Managing Network Device Security

Interconnecting Cisco Networking Devices, Part 1 (ICND1) v2.0

Securing Administrative Access

Managing Network Device Security

Network Device Security Overview

Network devices are vulnerable to these common threats:

- Remote access threats
  - Unauthorized remote access
- Local access and physical threats
  - Damage to equipment
  - Password recovery
  - Device theft
- Environmental threats
  - Extreme temperature
  - High humidity
- Electrical threats
  - Insufficient power supply voltage
  - Voltage spikes
- Maintenance threats
  - Improper handling
  - Poor cabling
  - Inadequate labeling

Securing Access to Privileged EXEC Mode

Configuring enable password:

```
Switch(config)#enable password C1sco123
```

Configuring enable secret password:

```
Switch(config)#enable secret sanfran
```

Verification of configured passwords:

```
Switch#show running-config | include enable
enable secret 5 $1$WPHF$uWo4ucV0/vA1/abu6L1WQ1
enable password C1sco123
```

Securing Access to Privileged EXEC Mode (Cont.)

Encrypting plaintext passwords:

```
Switch(config)#service password-encryption
Switch(config)#exit
Switch#show running-config | include enable
enable secret 5 $1$vWZa$2sYQLDv4R4xMtU5NFDrbX.
enable password 7 04785A150C2E1D1C5A
```

Securing Console Access

Console password:

```
Switch(config)#line console 0
Switch(config-line)#password C1sco123
Switch(config-line)#login
```

EXEC timeout:

```
Switch(config-line)#exec-timeout 5
```

Securing Remote Access

Virtual terminal password:

```
Switch(config)#line vty 0 15
Switch(config-line)#login
Switch(config-line)#password CiScO
```

EXEC timeout:

```
Switch(config-line)#exec-timeout 5
```

Securing Remote Access (Cont.)

Configuring SSH:

```
Switch(config)#hostname SwitchX
SwitchX(config)#ip domain-name cisco.com
SwitchX(config)#username user1 secret C1sco123
SwitchX(config)#crypto key generate rsa modulus 1024
The name for the keys will be: SwitchX.cisco.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
SwitchX(config)#line vty 0 15
SwitchX(config-line)#login local
SwitchX(config-line)#transport input ssh
SwitchX(config-line)#exit
SwitchX(config)#ip ssh version 2
```

Securing Remote Access (Cont.)

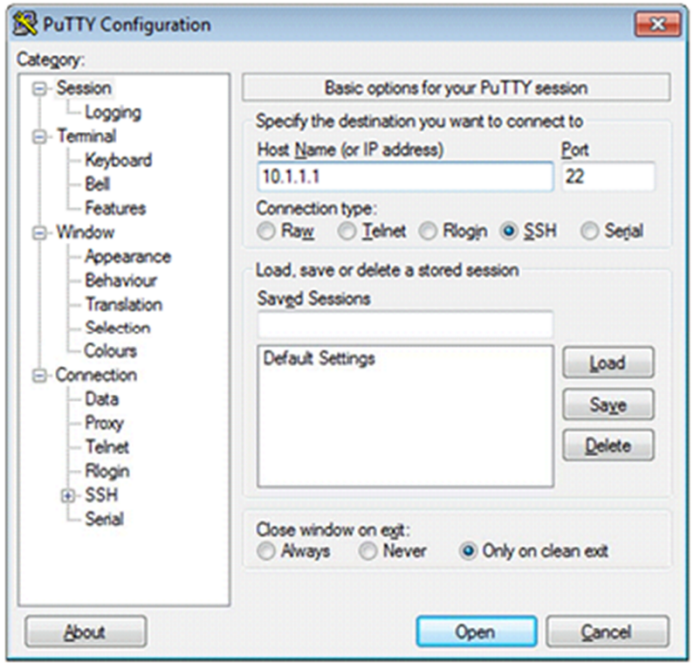
Verify that SSH is enabled:

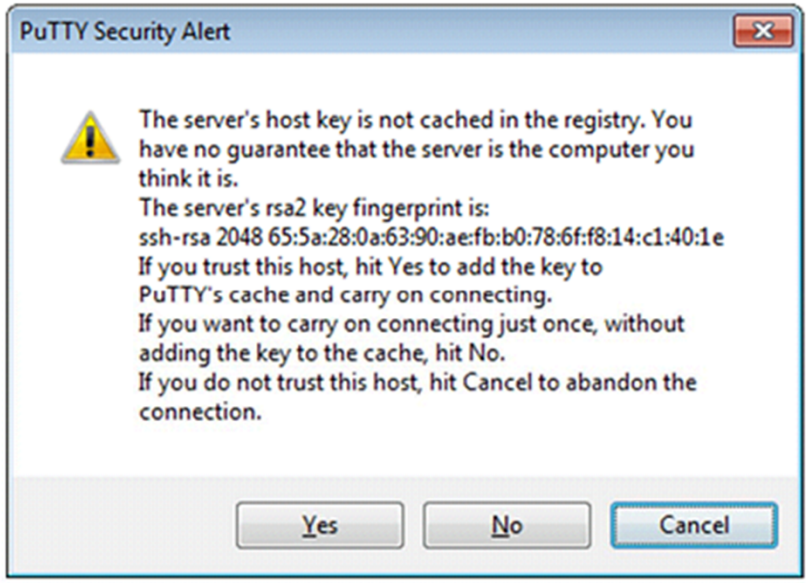
```
Switch#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

Check the SSH connection to the device:

```
Switch#show ssh
Connection  Version  Encryption     State              Username
0           1.5      3DES           Session started    cisco
```

Securing Remote Access (Cont.)



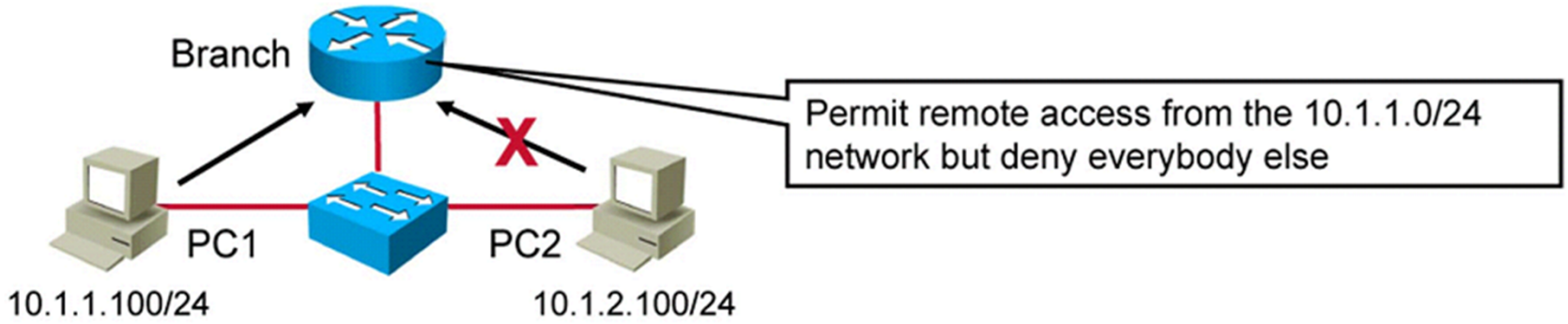


Enabling Remote Access Connectivity

Configure the IP address of a default gateway on a switch

```
SwitchX(config)#ip default-gateway 10.1.1.1
```

Limiting Remote Access with ACLs



Use an ACL to permit Telnet access from 10.1.1.0 /24 but deny everybody else:

```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#access-list 1 deny any log
```

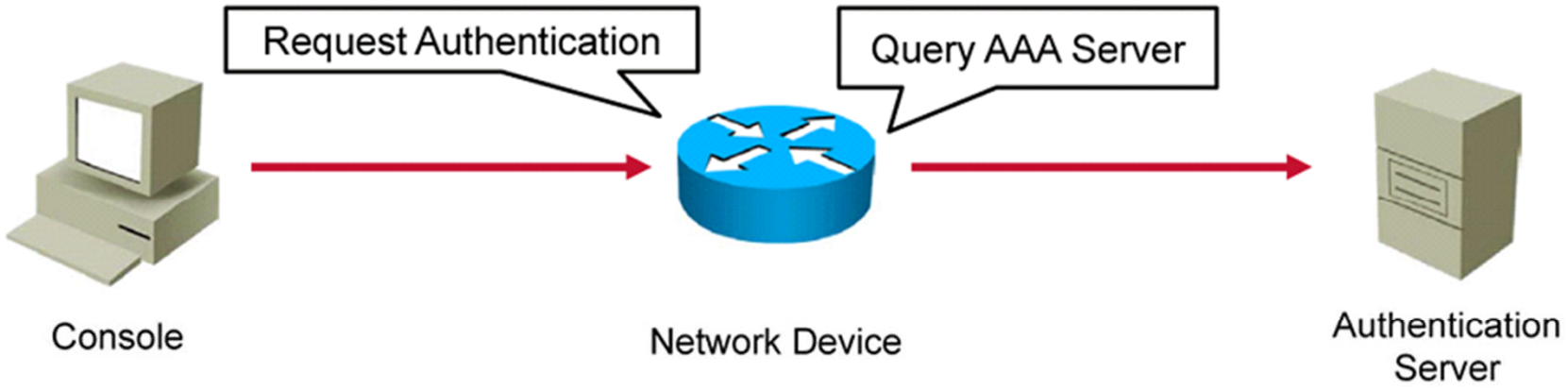
Apply the ACL on vty lines:

```
Router(config)#line vty 0 15
Router(config-line)#access-class 1 in
```

External Authentication Options

External authentication may be preferable to local authentication:

- A local authentication database can be an administrative burden.
- External authentication provides scalability.
- You can use RADIUS or TACACS+.



Configuring the Login Banner

Configure a login banner:

```
Switch(config)#banner login "Access for authorized users only. Please enter
your username and password."
```

A user connecting to the device sees this message:

```
Access for authorized users only. Please enter your username and password.
User Access Verification
Username:
```

Summary

- Security threats to network devices include remote access threats, physical and local access threats, environmental threats, electrical threats, and maintenance threats.
- You can secure a network device by using passwords to restrict access.
- You can secure console access to a network device by using console passwords and by using an EXEC timeout setting to prevent access from connected terminals.
- You can secure a network device for Telnet and SSH access by using vty passwords to restrict access and an EXEC timeout setting to prevent access from connected terminals.
- You can secure a network device for Telnet and SSH access by using an ACL to limit the users who can access the device.
- If you want a scalable option instead of a local authentication database, use the RADIUS or TACACS+ external authentication service.
- Use the **banner** command to configure a login or MOTD banner.

Implementing Device Hardening

Managing Network Device Security

Securing Unused Ports

- Unsecured ports can create a security vulnerability.
- A device that is plugged into an unused port is added to the network.
- Unused ports can be secured by disabling interfaces (ports).

Disabling an Interface (Port)

To shut down multiple ports, use the **interface range** command and use the **shutdown** command.

