   ---------  ----------
 10       Enabled          Active

SW1# show port-security interface GigabitEthernet0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Sticky MAC Addresses       : 1
Security Violation Count   : 0
```

What to verify

- DAI is active on VLAN 10.
- Port security is enabled and the legitimate MAC is learned as sticky.
- Violation counter is zero before the controlled attack.

Controlled test A — Rogue DHCP server offer

```
ROGUE-PC / rogue DHCP process sends DHCPOFFER on Gi0/2

SW1# show ip dhcp snooping statistics
Packets dropped on untrusted ports: 4

SW1# show logging | include DHCP_SNOOPING
%DHCP_SNOOPING-5-DHCP_SNOOPING_DROP: DHCP message dropped on untrusted port Gi0/2
```

What to verify

- Server-originated DHCP messages arriving on an untrusted access port are dropped.
- Legitimate clients continue to use the trusted uplink.

Controlled test B — MAC-address violation

```
Connect a second source MAC through Gi0/1.

SW1# show port-security interface GigabitEthernet0/1
Port Status                : Secure-up
Violation Mode             : Restrict
Maximum MAC Addresses      : 1
Security Violation Count   : 1
```

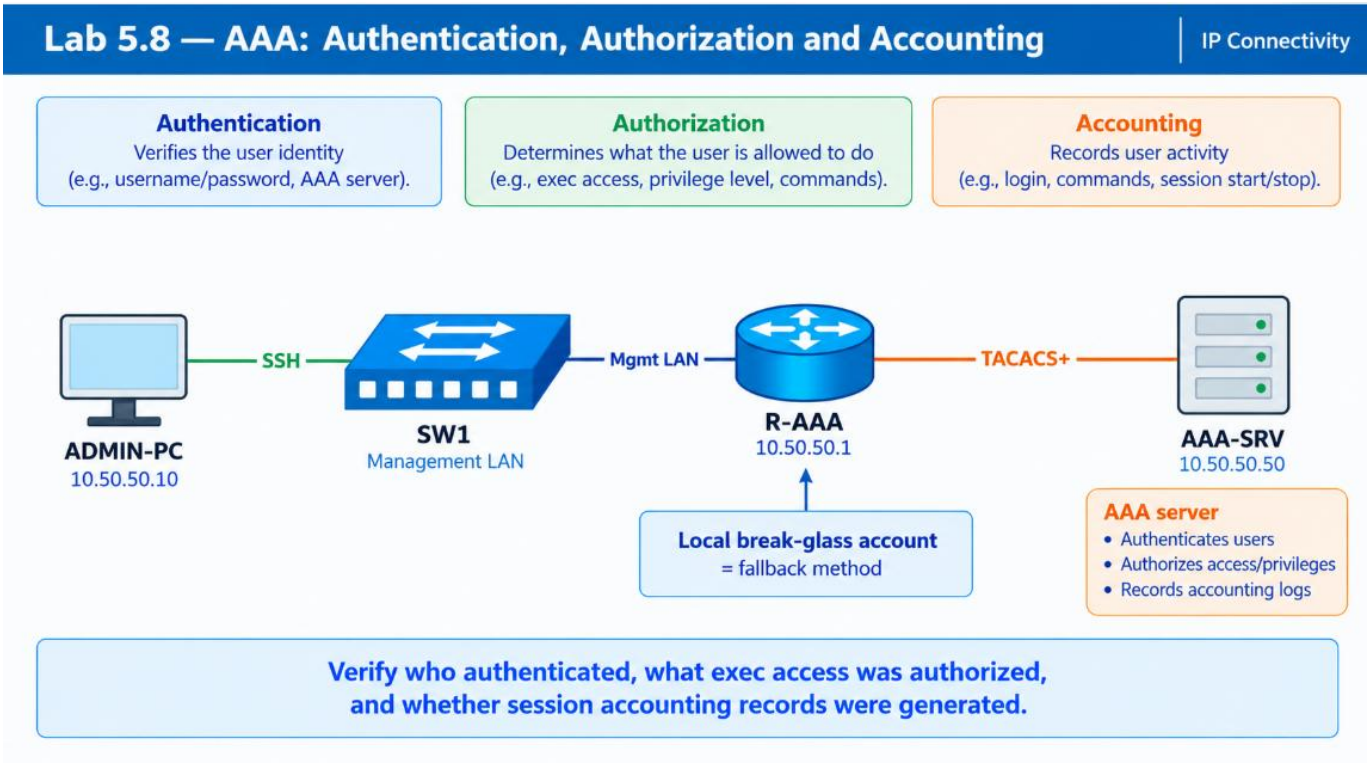
What to verify

- The port remains up in restrict mode, but violating frames are dropped.
- The security violation counter increases.

Lab 5.8 — AAA: Authentication, Authorization and Accounting

Configure TACACS+ as the primary management authentication method with a local break-glass account as fallback. Use the lab to separate the three AAA functions.

Lab topology



Addressing / device plan

Device	Role	IPv4
R-AAA	Managed router	10.50.50.1/24
AAA-SRV	TACACS+ server	10.50.50.50/24
ADMIN-PC	SSH client	10.50.50.10/24

Step 1 — Configure AAA server values

