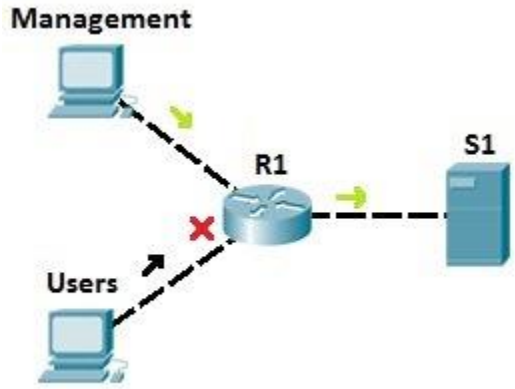
ACL Security

What are ACLs (Access Control Lists)?

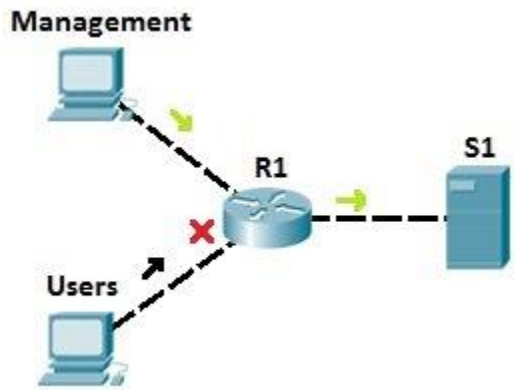
ACLs are a set of rules used most commonly to filter network traffic. They are used on network devices with packet filtering capatibilites (e.g. routers or firewalls). ACLs are applied on the interface basis to packets leaving or entering an interface.



ACL Types: Standard and Extended

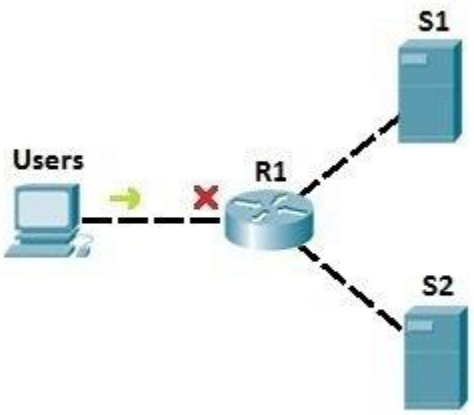
1. Standard Access Control Lists – with standard access lists, you can filter traffic only on the source IP address of a packet. These types of access lists are not as powerful as extended access lists, but they are less processor-intensive for the router.

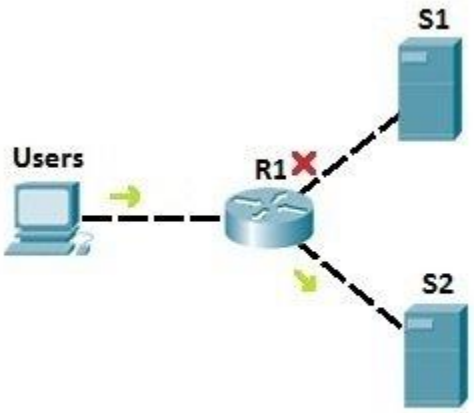
The following example describes the way in which standard access lists can be used for traffic flow control:

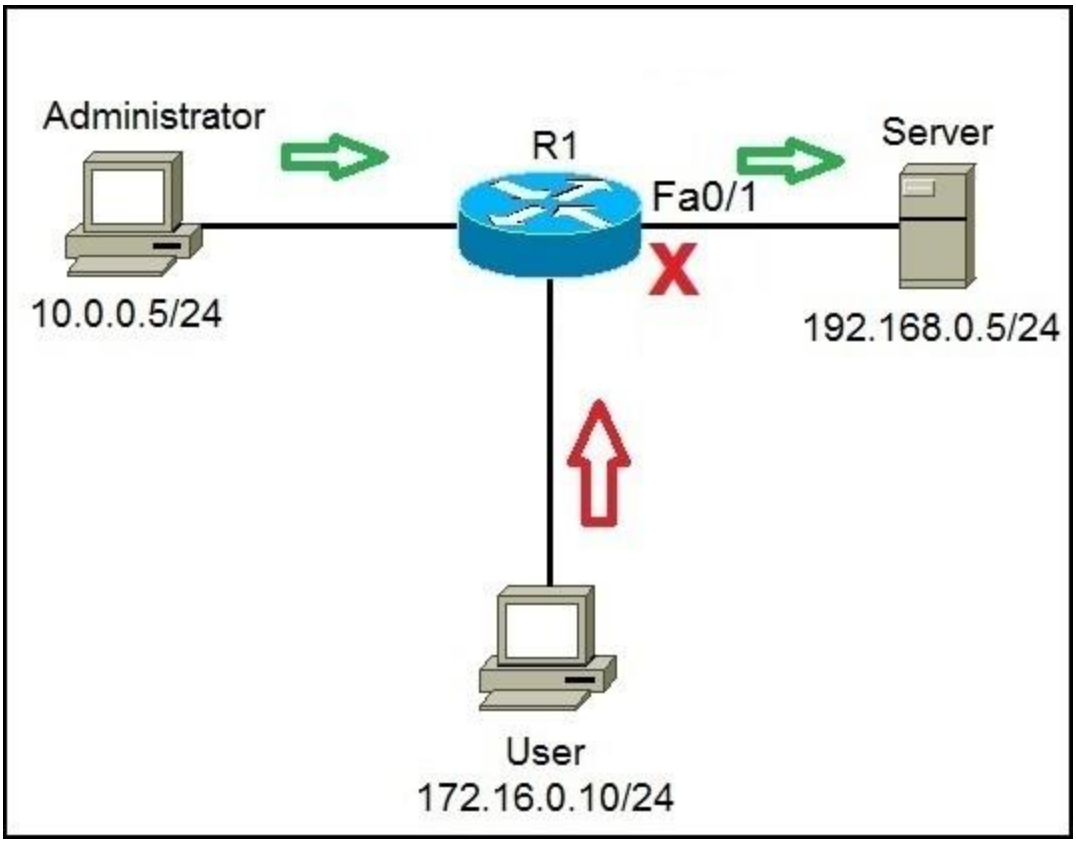


2. Extended Access Control Lists – with extended access lists, you can be more precise in your network traffic filtering. You can evaluate the source and destination IP addresses, type of layer 3 protocol, source and destination port, etc. Extended access lists are more complex to configure and consume more CPU time than standard access lists, but they allow a much more granular level of control.

To demonstrate the usefulness of extended ACLs, we will use the following example:







An **Access Control List (ACL)** is a set of rules that is usually used to filter network traffic. ACLs can be configured on network devices with packet filtering capatibilites, such as routers and firewalls.

