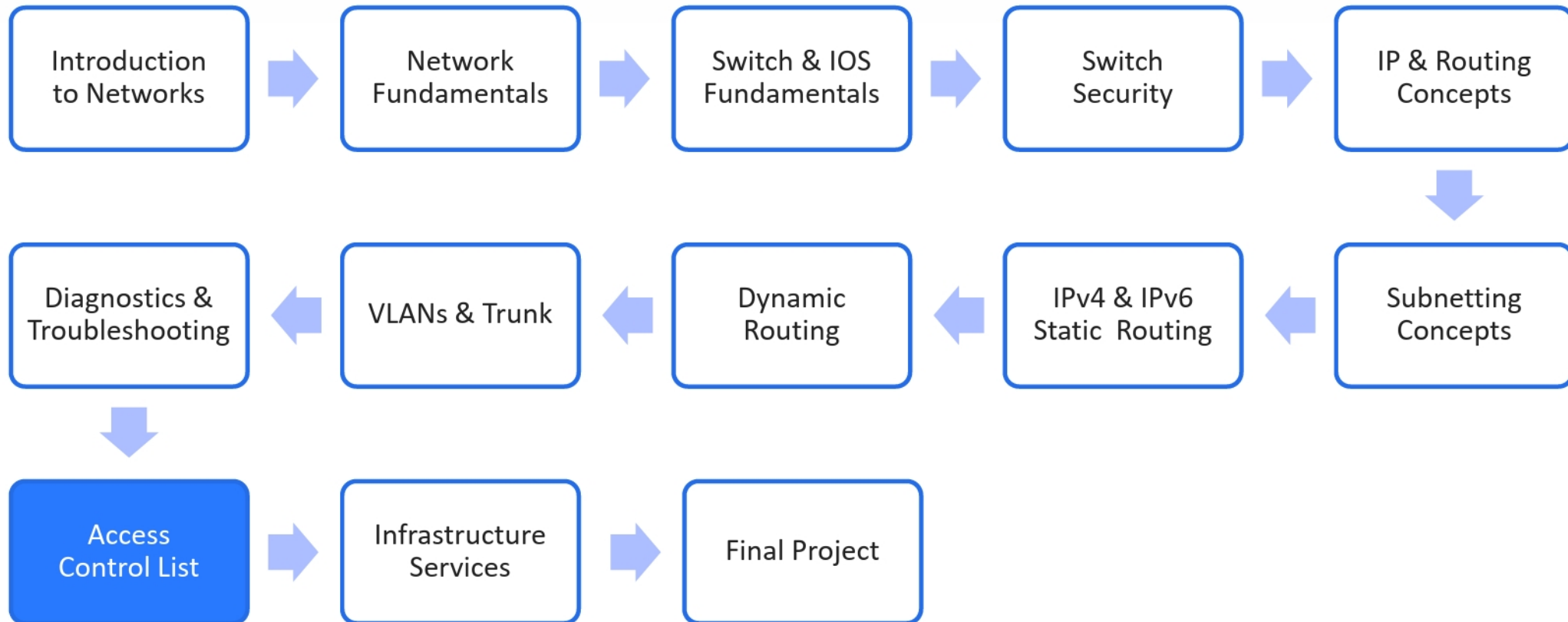


Cybersecurity Professional Program

Access Control List

Computer Networking

Computer Networking Course Path



Overview

Lesson Objective

The object of this lesson is to understand the basic concepts of an Access Control List, and how named and numbered standard ACLs are configured.

The lesson also explains Extended Access Lists.



ACL Overview

Standard ACL Implementation

Extended ACL Implementation

Access Control list

ACL OVERVIEW

Concept: Access Control List

Where it is used



ACL's are used in

- Computer Networks (Firewalls, Switches and Routers)
- Computer File Systems (Servers and Workstation)
- Web Portals (Canvas, Amazon.com)
- Cloud Configurations (Amazon Web Service VPC, Microsoft Azure VNET)



ACL Definition – Computer Networks

What is ACL?



ACL (Access Control List) is a rule-based feature that allows network administrators and engineers to configure basic traffic filtering.

ACL is a series of commands that, based on information in the packet header, determine whether to drop a packet or forward it.



Stateless vs Stateful

Stateless vs Stateful



One device that you place on ACL's are firewalls.

- Stateless firewalls will remember the state of the session and close it once it is completed.
- Stateful firewalls will understand the details of a connection and allow the return traffic.

Most decent firewalls today are stateful.



ACL Advantages

Advantages of configuring an Access List on a device:

Network Performance



Network performance can be improved by allowing only relevant services to communicate with devices across the network.