```
AAA SERVER / GUI VALUES
Service:              TACACS+
Server IP:            10.50.50.50/24
Default gateway:      10.50.50.1
Network client:       R-AAA / 10.50.50.1
Shared secret:        TacacsKey!2026
User:                 netops
User password:        N3tOps!2026
User privilege:       Administrative / privilege 15
Accounting/logging:   Enabled
```

What to verify

- The server recognizes R-AAA as an authorized AAA client.

- The shared secret exactly matches the router configuration.
- The `netops` user exists and accounting/logging is enabled.

Step 2 — Configure R-AAA

```
enable
configure terminal
hostname R-AAA
interface GigabitEthernet0/0
 ip address 10.50.50.1 255.255.255.0
 no shutdown
!
username breakglass privilege 15 secret LocalFallback!2026
ip domain-name nga.lab
crypto key generate rsa modulus 2048
ip ssh version 2
!
aaa new-model
tacacs server TAC1
 address ipv4 10.50.50.50
 key TacacsKey!2026
!
aaa group server tacacs+ TAC-GRP
 server name TAC1
!
aaa authentication login default group TAC-GRP local
aaa authorization exec default group TAC-GRP local if-authenticated
aaa accounting exec default start-stop group TAC-GRP
!
ip tacacs source-interface GigabitEthernet0/0
!
line vty 0 4
 login authentication default
 authorization exec default
 transport input ssh
end
```

Router verification

```
R-AAA# show running-config | section aaa
aaa new-model
aaa group server tacacs+ TAC-GRP
 server name TAC1
aaa authentication login default group TAC-GRP local
aaa authorization exec default group TAC-GRP local if-authenticated
aaa accounting exec default start-stop group TAC-GRP

R-AAA# show running-config | section tacacs
tacacs server TAC1
 address ipv4 10.50.50.50
 key 7 <encrypted-value>
```

What to verify

- AAA new-model is enabled.
- Authentication tries TACACS+ first and local credentials second.
- Exec authorization uses the same remote-first/local-fallback policy.
- Accounting is configured to send start/stop exec records to the TACACS+ group.

Step 3 — Test TACACS+ login

```
ADMIN-PC> ssh -l netops 10.50.50.1
Password: N3tOps!2026
R-AAA#

AAA-SRV LOG:
Authentication: PASS user=netops client=10.50.50.1
Authorization:  PASS service=exec user=netops
Accounting:     START user=netops service=exec
```

What to verify

- Authentication answers the question: who are you?
- Authorization answers the question: what are you allowed to do?
- Accounting records the management session.

Controlled test — AAA server unavailable

```
Temporarily disconnect AAA-SRV or disable its TACACS+ service.