ACLs containts a list of conditions that categorize packets and help you determine when to allow or deny network traffic. They are applied on the interface basis to packets leaving or entering an interface. Two types of ACLs are available on a Cisco device:

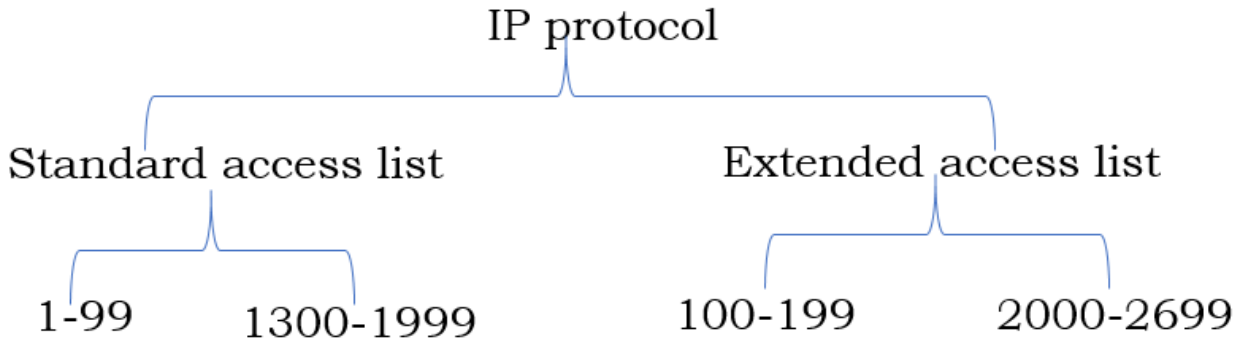
- **standard access lists** – allow you to evaluate only the source IP address of a packet. Standard ACLs are not as powerful as extended access lists, but they are less CPU intensive for the device.
- **extended access lists** – allow you to evaluate the source and destination IP addresses, the type of Layer 3 protocol, source and destination port, and other parameters. Extended ACLs are more complex to configure and require more CPU time than the standard ACLs, but they allow more granular level of control.

access-list

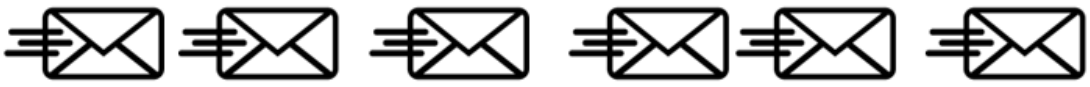
1. Standard-numbered
2. Extended-numbered

ip access-list

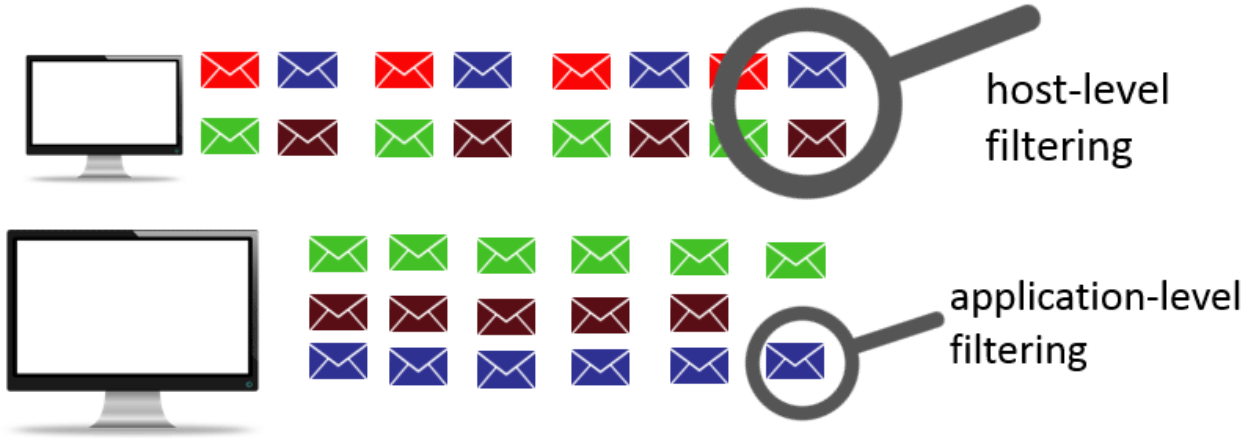
1. Standard-numbered
2. Standard-named
3. Standard-numbered with the sequence editing feature
4. Standard-named with the sequence editing feature
5. Extended-numbered
6. Extended-named
7. Extended-numbered with the sequence editing feature
8. Extended-named with the sequence editing feature



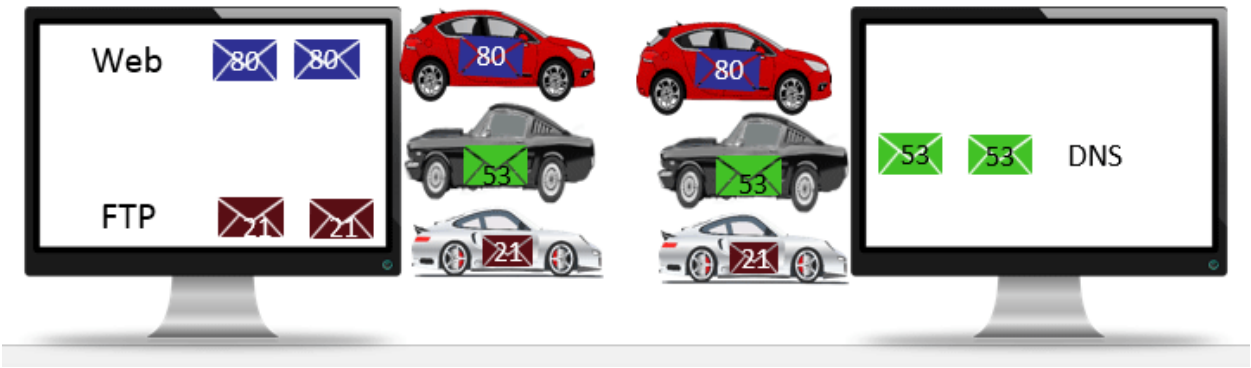
If you use the permit option, the router will allow the packet that matches the condition defined next to it.



If you use the deny option, the router will block the packet that matches the condition defined next to it.

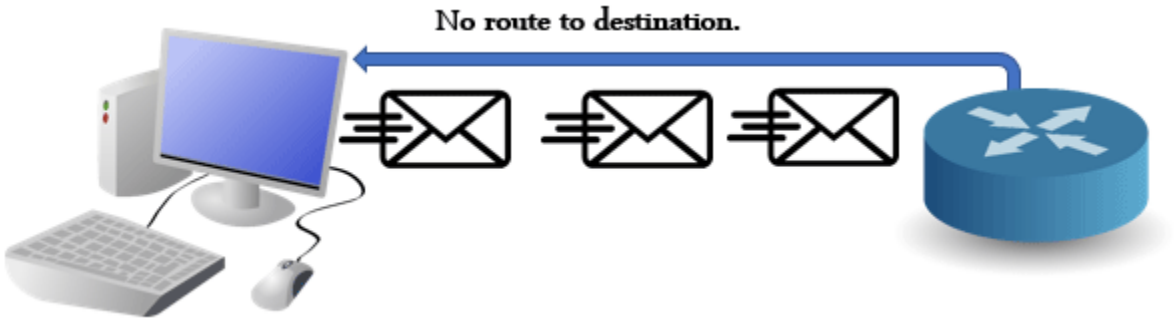


Application-level filtering



ICMP

Sending a packet is not a guarantee of the packet being delivered. Sometimes packets get lost on the way to the destination. In such a case, the nearest device sends the error message back to the sender. From the message, the sender can know about the undelivered packets and their possible reasons. Networking devices use the ICMP protocol to send error messages.