For example, restricting the network to block video traffic can improve network performance.



Securing the Network



In a network environment, users may be restricted from accessing sensitive services.

ACL provides a basic level of network security by allowing some hosts to access parts of the network, while preventing others from accessing the same parts.



Additional ACL Capabilities

Protocol Restriction



ACLs can also restrict the following:

- Routing protocol advertisement messages
- Packets from security protocols
- Packets from other protocols, such as ICMP



Standard Vs Extended

There are Standard ACLs and Extended ACLs, with the difference in the parameters examined in the process.

Standard ACLs



Standard ACLs examine only the **source IP address** when implementing restrictions. Cisco recommends to place this type of ACL as close to the destination device as possible.



Extended ACLs



Extended ACLs filter packets according to the following parameters: protocol type, source or destination IP address, and source or destination port.

Cisco recommends to place this type of ACL as close to the source as possible.



Traffic Direction

When configuring ACL, traffic direction, inbound or outbound, must be specified on an interface. This is done so that the router will implement the proper restrictions when examining the source network and destination.

Inbound ACL



Configures the ACL for inbound traffic.
The router will examine incoming traffic to the interface.



Outbound ACL



Configures the ACL for outbound traffic.
The router will examine outgoing traffic from the interface.



Wildcards

What are Wildcards?



Wildcards are inverted subnet masks that can be used in statements in both Extended and Standard ACLs.

For example, 255.255.255.0

(binary equivalent = 11111111.11111111.11111111.00000000)

inverts to a wildcard mask of 0.0.0.255

(binary equivalent = 00000000.00000000.00000000.11111111)



ACL Order

The order of statements in an ACL is **crucial**.

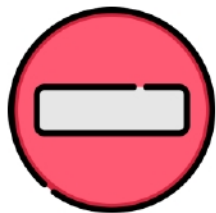
Check Order



ACEs (Access Control Entries), which represent the order of statements in the ACL, are crucial and must be carefully planned. The router checks each packet's parameters against the ACEs to find a matching condition. When a condition is met, the ACL will be applied, and additional ACEs will be ignored.



Implicit Deny



At the end of every ACL, there is an invisible statement called **implicit deny**. When no match is found for a packet, the implicit deny is applied to the packet.

Note: Each ACL must have at least one Permit statement!



Access Control List

STANDARD ACL IMPLEMENTATION

Standard ACL Placement

Where are Standard ACLs Placed?



Standard ACLs are placed as close to the destination as possible. Cisco set this rule because placing standard ACLs at the source of traffic will prevent communication with any network hosting interfaces to which the ACL applies.



Standard ACLs filter traffic only according to the source IP address.

Named Vs Numbered

ACLs can be assigned unique names or numbers.

Standard Named ACL



Standard Named Access Control Lists allow unique names to be assigned to ACLs.



Standard Numbered ACL



Standard Numbered Access Control Lists allow unique numbers to be assigned to ACLs.

The Standard Numbered ACL range includes 1-99 and 1300-1999.



Standard Numbered ACLs

Command

<code>access-list</code>	<code><access-list-number></code>	<code><deny permit remark></code>	<code><source-address></code>	<code><source-wildcard></code>
1	2	3	4	5

</>

1. Beginning syntax to configure a numbered ACL.
2. Decimal number from 1 to 99, or 1300 to 1999 (only for Standard ACLs).
3. Deny - denies access if the conditions match, Permit - permits access if the conditions match, Remark - adds a remark about entries.
4. IP of the network or host from which the packets were sent. You can specify **any** instead of using a 32-bit address.
5. 32-bit wildcard mask that will be applied on the source.

Command Example

```
R1(config)# access-list 10  
permit 192.168.10.0 0.0.0.255
```



Standard ACL Scenario

Scenario #1:

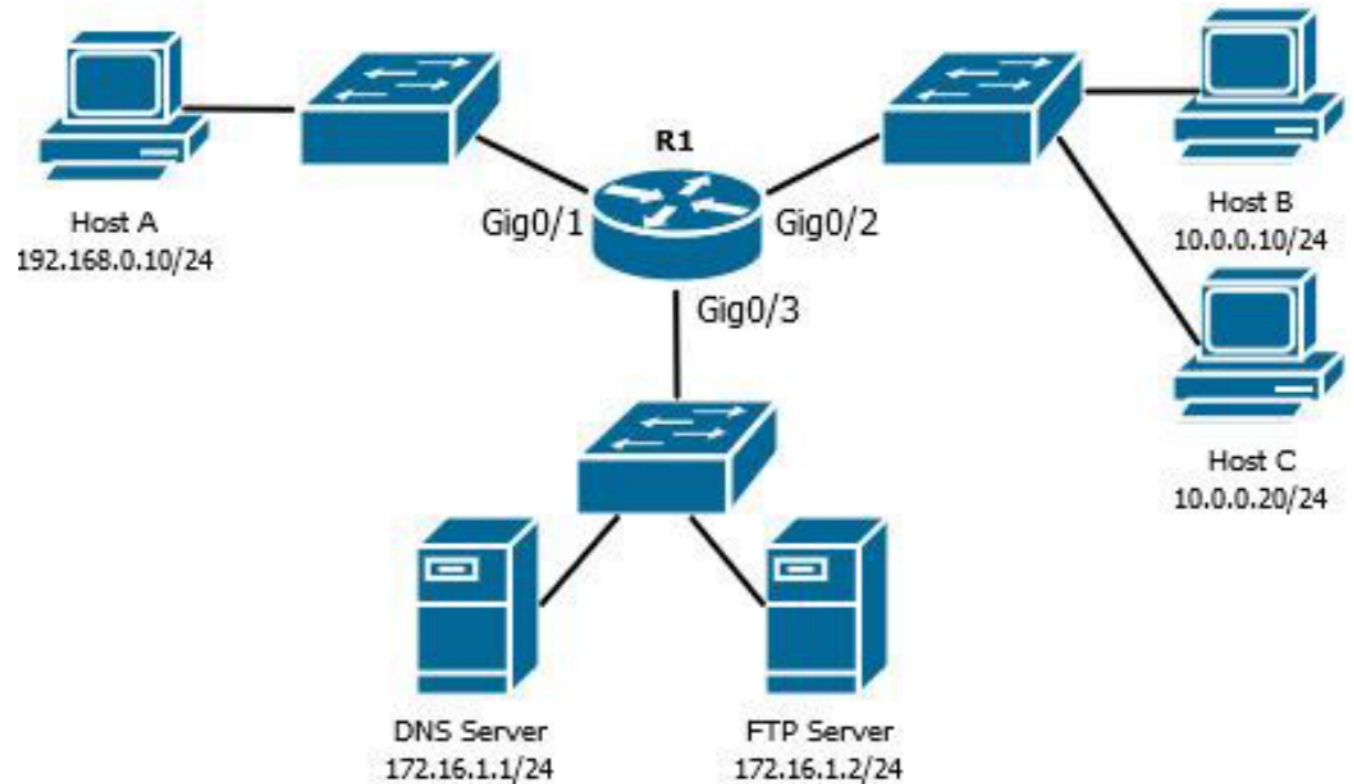
A network administrator decided that new users on network 10.0.0.0/24 will not have access to the server network, but will be able to communicate with neighboring network 192.168.0.0/24

Scenario #2:

After malicious software was discovered on Host A, an administrator decided to temporarily block access from the Host to 10.0.0.0/24, until the threat was removed.

The following slides include ACL configuration examples based on these scenarios.

Network Example



Standard Numbered ACL Config Example

ACL configuration example based on scenario #1.

Step 1 - Create a numbered ACL using the **access-list** command.

Step 2 - Choose the interface for which the ACL will apply, using the **interface** command.

Step 3 - **ip access-group 1 out** command links ACL 1 to the Gigabitethernet 0/3 interface in the outbound direction.

Configure ACL 1 on R1

```
R1(config)#access-list 1 deny 10.0.0.0 0.0.0.255
R1(config)#access-list 1 permit any
R1(config)# interface Gigabitethernet 0/3
R1(config-if)#ip access-group 1 out
R1(config-if)#exit
```

Standard Named ACL Config Example

ACL configuration example based on scenario #2.

Step 1 - Use the **ip access-list standard** command to create a named ACL.

Step 2 - In ACL configuration mode, create Deny and Permit ACE statements.

Step 3 - Apply the ACL on an interface using the **ip access-group** command, and specify the traffic direction (in or out).

Configure ACL Block_Host_A on R1

```
R1(config)# ip access-list standard Block_Host_A
R1(config-std-nacl)#deny host 192.168.0.10
R1(config-std-nacl)#permit any
R1(config-std-nacl)#exit
R1(config)#interface GigabitEthernet 0/2
R1(config-if)#ip access-group Block_Host_A out
R1(config-if)#exit
```

Verify ACL Settings

ACL rules can be verified in different ways, one of which is by searching the running-config file using an include filter.

Run **show running-config** to display on which interface each ACL is applied.

The **show access-list** command can also be used.