ADMIN-PC> ssh -l breakglass 10.50.50.1
Password: LocalFallback!2026
R-AAA#

R-AAA# show logging | include TACACS|AAA
%AAA-3-ACCT_LOW_MEM_UID_FAIL / TACACS server timeout messages may appear depending on platform.
```

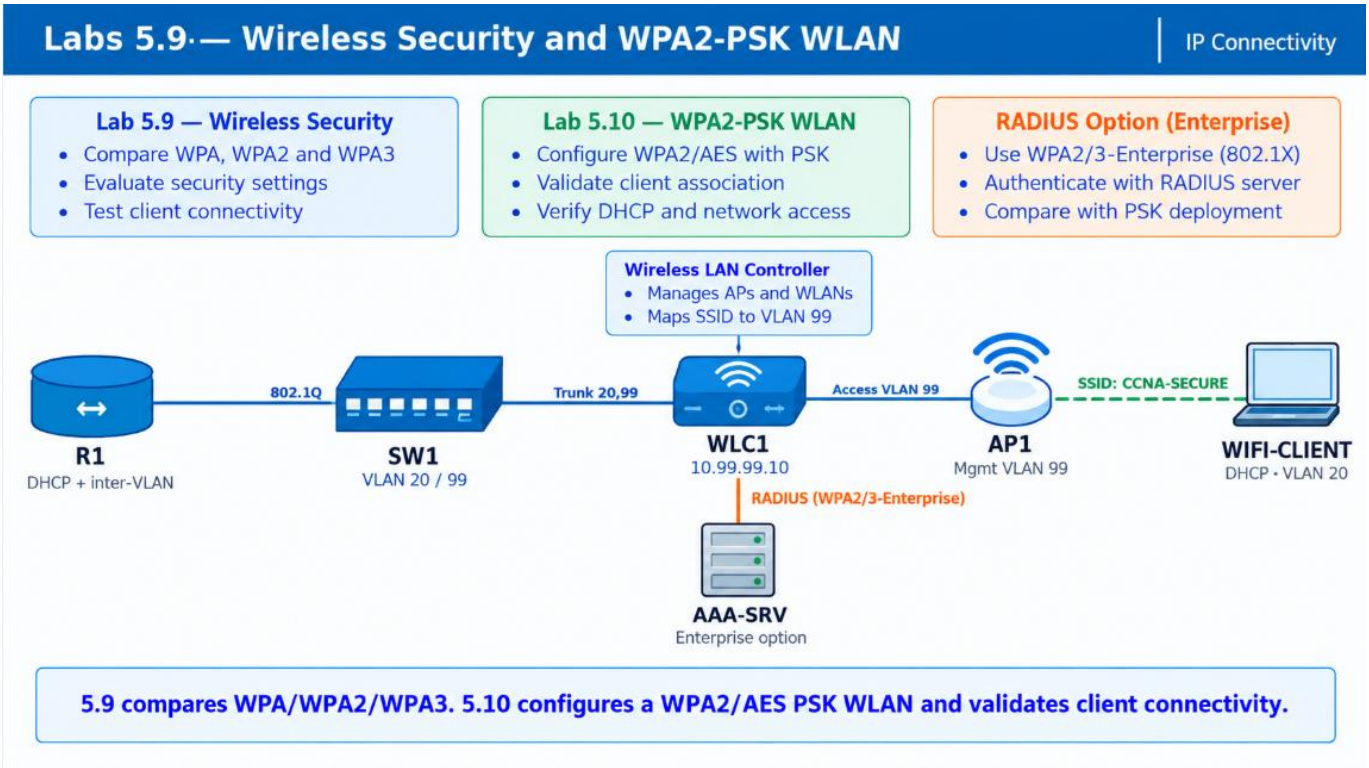
What to verify

- When TACACS+ is unreachable, the method list falls back to the local database.
- The local account is a break-glass mechanism; it should be tightly controlled in production.

Lab 5.9 — Wireless Security Protocols: WPA, WPA2 and WPA3

Interpret wireless security profiles and select the strongest protocol that meets the client and infrastructure requirements. This is a configuration-analysis lab rather than an IOS CLI lab.

Lab topology



Security protocol comparison

Protocol	Encryption / integrity	Typical authentication	Training conclusion
WPA	TKIP (legacy)	PSK or 802.1X	Legacy; avoid for new deployments
WPA2	AES-CCMP	PSK or 802.1X	Common secure baseline when configured correctly
WPA3	AES-based modern suites / PMF	SAE or Enterprise	Preferred where client/infrastructure support exists

Scenario 1 — Corporate WLAN

REQUIREMENTS
- Managed corporate laptops
- Central identity service available
- Per-user identity and revocation required
- Modern client support

SELECT:
WPA3-Enterprise (or WPA2-Enterprise where compatibility requires it)
Authentication: 802.1X / RADIUS
Avoid: Shared PSK for large managed enterprise user populations

What to verify

- The selected security method provides per-user/device identity rather than one shared secret.
- RADIUS/AAA can centrally allow, deny and revoke access.
- Client support is validated before enforcing the newest protocol.

Scenario 2 — Small training WLAN