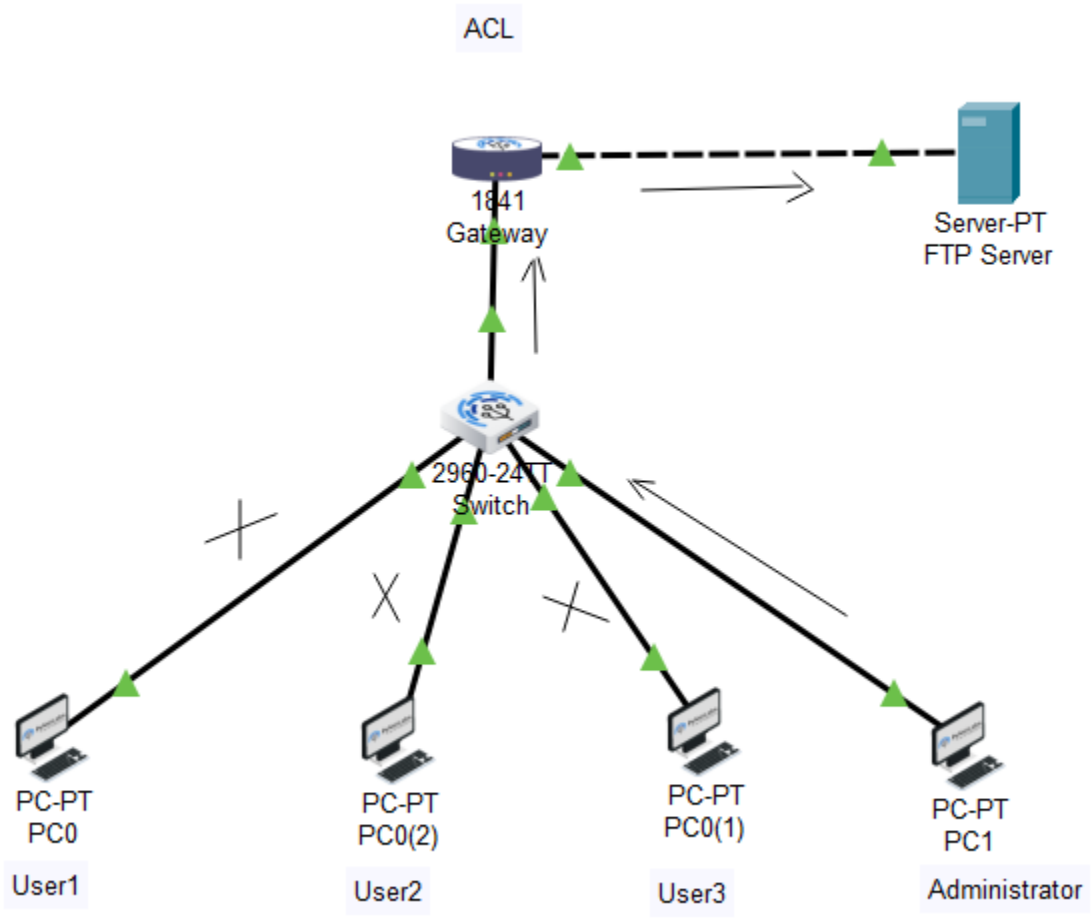
ACLs or Access control Lists can be used for two purposes, namely:

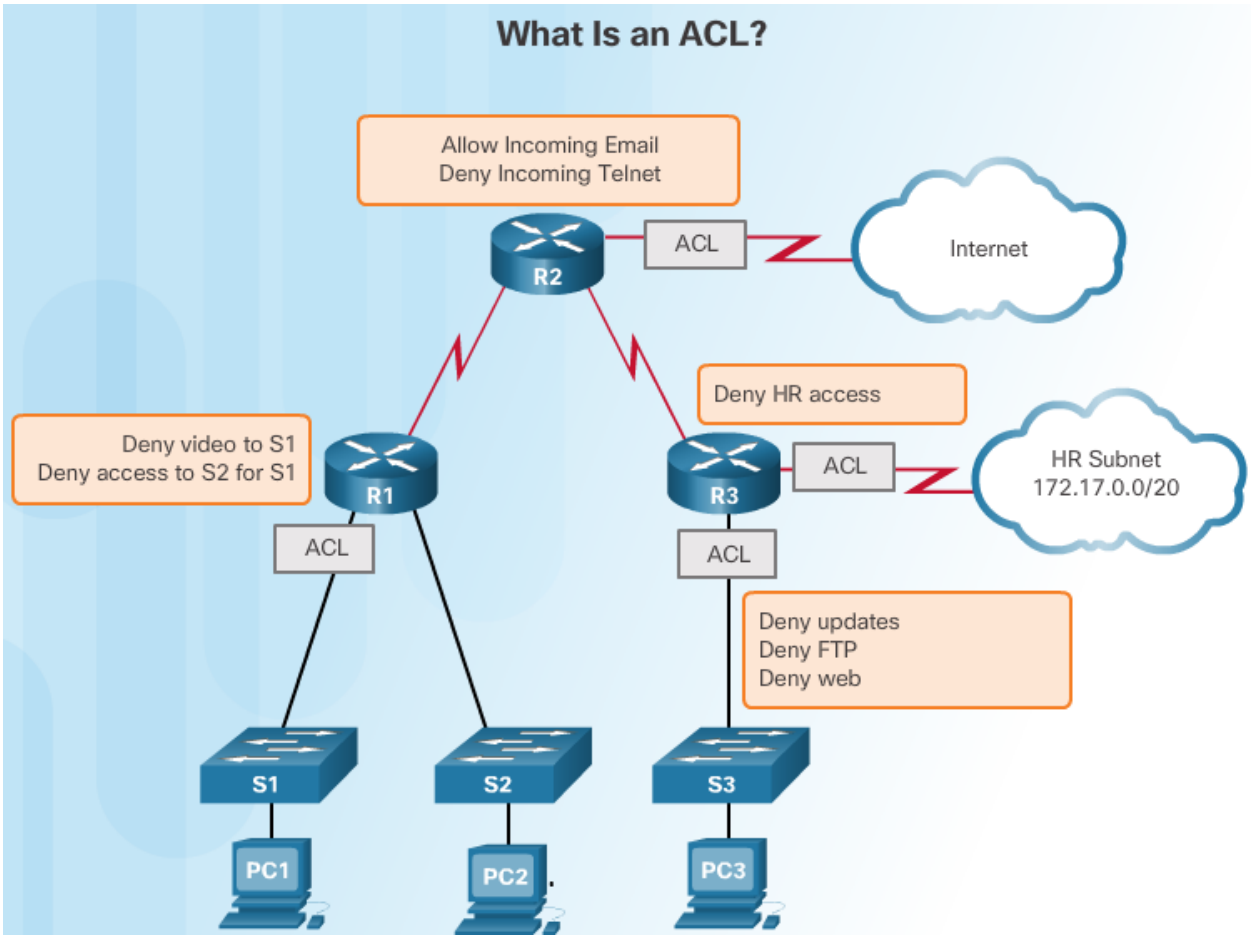
1. To filter traffic
2. To identify traffic

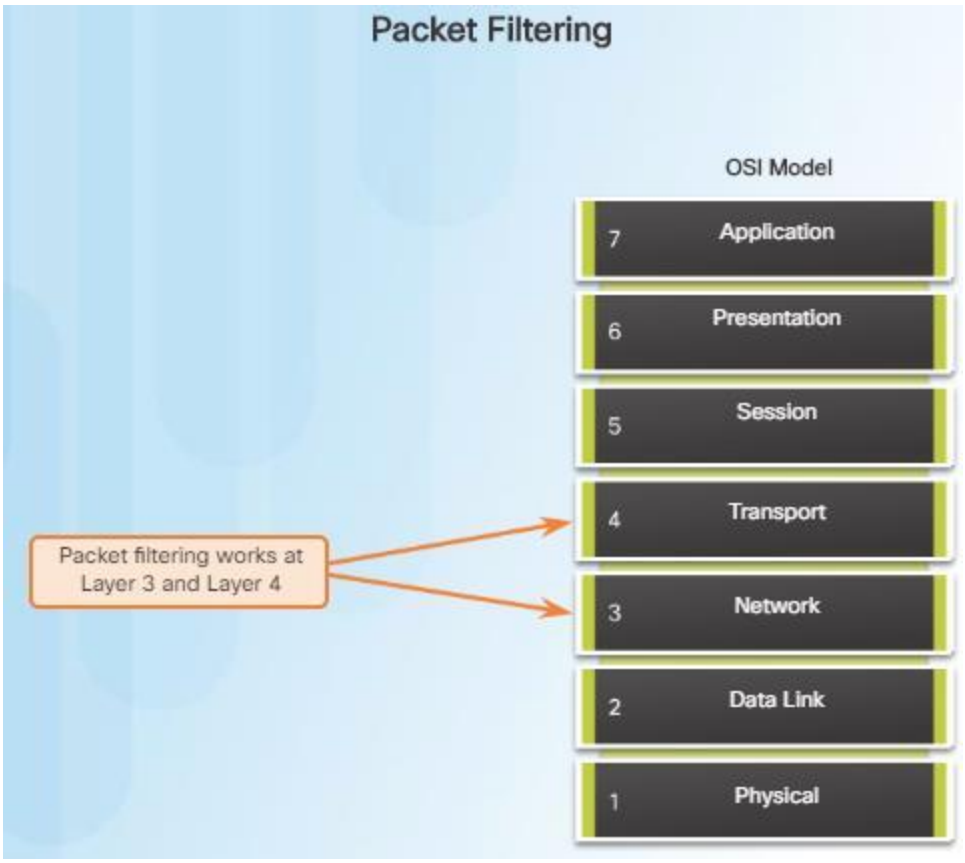
As mentioned above, access lists are a set of rules organized in a rule table. A condition, either permit or deny, is provided by each rule or line in an access list.