Display ACL Settings on R1

```
R2#show access-list
Standard IP access list Block_Host_A
 10 deny host 192.168.0.10
 20 permit any
Standard IP access list 1
 10 deny 10.0.0.0 0.0.0.255
 20 permit any

R1#show running-config
interface GigabitEthernet0/2
 ip address 10.0.0.150 255.255.255.0
 ip access-group Block_Host_A out
!
interface GigabitEthernet0/3
 ip address 172.16.0.150 255.255.255.0
 ip access-group 1 out
```



Lab NET-11-L1

Implement Standard and Extended ACLs
(Tasks 4-6)
30–60 Min.



Mission

The objective of this lab is to plan, configure, and verify standard and extended ACLs.

Steps

- Configure a Numbered Extended ACL.
- Configure a Named Extended ACL (optional).
- Modify an Extended ACL (optional).

Environment & Tools

- OS: All platforms
- Tools: Cisco Packet Tracer 7.2.2, or higher

Related Files

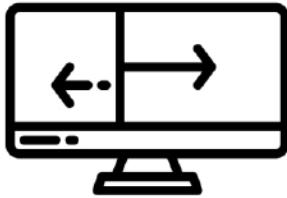
- Lab document
- NET-11-L1.pka

Access Control List

EXTENDED ACL IMPLEMENTATION

Extended ACLs

What are Extended ACLs?



Extended ACLs filter packets based on the following attributes:

- Source and destination IP addresses.
- Source and destination Layer4 protocols (UDP and TCP).
- Protocol type or number. For example: IP, HTTPS, 80, etc.
- Extended ACLs use the following range of numbers: 100 to 199 and 2000 to 2699.



Extended ACL Placement

Where are Extended ACLs Placed?



Configure Extended ACLs as close as possible to the source of the traffic being filtered.

Doing so ensures that traffic will be denied and prevented from traversing the network infrastructure.



It's important to understand that even if the ACL is not placed as close as possible to the source, the ACL will still operate as it should.

Extended Numbered ACLs

Command

<code>access-list</code>	<code><number></code>	<code><action></code>	<code><protocol></code>	<code><source-address></code>	<code><destination-address></code>	<code><operator></code>
1	2	3	4	5	6	



1. Syntax used to configure a numbered ACL.
2. Decimal numbers. Extended ACLs use **100-199** and **2000-2699**.
3. Deny - denies access if the conditions match, Permit - permits access if the conditions match, Remark - adds a remark about entries.
4. The name of the protocol being used: IP, TCP, UDP, ICMP, etc.
5. The source and destination of the network traffic, which can be Host, or a network 32-bit address. The **any** option can be used, and different combinations can also be used.
6. For logical port configuration, the following operators can be used for more control: **lt** (less than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), and **range** (inclusive range).

Command Examples

```
R1(config)#access-list 101  
deny ip host 10.0.0.1 host  
172.16.0.2
```

```
R1(config)#access-list 101  
deny tcp host 10.0.0.2 host  
172.16.0.3 eq 22
```



Extended ACL Examples

Scenario #1:

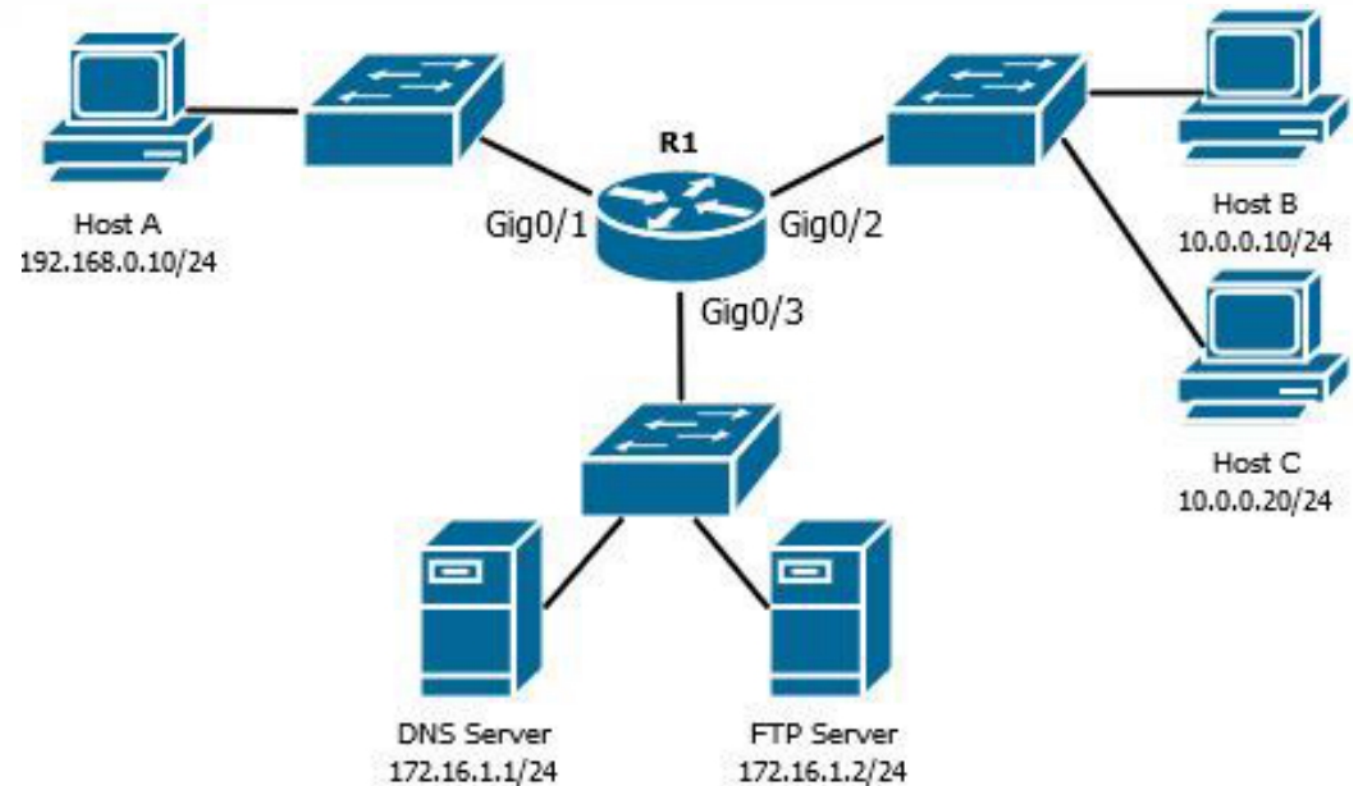
Due to new procedures and changes in the organizational structure, Hosts A and C are not allowed to communicate.

Scenario #2:

The network administrator decided that the enterprise department on network 10.0.0.0/24 cannot access the FTP service on the FTP server, due to the risk of exposing sensitive information. It can however receive services from the same server, such as DHCP.

The following slides include ACL configuration examples based on these scenarios.

Network Example



Extended Numbered ACL Configuration Example

ACL configuration examples
based on scenario #1.

Step 1 - Create a numbered ACL
using the **access-list** command.

Step 2 - Choose the interface for
which the ACL will apply, using
the **interface** command.

Step 3 - **ip access-group 1 in**
command links ACL 1 to the
GigabitEthernet 0/1 interface
in the inbound direction.

Configure ACL 100 on R1

```
R1(config)#access-list 100 deny ip host 192.168.0.10 host 10.0.0.20
R1(config)#access-list 100 permit ip any any
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip access-group 100 in
R1(config-if)#exit
```

Extended Named ACL Configuration Example

ACL configuration examples based on scenario #2.

Step 1 - Use the **ip access-list standard** command to create a named ACL.

Step 2 - In ACL configuration mode, create Deny and Permit ACE statements.

Step 3 - Apply the ACL on an interface using the **ip access-group** command and specify the traffic direction (in or out).

Configure ACL Block_FTP on R1

```
R1(config)#ip access-list extended Block_FTP
R1(config-ext-nacl)#deny tcp 10.0.0.0 0.0.0.255 host 172.16.1.2 eq 21
R1(config-ext-nacl)#deny tcp 10.0.0.0 0.0.0.255 host 172.16.1.2 eq 20
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#interface gigabitEthernet 0/2
R1(config-if)#ip access-group Block_FTP in
R1(config-if)#exit
```

Verify ACL Settings

ACL rules can be verified in various ways, one of which is by searching the running-config file using an include filter.

Run the **show running-config** command can to display on which interface each ACL is applied.

The **show access-list** command can also be used.

Display ACL Settings on R1

```
R2#show access-list
Extended IP access list 100
  10 deny ip host 192.168.0.10 host 10.0.0.20
  20 permit ip any any
Extended IP access list Block_FTP
  10 deny tcp 10.0.0.0 0.0.0.255 host 172.16.1.2 eq 21
  20 deny tcp 10.0.0.0 0.0.0.255 host 172.16.1.2 eq 20
  30 permit ip any any

R1#show running-config
interface GigabitEthernet0/1
  ip address 192.168.0.150 255.255.255.0
  ip access-group 100 in
!
interface GigabitEthernet0/2
  ip address 10.0.0.150 255.255.255.0
  ip access-group Block_FTP in
```



QUESTIONS?



THANK YOU