```
REQUIREMENTS
- Small number of lab clients
- No RADIUS server
- WPA3 support is inconsistent
- Simple shared access is acceptable

SELECT:
WPA2-Personal
Cipher: AES/CCMP
Authentication: Pre-shared key (PSK)
Do not select TKIP when AES is available.
```

What to verify

- WPA2/AES is appropriate for this constrained training scenario.
- The PSK must be long, unique and protected.
- WPA/TKIP is not selected merely for convenience.

Scenario 3 — Migration design

```
MIGRATION CHECK
1. Inventory client WPA3 support.
2. Enable a transition/migration plan only when required.
3. Validate protected management frame requirements.
4. Remove legacy WPA/TKIP after unsupported clients are remediated.
5. Verify all WLANs use the intended security profile.
```

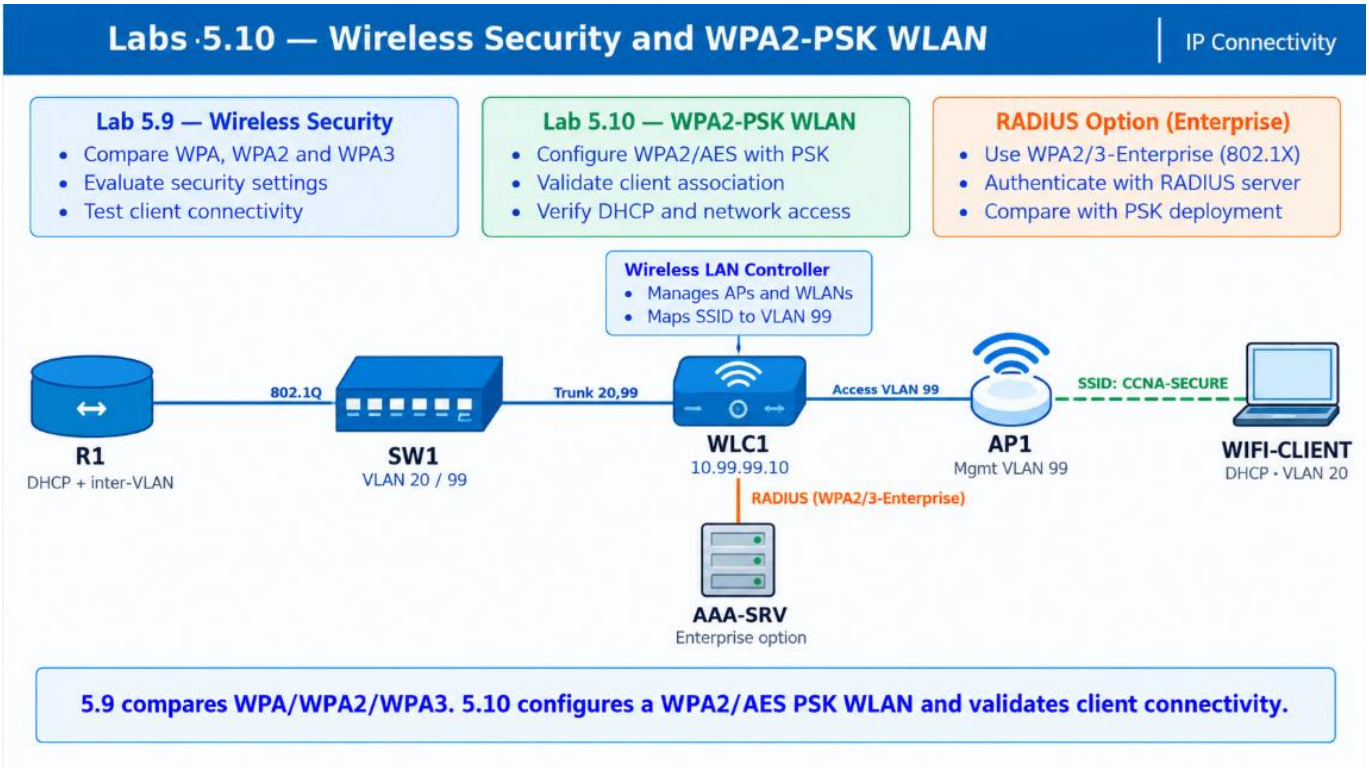
What to verify

- Wireless security is treated as a client-capability and policy decision, not just a checkbox.
- Legacy compatibility has an explicit removal plan.

Lab 5.10 — Configure and Verify a WLAN Using WPA2 PSK

Configure a secure training WLAN with WPA2/AES PSK. The wired infrastructure is configured by CLI; WLAN security is configured in the WLC GUI and verified from the wireless client.

Lab topology



Addressing / VLAN plan

Component	VLAN / interface	Addressing
R1	Gi0/0.20 WLAN users	10.20.20.1/24
R1	Gi0/0.99 management	10.99.99.1/24
WLC1 management	VLAN 99	10.99.99.10/24; GW 10.99.99.1
WLC1 dynamic interface	VLAN 20 WLAN20	10.20.20.2/24; GW 10.20.20.1
AP1	Management VLAN 99	DHCP or 10.99.99.20/24
WIFI-CLIENT	SSID CCNA-SECURE	DHCP from VLAN 20

Step 1 — Configure R1 routing and DHCP

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.20.20.1 255.255.255.0
!
interface GigabitEthernet0/0.99
 encapsulation dot1Q 99 native
 ip address 10.99.99.1 255.255.255.0
!
ip dhcp excluded-address 10.20.20.1 10.20.20.20
ip dhcp excluded-address 10.99.99.1 10.99.99.20
!
ip dhcp pool WLAN-USERS
 network 10.20.20.0 255.255.255.0
 default-router 10.20.20.1
 dns-server 8.8.8.8
!
ip dhcp pool AP-MGMT
 network 10.99.99.0 255.255.255.0
 default-router 10.99.99.1
 dns-server 8.8.8.8
end
```