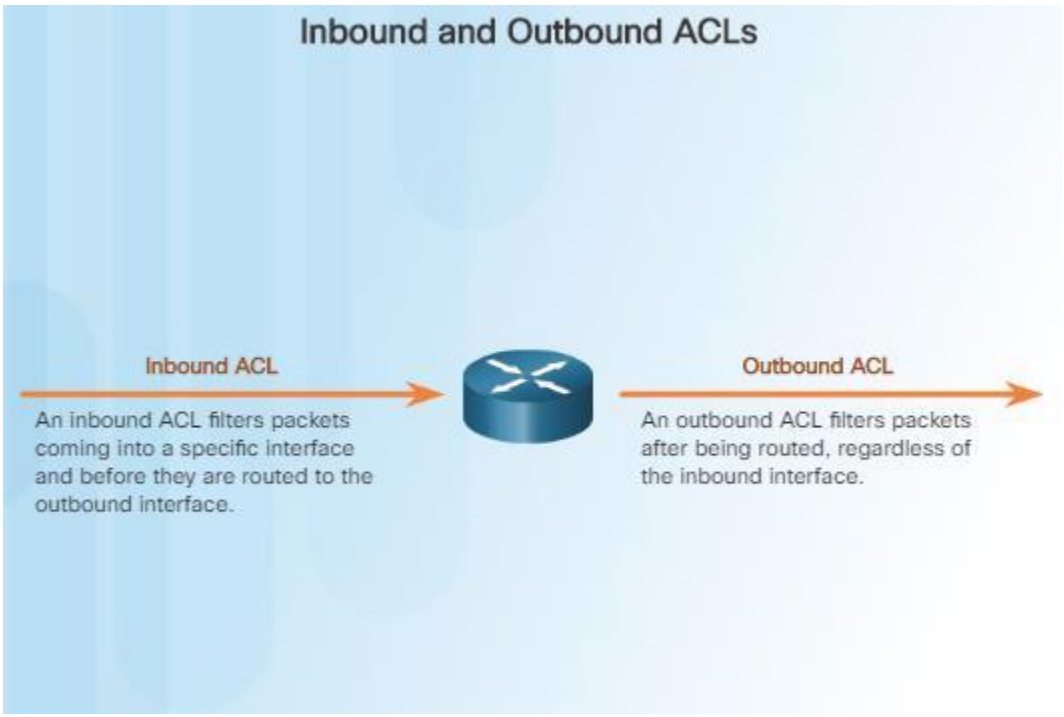
- When an access list is used to filter the traffic -
  - a permit statement is used to "allow" traffic,
  - Whereas, to "block" traffic, a deny statement is used.
- In a similar way, when identifying traffic with an access list -
  - a permit statement is used to include traffic

- A deny statement, on the other hand, makes it clear that the traffic should "not" be included.

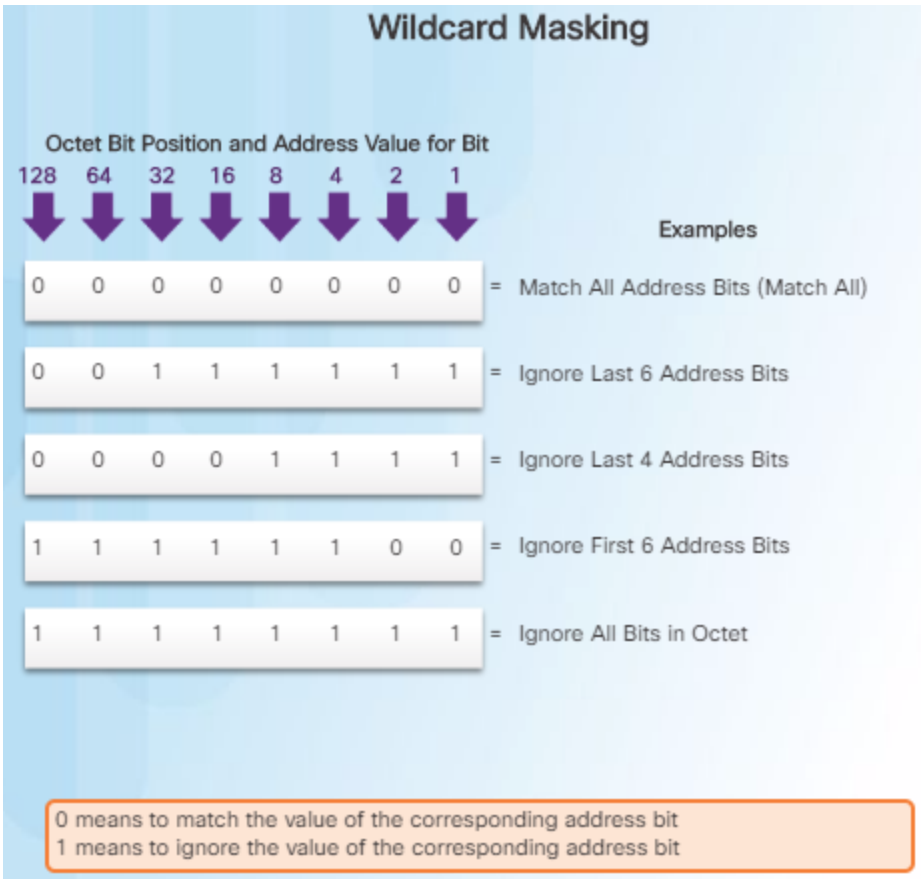



What Is an ACL?
Allow Incoming Email
Deny Incoming Telnet
ACL
Internet
R2
Deny HR access
Deny video to S1
Deny access to S2 for S1
R1
R3
ACL
HR Subnet
172.17.0.0/20
ACL
ACL
Deny updates
Deny FTP
Deny web
S1
S2
S3
PC1
PC2
PC3


Packet Filtering
OSI Model
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Packet filtering works at Layer 3 and Layer 4


Inbound and Outbound ACLs
Inbound ACL
An inbound ACL filters packets coming into a specific interface and before they are routed to the outbound interface.
Outbound ACL
An outbound ACL filters packets after being routed, regardless of the inbound interface.