```
SwitchX(config)#interface range FastEthernet0/1 - 3
SwitchX(config-if-range)#shutdown
```

```
SwitchX#show running-config
<output omitted>
!
interface FastEthernet0/1
  shutdown
!
interface FastEthernet0/2
  shutdown
!
interface FastEthernet0/3
  shutdown
<output omitted>
```

The Fa0/1, Fa0/2, and Fa0/3 interfaces are disabled in the example.

Port Security

- How do you secure used ports?
- How do you prevent users from connecting unauthorized host devices to the network?

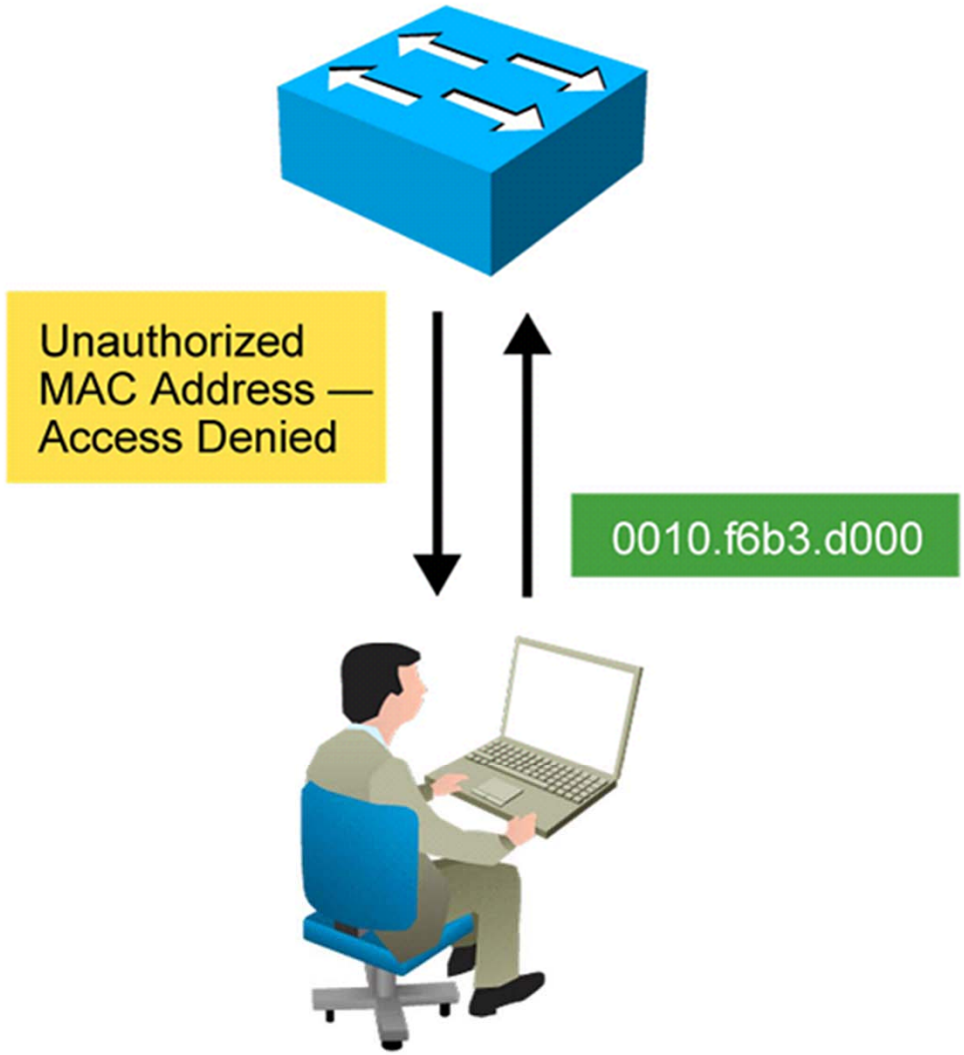
Example scenario:

- A classroom with PCs is connected to the network.
- How would you prevent students from unplugging classroom PCs and connecting their own notebooks to the network?

Port Security (Cont.)

Port security restricts port access by the MAC address.

- Dynamic (limited number of addresses)
- Static (static configuration of addresses)
- Combination (static plus dynamic)
- Sticky learning



Configuring Port Security

To configure port security on the Fa0/5 port to limit and identify the MAC addresses of stations that are allowed to access the port, do as follows:

1. Enable port security
2. Set the MAC address limit
3. Specify the allowable MAC addresses (optional)
4. Define the violation action

```
SwitchX(config)#interface FastEthernet0/5
SwitchX(config-if)#switchport mode access
SwitchX(config-if)#switchport port-security
SwitchX(config-if)#switchport port-security maximum 1
SwitchX(config-if)#switchport port-security mac-address sticky
SwitchX(config-if)#switchport port-security violation shutdown
```

Port Security Verification

```
SwitchX#show port-security interface FastEthernet 0/5
```

- Displays the port security settings that are defined for an interface

```
SwitchX#show port-security interface FastEthernet 0/5
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : fc99.47e5.2598:1
Security Violation Count    : 0
```

- Displays the port security settings that are defined for the FastEthernet 0/5 interface

Port Security Verification (Cont.)

```
SwitchX#show port-security interface FastEthernet 0/5
Port Security                          : Enabled
Port Status                            : Secure-shutdown
Violation Mode                         : Shutdown
Aging Time                             : 0 mins
Aging Type                             : Absolute
SecureStatic Address Aging             : Disabled
Maximum MAC Addresses                  : 1
Total MAC Addresses                    : 1
Configured MAC Addresses               : 0
Sticky MAC Addresses                   : 1
Last Source Address:Vlan               : 001a.2fe7.3089:1
Security Violation Count               : 1
```

- Displays the port security violation for the FastEthernet 0/5 interface

Port Security Verification (Cont.)

```
SwitchX#show interface status
Port      Name               Status       Vlan      Duplex  Speed Type
Fa0/1                        connected    1         a-full  a-100 10/100BaseTX
Fa0/2                        notconnect   1           auto   auto 10/100BaseTX
Fa0/3                        notconnect   1           auto   auto 10/100BaseTX
Fa0/4                        notconnect   1           auto   auto 10/100BaseTX
Fa0/5                        err-disabled 1            auto   auto 10/100BaseTX
<output omitted>
```

- Verifies the status of the interface

Port Security Verification (Cont.)