R1 verification

```
R1# show ip interface brief | include GigabitEthernet0/0
GigabitEthernet0/0       unassigned      YES unset  up  up
GigabitEthernet0/0.20    10.20.20.1      YES manual up  up
GigabitEthernet0/0.99    10.99.99.1      YES manual up  up

R1# show ip dhcp pool
Pool WLAN-USERS : 10.20.20.0/24
Pool AP-MGMT    : 10.99.99.0/24
```

What to verify

- Both VLAN gateway subinterfaces are up/up.
- DHCP scopes exist for WLAN users and AP management.

Step 2 — Configure SW1

```
enable
configure terminal
hostname SW1
vlan 20
 name WLAN_USERS
vlan 99
 name WLAN_MGMT
!
interface GigabitEthernet0/1
 description TO_R1
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 20,99
 no shutdown
!
interface GigabitEthernet0/2
 description TO_WLC1
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 20,99
 no shutdown
!
interface GigabitEthernet0/3
 description TO_AP1
 switchport mode access
 switchport access vlan 99
 spanning-tree portfast
 no shutdown
end
```

SW1 verification

```
SW1# show interfaces trunk
Port      Mode  Encapsulation  Status    Native vlan
Gi0/1     on    802.1q         trunking  99
Gi0/2     on    802.1q         trunking  99

Port      Vlans allowed on trunk
Gi0/1     20,99
Gi0/2     20,99

SW1# show vlan brief | include 20|99
20   WLAN_USERS  active
99   WLAN_MGMT   active    Gi0/3
```

What to verify

- R1 and WLC links carry VLANs 20 and 99.
- AP1 is placed in management VLAN 99.