Wildcard Masking



0 means to match the value of the corresponding address bit
1 means to ignore the value of the corresponding address bit

Wildcard Masks to Match IPv4 Hosts and Subnets

Example 1

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0	00000000.00000000.00000000.00000000
Result	192.168.1.1	11000000.10101000.00000001.00000001

Example 2

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	255.255.255.255	11111111.11111111.11111111.11111111
Result	0.0.0.0	00000000.00000000.00000000.00000000

Example 3

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000

Wildcard Mask Calculation

Example 1

```
  255.255.255.255
- 255.255.255.000
-----------------
              255
```

Example 2

```
  255.255.255.255
- 255.255.255.240
-----------------
               15
```

Example 3

```
  255.255.255.255
- 255.255.254.000
-----------------
            1.255
```

Wildcard Bit Mask Abbreviations

Example 1

- 192.168.10.10 0.0.0.0 matches all of the address bits
- Abbreviate this wildcard mask using the IP address preceded by the keyword `host` (`host 192.168.10.10`)

Example 2

- 0.0.0.0 255.255.255.255 ignores all address bits
- Abbreviate expression with the keyword `any`

The any and host Keywords

Example 1

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
!OR
R1(config)# access-list 1 permit any
```

Example 2

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
!OR
R1(config)# access-list 1 permit host 192.168.10.10
```

This is the format of the `host` and `any` optional keywords in an ACL statement.

ACL Traffic Filtering on a Router

One list per interface, per direction, and per protocol

With two interfaces and two protocols running, this router could have a total of 8 separate ACLs applied.

The Rules for Applying ACLs

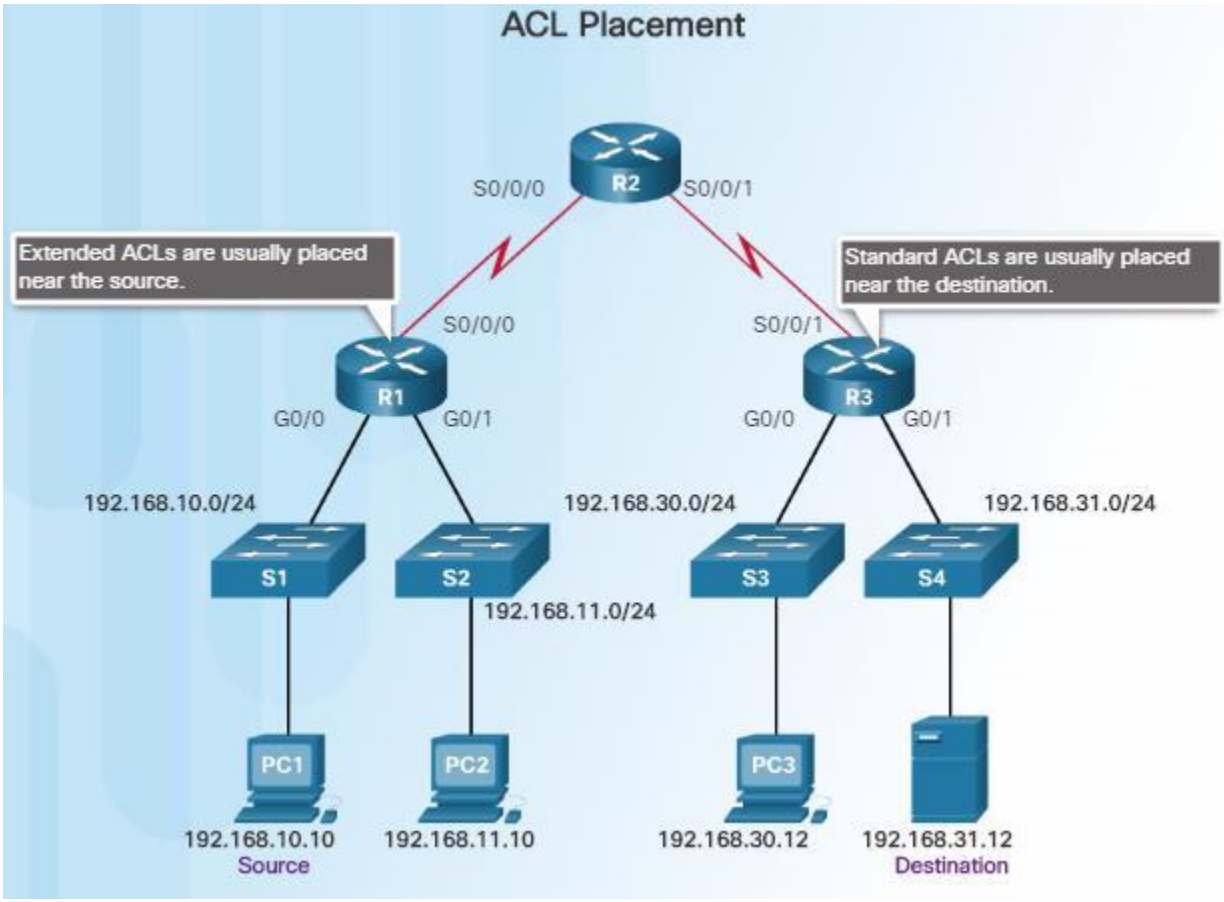
You can only have one ACL per protocol, per interface, and per direction:

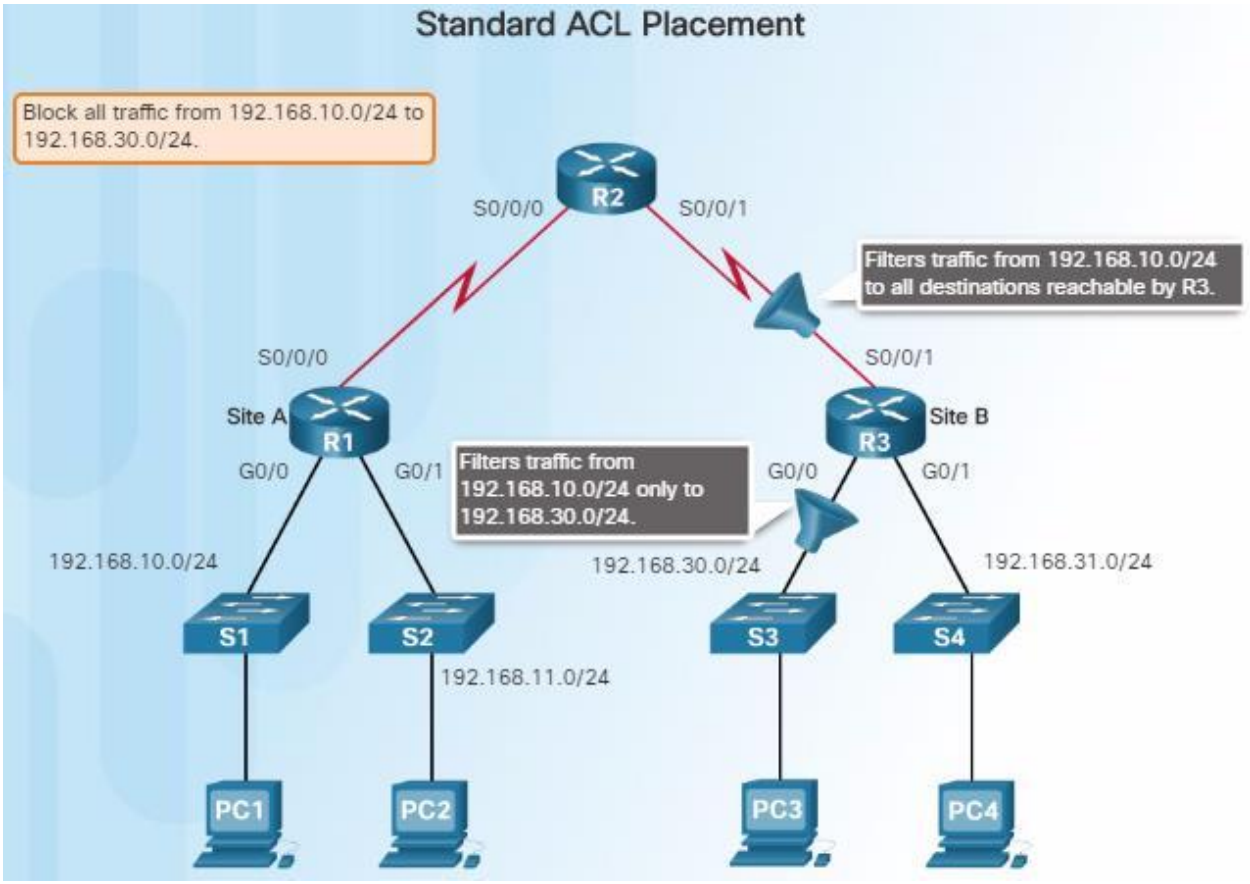
- One ACL per protocol (e.g., IPv4 or IPv6)
- One ACL per direction (i.e., IN or OUT)
- One ACL per interface (e.g., GigabitEthernet0/0)