```
SwitchX#show port-security address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan  Mac Address       Type                  Ports   Remaining Age (mins)
----  -----------       ----                  -----   -------------
   1  0008.dddd.eeee     SecureConfigured      Fa0/5         -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

- Displays the secure MAC addresses for all ports

```
SwitchX#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)       (Count)
------------------------------------------------------------------------
      Fa0/5         1             1             0          Shutdown
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

- Displays the port security settings for the switch

Disabling Unused Services

Some services on Cisco devices may not be needed and therefore can be disabled, providing these benefits:

- Helps preserve system resources
- Eliminates the potential for security exploits on the disabled services

```
Router#show control-plane host open-ports
Active internet connections (servers and established)
Prot   Local Address   Foreign Address          Service    State
 tcp            *:22                *:0      SSH-Server   LISTEN
 tcp            *:23                *:0           Telnet  LISTEN
 udp            *:49  172.26.150.206:0   TACACS service   LISTEN
 udp            *:67                *:0    DHCPD Receive   LISTEN
```

- Displays the UDP or TCP ports that the router is listening to

Disabling Unused Services (Cont.)

The following are some general best practices:

- The finger, identification, TCP, and UDP small servers should remain disabled on all routers and switches.
- You should disable Cisco Discovery Protocol on interfaces where the service may represent a risk.
- It is strongly recommend that you turn off the HTTP service running on the router (HTTPS can stay on).

Disabling Unused Services (Cont.)

There are two options to disable Cisco Discovery Protocol:

Disable it globally (on all interfaces)

```
Router(config)#no cdp run
```

Disable it on a specific interface

```
Router(config)#interface FastEthernet0/24
Router(config-if)#no cdp enable
```

It is recommended that you disable the HTTP service

```
Router(config)#no ip http server
```

Network Time Protocol

Correct time within networks is important:

- Correct time allows the tracking of events in the network in the correct order.
- Clock synchronization is critical for the correct interpretation of events within syslog data.
- Clock synchronization is critical for digital certificates.

Network Time Protocol (Cont.)

NTP provides time synchronization between network devices.

- NTP can get the correct time from an internal or external time source:
  - Local master clock
  - Master clock on the Internet
  - GPS or atomic clock
- A router can act as an NTP server and client. Other devices (NTP clients) synchronize time with the router (NTP server).

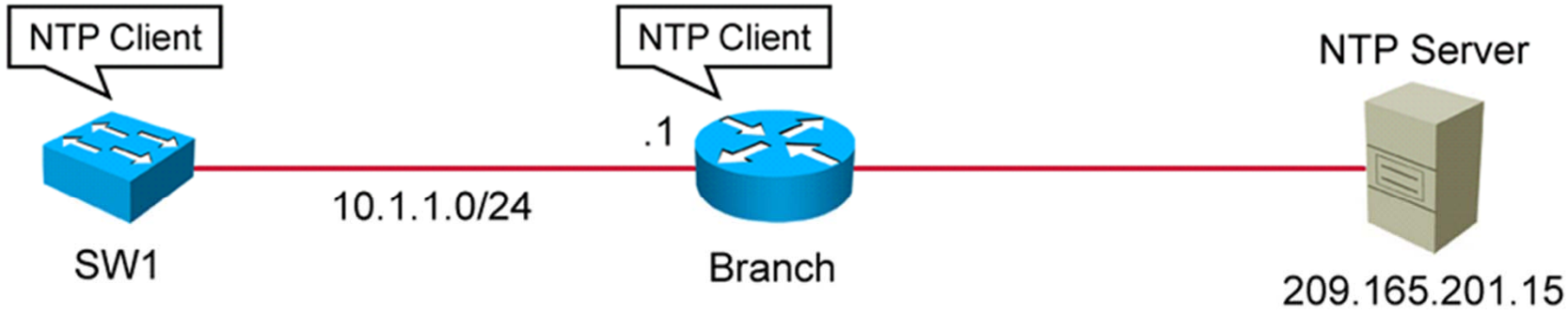
Configuring NTP

Configure the Branch router as the NTP client, which will synchronize its time with the NTP server.

```
Branch(config)#ntp server 209.165.201.15
```

Configure the SW1 switch as the NTP client, which will synchronize its time with the Branch router.

```
SW1(config)#ntp server 10.1.1.1
```



Verifying NTP

```
Branch#show ntp associations
  address         ref clock      st   when   poll reach   delay   offset disp
*~209.165.201.15  127.127.1.1    1    17     64   1       0.856   0.050  187.57
* sys.peer, #selected, + candidate, - outlyer, x falseticker, ~ configured
```

- Displays the status of NTP associations