Step 3 — Configure WLC management and WLAN interface

```
WLC GUI — MANAGEMENT / INTERFACE VALUES
Management IP:       10.99.99.10
Mask:                255.255.255.0
Default gateway:     10.99.99.1
Management VLAN:     99

Dynamic interface:
Name:                WLAN20
VLAN ID:             20
Interface IP:        10.20.20.2
Mask:                255.255.255.0
Gateway:             10.20.20.1
DHCP server:         10.20.20.1
```

What to verify

- WLC management is reachable through VLAN 99.
- The WLAN20 dynamic interface maps wireless user traffic into VLAN 20.
- The DHCP server points to the VLAN 20 gateway/router.

Step 4 — Create WLAN and WPA2-PSK security in the GUI

```
WLC GUI — WLAN PROFILE
WLAN ID:             20
Profile name:        CCNA-SECURE
SSID:                CCNA-SECURE
Interface/VLAN:      WLAN20 / VLAN 20
Status:              Enabled

Security:
Layer 2 security:    WPA2 Personal / PSK
Cipher:              AES / CCMP
PSK:                 CCNA-WPA2-2026!
TKIP:                Disabled
WLAN enabled:        Yes
```

What to verify

- SSID is exactly `CCNA-SECURE`.
- WLAN maps to the VLAN 20 dynamic interface.
- WPA2 uses AES/CCMP and the configured PSK.
- Legacy TKIP is not enabled.

Step 5 — Verify AP join and wireless client connectivity

```
WLC GUI — AP / CLIENT CHECKS
AP1 state:           Joined / Registered
AP1 management IP:  10.99.99.x
WLAN:                CCNA-SECURE enabled
Associated clients:  1 or more

WIFI-CLIENT> ipconfig
IPv4 Address.............: 10.20.20.21
Default Gateway.........: 10.20.20.1

WIFI-CLIENT> ping 10.20.20.1
Reply from 10.20.20.1: bytes=32 time<1ms TTL=255

R1# show ip dhcp binding
IP address      Client-ID / Hardware address     Type
10.20.20.21     00aa.bbcc.ddee                   Automatic
```

What to verify

- AP1 is joined to WLC1 on the management network.
- The client associates to `CCNA-SECURE` using the correct PSK.
- The client receives an address from VLAN 20, not VLAN 99.
- The client reaches its default gateway.
- R1 has a corresponding DHCP binding.

Controlled test — incorrect PSK

```
On WIFI-CLIENT:
Forget / delete the saved CCNA-SECURE profile.
Reconnect using an incorrect PSK.

Expected:
Association/authentication fails.
No valid VLAN 20 DHCP lease is obtained.

Reconnect using:
CCNA-WPA2-2026!

Expected:
Association succeeds and the client receives a 10.20.20.x address.
```

What to verify

- Incorrect credentials fail before normal user data connectivity is available.
- Correct credentials restore association, DHCP and gateway reachability.

Module 5 — Final Verification Checklist

Area	Verification command / evidence	Pass condition
Local device access	show ip ssh; show run | section line vty	SSH-only local authentication works
Password policy	show login	Length/lockout/delay policy visible and testable
IPsec VPN	show crypto isakmp sa; show crypto ipsec sa	Established SA and increasing packet counters
Standard ACL	show access-lists MGMT_ONLY	Only authorized management source allowed
Extended ACL	show access-lists USER_TO_SERVER	Expected permit/deny ACE counters increase
DHCP snooping	show ip dhcp snooping; show ip dhcp snooping binding	Trusted uplink and correct client binding
DAI	show ip arp inspection	DAI active on protected VLAN
Port security	show port-security interface ...	Secure-up; expected sticky MAC and violation behavior
AAA	AAA server logs + router AAA config	AuthN/AuthZ/accounting behavior observed
WLAN security	WLC GUI + client IP/ping	WPA2/AES PSK works and user lands in VLAN 20

Core command reference

```
show ip ssh
show users
show login
show access-lists
show crypto isakmp sa
show crypto ipsec sa
show ip dhcp snooping
show ip dhcp snooping binding
show ip arp inspection
show port-security interface GigabitEthernet0/1
show running-config | section aaa
show running-config | section tacacs
show ip dhcp binding
show interfaces trunk
```

What to verify

- Students can state exactly which output field proves each security control is working.
- Configuration, verification and controlled-failure evidence are kept in one forward sequence with no duplicated base configuration blocks.