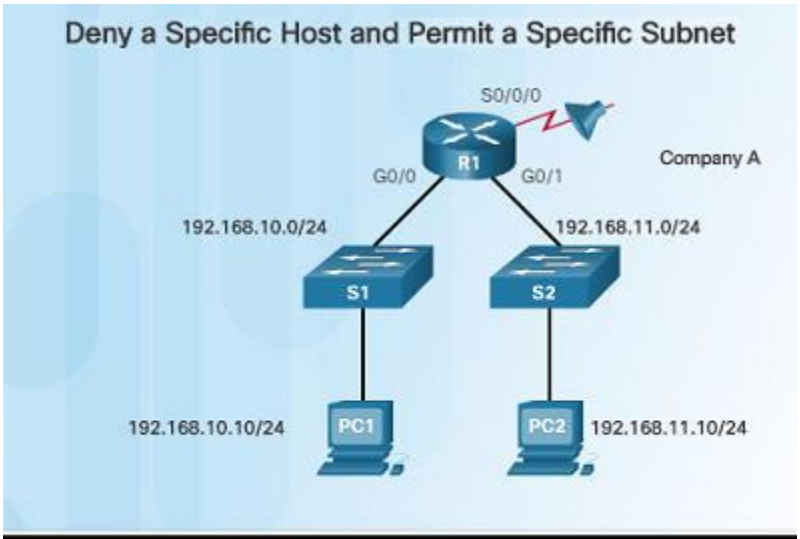
ACL Best Practices

Guideline	Benefit
Base your ACLs on the security policy of the organization.	This will ensure you implement organizational security guidelines.
Prepare a description of what you want your ACLs to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit, and save ACLs.	This will help you create a library of reusable ACLs.
Test your ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

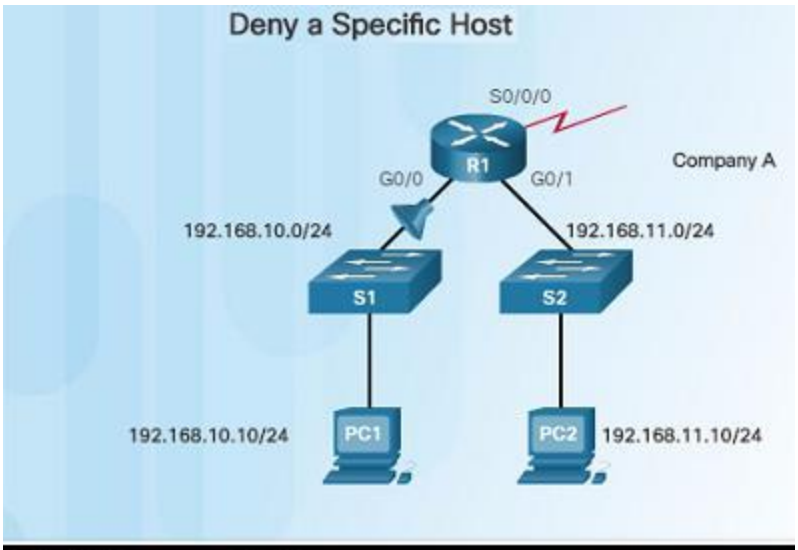
ACL Placement



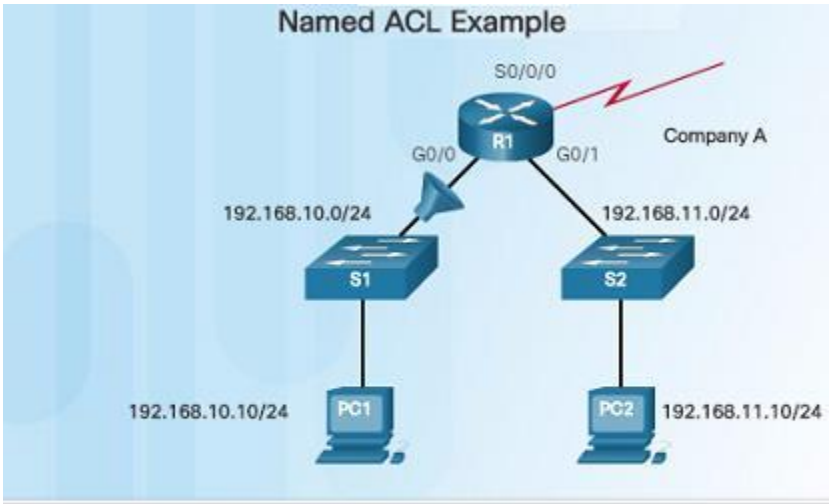





```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```




```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit any
R1(config)# interface g0/0
R1(config-if)# ip access-group 1 in
```




```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Editing Numbered ACLs Using a Text Editor

Configuration

```
R1(config)# access-list 1 deny host 192.168.10.99
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 1

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.99
access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 2

```
<Text editor>
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 3

```
R1# config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 4

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Editing Numbered ACLs Using Sequence Numbers

Configuration

```
R1(config)# access-list 1 deny host 192.168.10.99
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Step 1

```
R1# show access-lists 1
Standard IP access list 1
    10 deny   192.168.10.99
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

Step 2

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1#
```

Step 3

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

```
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

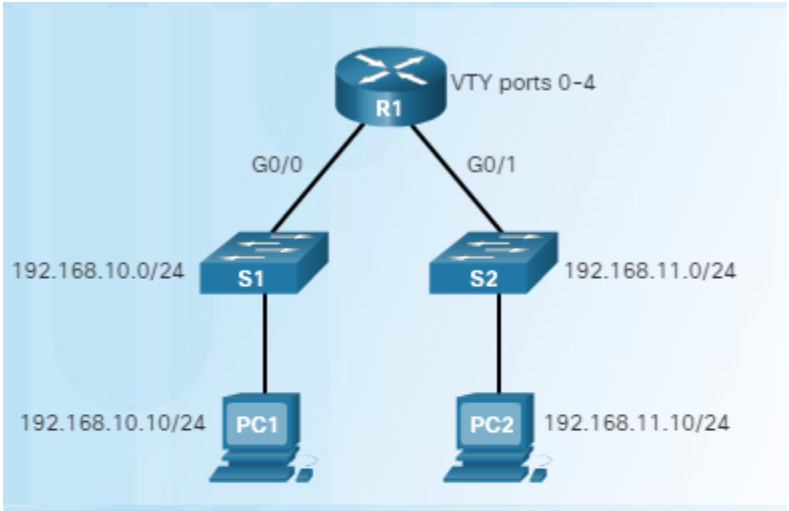
```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
  Inbound access list is not set
<output omitted>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
  Inbound access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
  10 deny 192.168.10.10
  20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
  15 deny 192.168.11.11
  10 deny 192.168.11.10
  20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