```
Branch#show ntp status
Clock is synchronized, stratum 2, reference is 209.165.201.15
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is D40ADC27.E644C776 (13:18:31.899 UTC Mon Sep 24 2012)
clock offset is 6.0716 msec, root delay is 1.47 msec
root dispersion is 15.41 msec, peer dispersion is 3.62 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000091
s/s
system poll interval is 64, last update was 344 sec ago.
```

- Displays the status of NTP

Summary

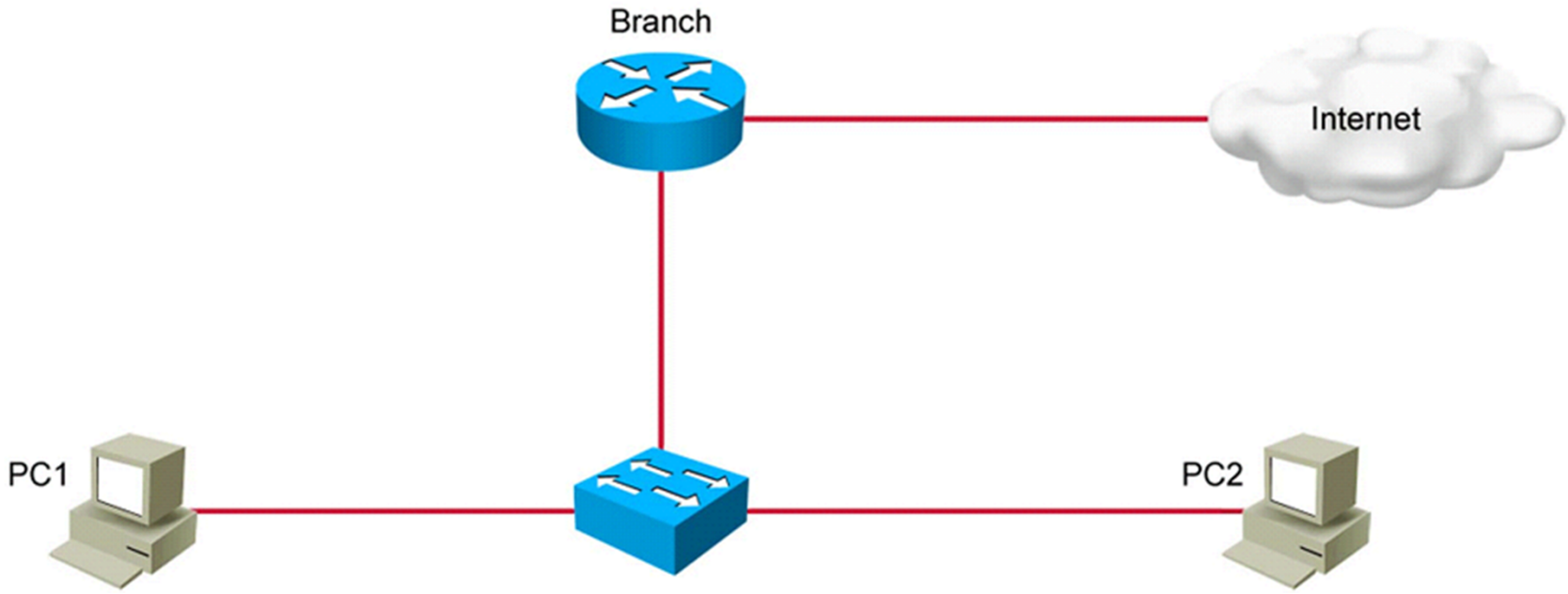
- Secure unused ports by disabling interfaces.
- The port security feature restricts a switch port to a specific set or number of MAC addresses.
- Before port security can be activated, the port mode must be set to static switchport mode.
- Use the **show port-security interface** command to display the port security settings that are defined for an interface.
- Some services on Cisco devices may not be needed and therefore can be disabled.
- NTP provides time synchronization between network devices.
- A Cisco router can act as an authoritative NTP server.
- Use the **show ntp associations** command to display the status of NTP associations.

Implementing Traffic Filtering with ACLs

Managing Network Device Security

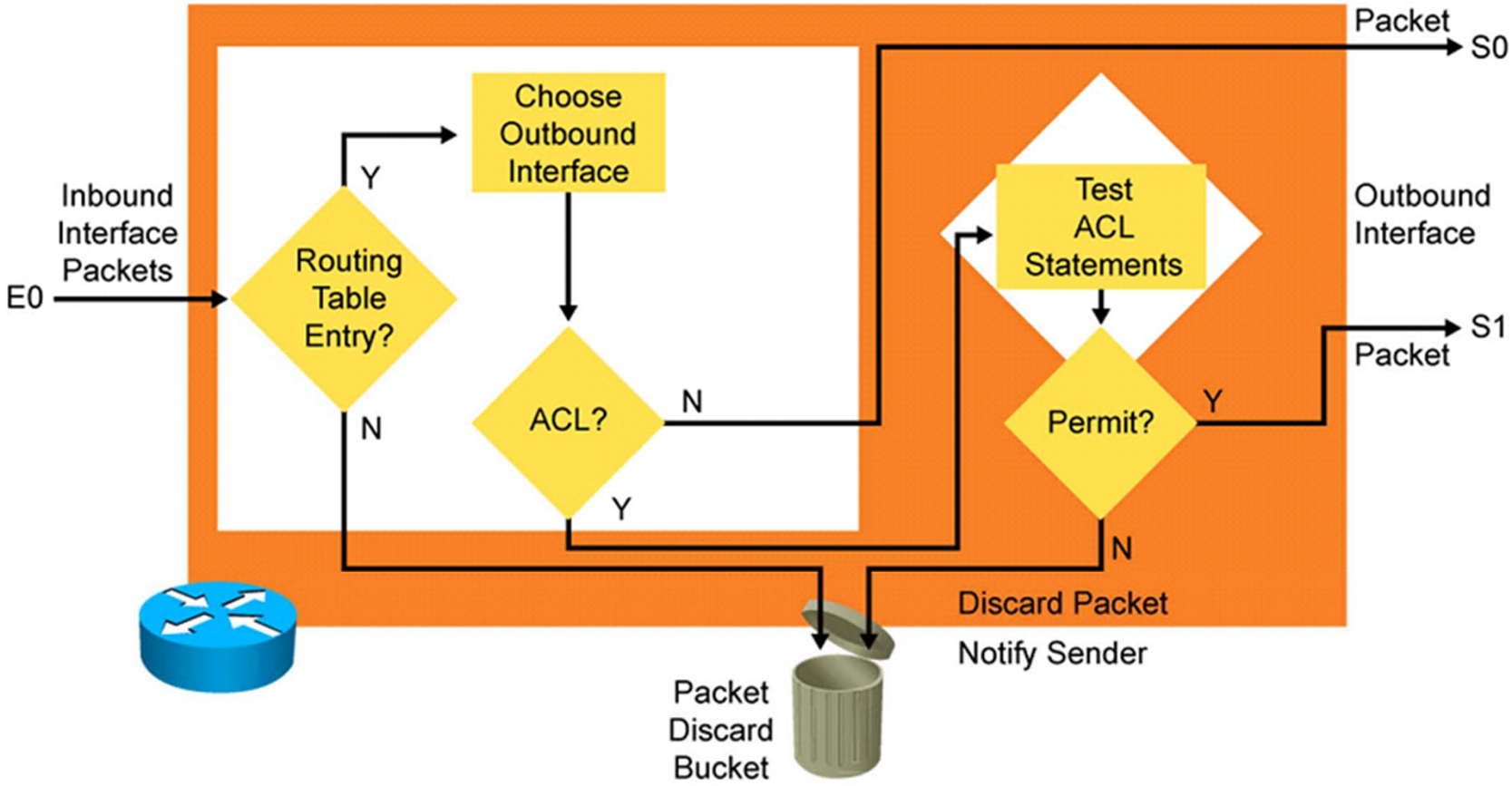
Using ACLs to Filter Network Traffic

How can you restrict Internet access for PC2?



ACL Operation

ACL operation outbound



Applying ACLs to Interfaces

Applies ACL 1 on the interface as an outbound filter:

```
Branch(config-if)#ip access-group 1 out
```

Applies ACL 2 on the interface as an inbound filter:

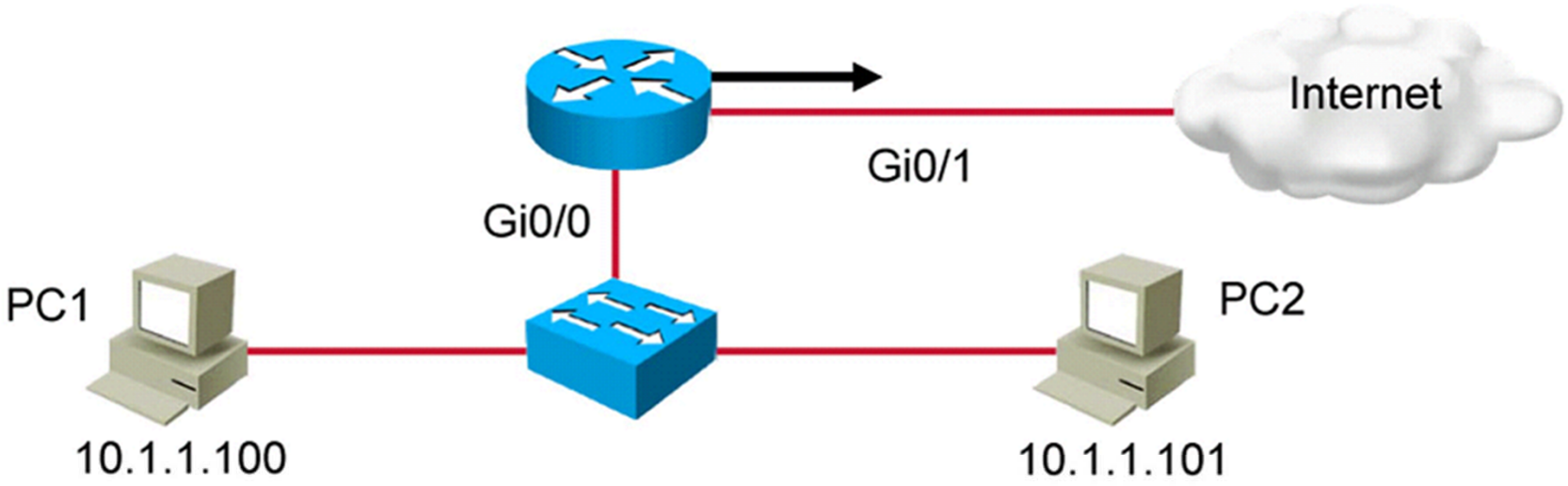
```
Branch(config-if)#ip access-group 2 in
```

Important: Only one ACL per protocol, per direction, and per interface is allowed.

Applying ACLs to Interfaces (Cont.)

Example:

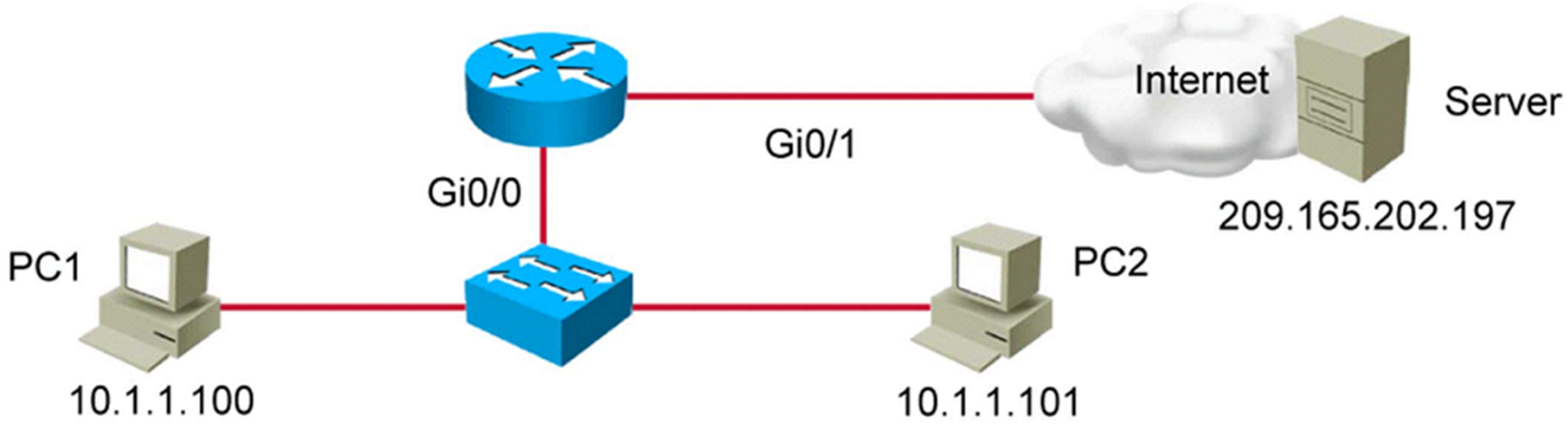
- Deny Internet access for a specific host (10.1.1.101).
- Allow all other LAN hosts to access the Internet.