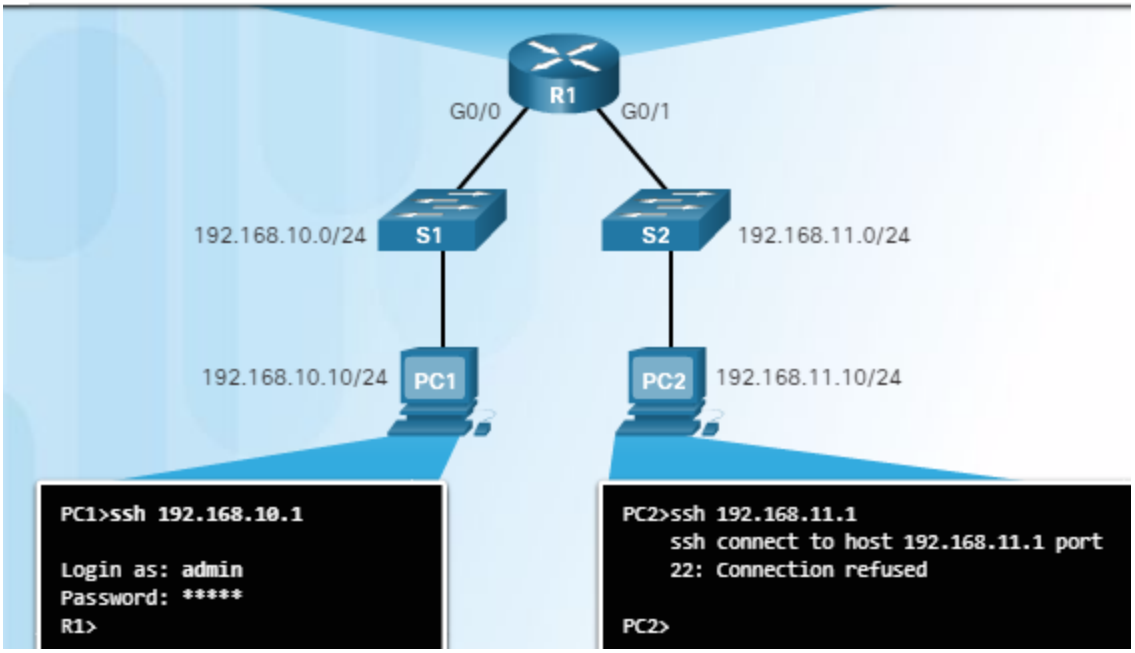
```
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10 (8 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# clear access-list counters 1
R1#
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

Matches have been cleared.

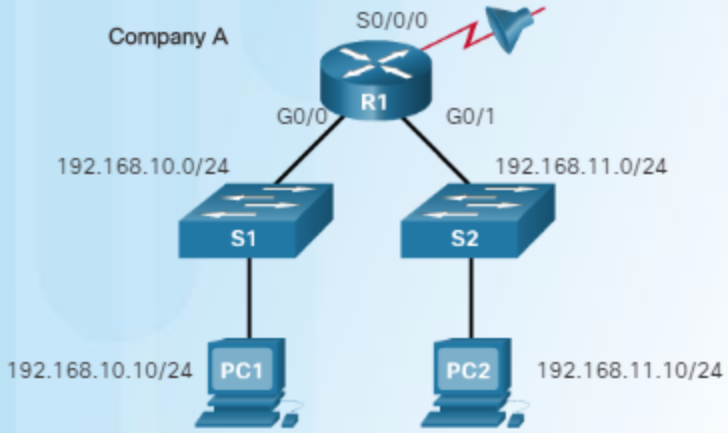



```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

```
R1# show access-lists
Standard IP access list 21
    10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
    20 deny any (1 match)
R1#
```



Entering Criteria Statements



ACL 1

```
R1(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
```

ACL 2

```
R1(config)# access-list 2 permit ip 192.168.10.0 0.0.0.255
R1(config)# access-list 2 deny any
```

Conflict with Statements

```
R1(config)# access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 3 permit host 192.168.10.10
%Access rule can't be configured at higher sequence num as it is part of the existing
rule at sequence num 10
R1(config)#
```

ACL 3: Host statement conflicts with previous range statement.

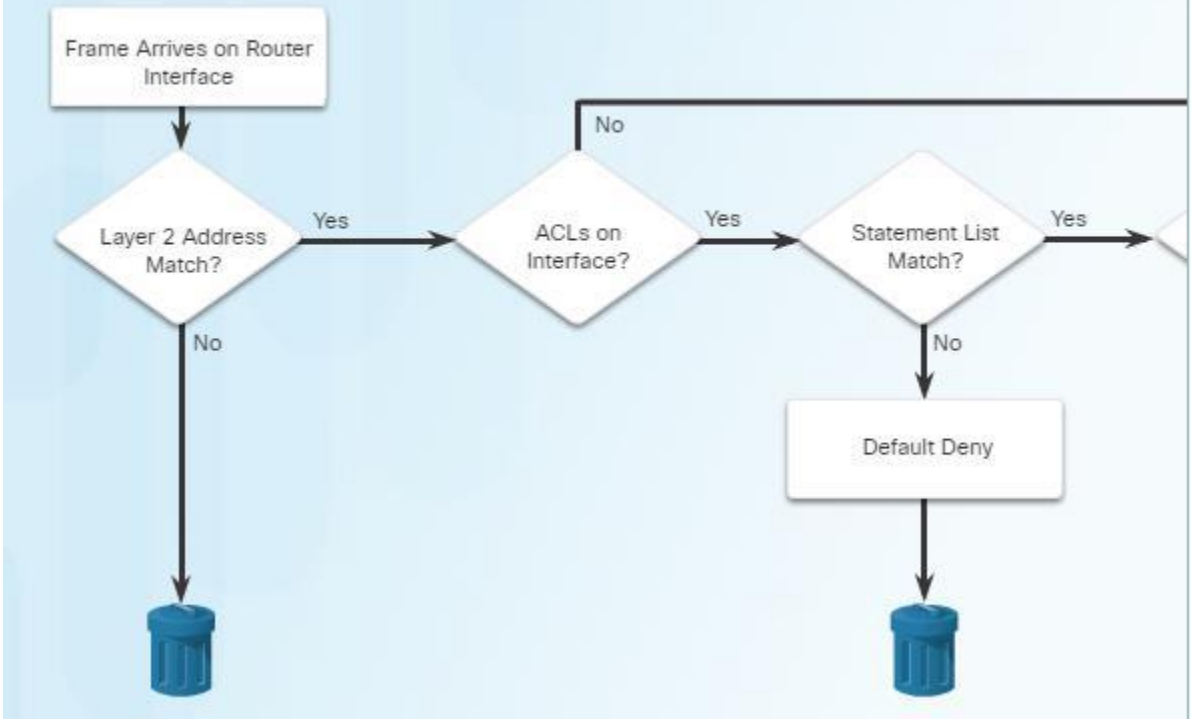
Sequencing Considerations During Configuration