```
Branch(config)#access-list 1 deny 10.1.1.101
Branch(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Branch(config)#interface GigabitEthernet 0/1
Branch(config-if)#ip access-group 1 out
```

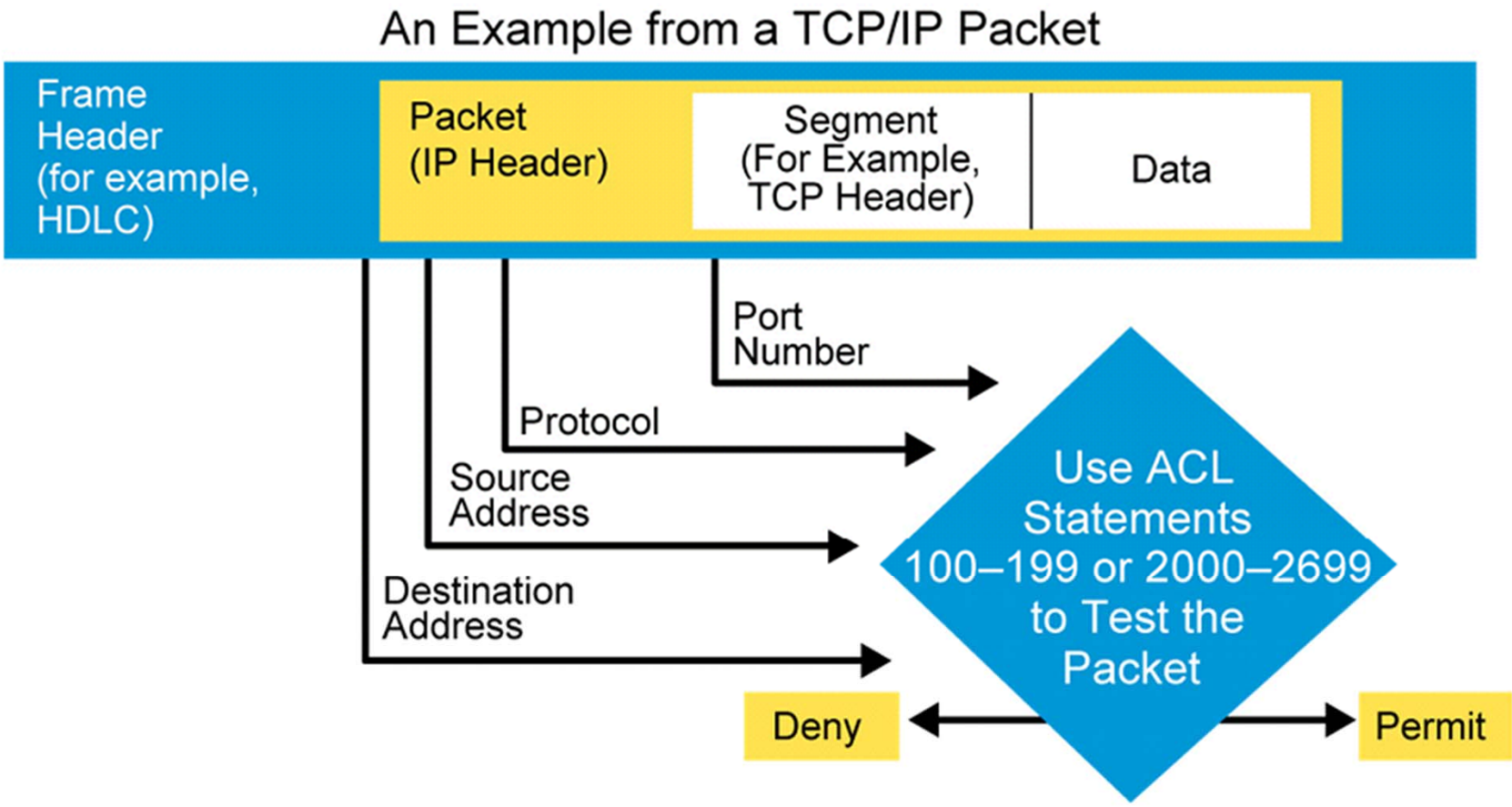
The Need for Extended ACLs

- How can you prevent PC2 from accessing only a specific server on the Internet?
- How can you allow other users only web access?



The Need for Extended ACLs (Cont.)

Testing packets with extended IPv4 ACLs



Configuring Numbered Extended IPv4 ACLs

```
Branch(config)#access-list 110 deny ip host 10.1.1.101 host 209.165.202.197
Branch(config)#access-list 110 permit tcp 10.1.1.0 0.0.0.255 any eq 80
```

- The number 110 is chosen to define an ACL as an extended ACL.
- The first statement matches IP traffic between two specific hosts and denies it.
- The second statement matches HTTP TCP traffic from network 10.1.1.0 /24.
  - The operator eq (equal) is used to match TCP port 80.
- The implicit deny statement is present at the end of the ACL

```
Branch(config-if)#ip access-group 110 in
```

An extended ACL is activated on the interface in the same way as a standard ACL.

Configuring Named ACLs

The ACL configuration mode is used to configure a named ACL.