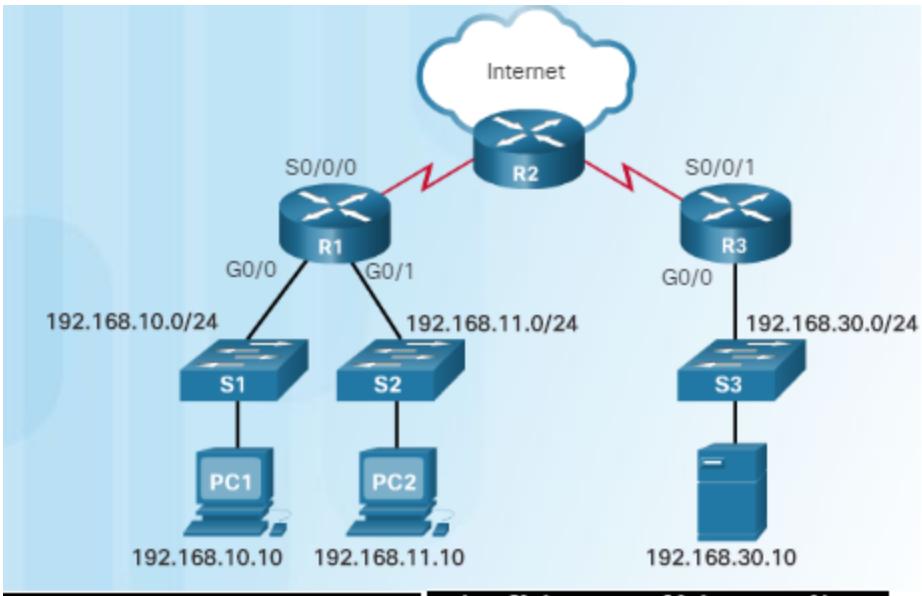
```
R1(config)# access-list 1 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 1 deny 192.168.20.0 0.0.0.255
R1(config)# access-list 1 deny 192.168.30.0 0.0.0.255
R1(config)# access-list 1 permit 10.0.0.1
R1(config)# access-list 1 permit 10.0.0.2
R1(config)# access-list 1 permit 10.0.0.3
R1(config)# access-list 1 permit 10.0.0.4
R1(config)# access-list 1 permit 10.0.0.5
R1(config)# end
R1# show running-config | include access-list 1
access-list 1 permit 10.0.0.2
access-list 1 permit 10.0.0.3
access-list 1 permit 10.0.0.1
access-list 1 permit 10.0.0.4
access-list 1 permit 10.0.0.5 access-list 1 deny 192.168.10.0 0.0.0.255
access-list 1 deny 192.168.20.0 0.0.0.255
access-list 1 deny 192.168.30.0 0.0.0.255
R1#
```

Range (network) statements

Host statements

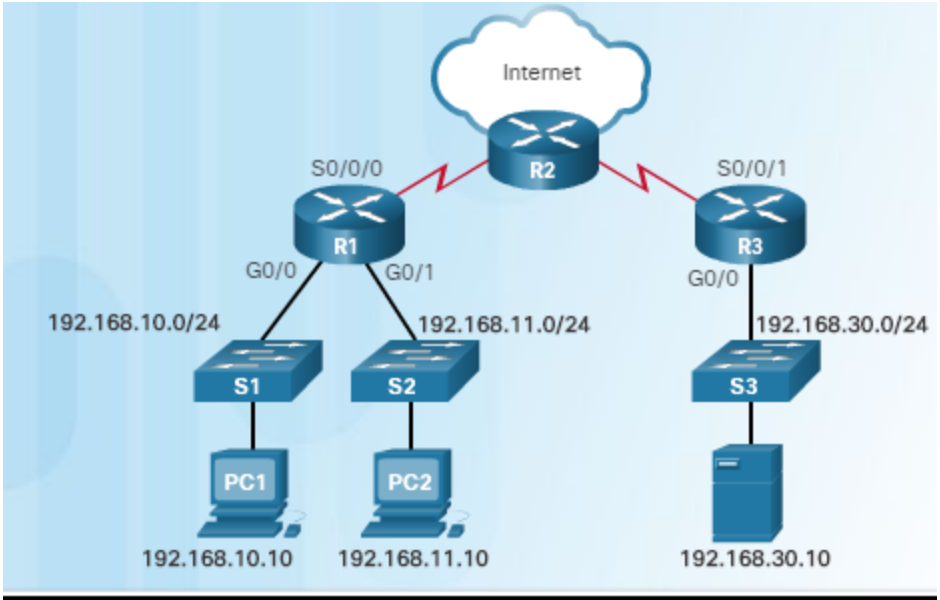
ACL and Routing Processes in a Router



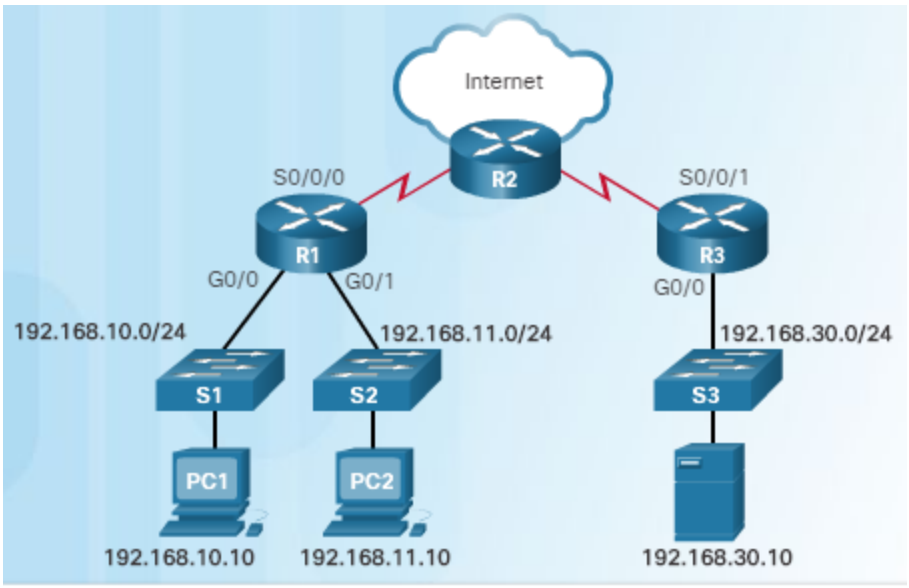



```
R3# show access-list
Standard IP access list 10
    10 deny 192.168.11.10
R3#
```

```
R3(config)# access-list 10 permit any
R3(config)# end
R3# show access-list
Standard IP access list 10
    10 deny 192.168.11.10
    20 permit any (4 match(es))
R3#
```



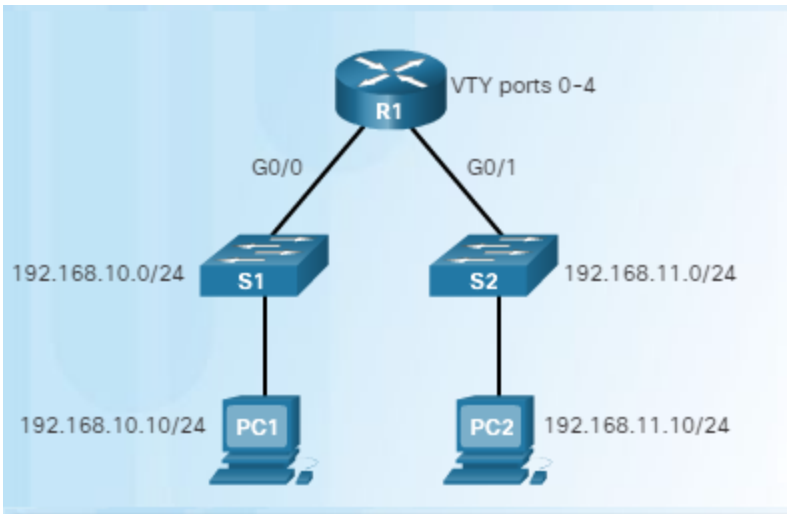

```
R1# show run | section interface
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
interface GigabitEthernet0/1
ip address 192.168.11.1 255.255.255.0
ip access-group 20 in
duplex auto
speed auto
<output ommitted>
```




```
R1# show run | section line vty
line vty 0 4
 access-class PC1-SSH in
 login
 transport input ssh
R1# show access-list
Standard IP access list PC1-SSH
    10 permit 192.168.10.1
    20 deny   any (5 match(es))
R1#
```

```
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10 (8 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# clear access-list counters 1
R1#
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

Matches have been cleared.




```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

```
R1# show access-lists
Standard IP access list 21
    10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
    20 deny any (1 match)
R1#
```