```
Branch(config)#ip access-list extended WEB_ONLY
Branch(config-ext-nacl)#permit tcp 10.1.1.0 0.0.0.255 any eq www
Branch(config-ext-nacl)#20 permit tcp 10.1.1.0 0.0.0.255 any eq 443
```

- The alphanumeric name string (WEB_ONLY in the example) must be unique.
- If sequence numbers are not configured, they are generated automatically, starting at 10 and incrementing by 10.
- The **no 10** command removes the specific test that is numbered with 10 from the named ACL.

```
Branch(config-if)#ip access-group WEB_ONLY in
```

Named ACLs are activated on an interface with the same command as numbered ACLs.

Configuring Named ACLs (Cont.)

Edit an ACL in the access-list configuration mode to deny web access for host 10.1.1.25:

```
Branch#show access-lists
Extended IP access list WEB_ONLY
    10 permit tcp 10.1.1.0 0.0.0.255 any eq www
    20 permit tcp 10.1.1.0 0.0.0.255 any eq 443
Branch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Branch(config)#ip access-list extended WEB_ONLY
Branch(config-ext-nacl)#5 deny ip host 10.1.1.25 any
Branch(config-ext-nacl)#end
Branch#show access-lists
Extended IP access list WEB_ONLY
    5 deny ip host 10.1.1.25 any
    10 permit tcp 10.1.1.0 0.0.0.255 any eq www
    20 permit tcp 10.1.1.0 0.0.0.255 any eq 443
```

ACL Configuration Guidelines

These guidelines are recommended:

- The type of ACL, standard or extended, determines what is filtered.
- Only one ACL per interface, per protocol, and per direction is allowed.
- The most specific statement should be at the top of an ACL. The most general statement should be at the bottom of an ACL.
- The last ACL test is always an implicit “deny everything else” statement, so every list needs at least one permit statement.
- When placing an ACL in a network, follow these guidelines:
  - Place extended ACLs close to the source.
  - Place standard ACLs close to the destination.
- An ACL can filter traffic going through the router or traffic to and from the router, depending on how it is applied.

Monitoring ACLs

```
Branch#show access-lists
```

- Displays the content of ACLs

```
Branch#show access-lists
Standard IP access list SALES
    10 deny 10.1.1.0, wildcard bits 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list ENG
    10 permit tcp host 10.22.22.1 any eq telnet (25 matches)
    20 permit tcp host 10.33.33.1 any eq ftp
    30 permit tcp host 10.44.44.1 any eq ftp-data
```

Monitoring ACLs (Cont.)

```
Branch#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 10.1.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is WEB_ONLY
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  <text omitted>
```

- Shows whether an ACL is applied to an interface

Troubleshooting Common ACL Errors: Scenario 1

Host 10.10.1.1 has no connectivity with 10.1.1.2.

```
Branch#show access-lists 10
Standard IP access list 10
    10 permit 172.16.0.0, wildcard bits 0.0.0.255
```

Troubleshooting Common ACL Errors: Scenario 2

Host 10.10.1.1 has no connectivity with 10.1.1.2.

```
Branch#show access-lists 10
Standard IP access list 10
    10 deny   10.10.1.0, wildcard bits 0.0.0.255
    20 permit 10.10.1.1
    30 permit any
```

Troubleshooting Common ACL Errors: Scenario 3

Users from the 192.168.1.0 network cannot open a TFTP session to 10.1.1.2.

```
Branch#show access-lists 120
Extended IP access list 120
    10 deny tcp 172.16.0.0 0.0.255.255 any eq telnet
    20 deny tcp 192.168.1.0 0.0.0.255 any eq smtp
    30 permit tcp any any
```

Troubleshooting Common ACL Errors: Scenario 4

Users from the 172.16.0.0 network can use Telnet to connect to 10.1.1.2, but this connection should not be allowed.

```
Branch#show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.1.0 0.0.0.255 any eq smtp
    30 permit ip any any
```

Troubleshooting Common ACL Errors: Scenario 5

Host 10.10.1.1 can use Telnet to connect to 10.1.1.2, but this connection should not be allowed.

```
Branch#show access-lists 140
Extended IP access list 140
    10 deny tcp host 10.160.22.11 any eq telnet
    20 deny tcp 192.168.1.0 0.0.0.255 any eq smtp
    30 permit ip any any
```

Troubleshooting Common ACL Errors: Scenario 6

Host 10.1.1.2 can use Telnet to connect to 10.10.1.1, but this connection should not be allowed.


```
Branch#show access-lists 150
Extended IP access list 150
    10 deny tcp host 10.1.1.2 any eq telnet
    20 permit ip any any
Branch#show running-config interface Serial 0/0/0
interface Serial0/0/0
 ip address 10.160.22.33 255.255.255.0
 ip access-group 150 in
<output omitted>
```

Troubleshooting Common ACL Errors: Scenario 7

Host 10.10.1.1 can use Telnet to connect into the Branch router IP address, but this connection should not be allowed.

```
Branch#show access-lists 160
Extended IP access list 160
    10 deny tcp any host 10.160.22.33 eq telnet
    20 permit ip any any
```

Summary

- ACLs that are used for traffic filtering can operate in the inbound or outbound direction.
- One ACL per protocol, per direction, per interface is supported.
- Extended ACLs are used to filter traffic based on source and destination IP addresses, protocol, and port numbers.
- Numbered, extended ACLs use numbers from 100 to 199 and from 2000 to 2699.

Summary (Cont.)

- Access-list configuration mode allows adding, modifying, and deleting individual statements from an ACL.
- Place more specific statements at the top of an ACL and more general ones at the bottom.
- Use the **show access-lists** verification command to troubleshoot common ACL configuration errors.

Module Summary

- You should secure network devices by using passwords to restrict console, SSH, and Telnet access.
- Device hardening includes disabling unused ports, disabling unneeded services, configuring the port security feature, and configuring NTP.
- ACLs can be used for traffic filtering.