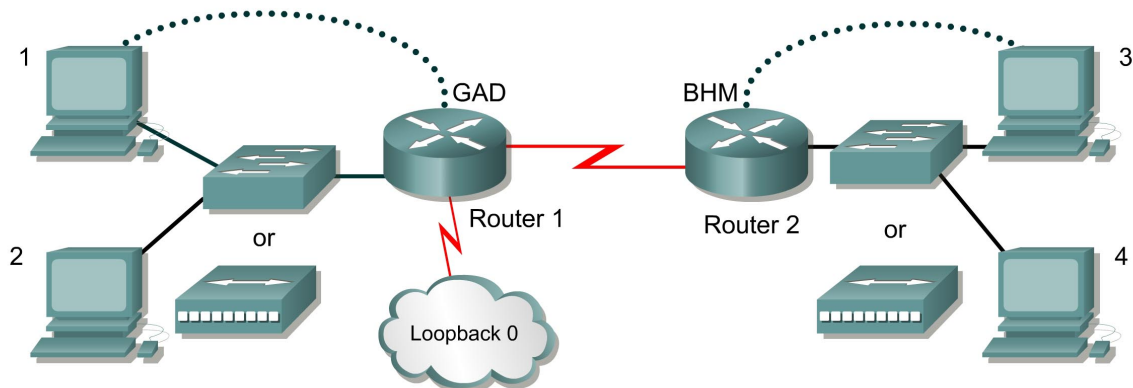


Lab 11.2.1b Standard ACLs – Instructor Version 2500



Straight-through cable	—————
Serial cable	—————
Console (Rollover)	
Crossover cable	-----

Router Name	FA0/0 Address	Interface Type S0/0	S0/0 Address	LO0 Address	Routing	Enable password	VTY password
GAD	192.168.1.1 /24	DCE	192.168.2.1 /24	172.16.1.1 /24	RIP	cisco	class
BHM	192.168.3.1 /24	DTE	192.168.2.2 /24	--	RIP	cisco	class

Host	IP Address	Subnet Mask	Gateway
1	192.168.1.2	255.255.255.0	192.168.1.1
2	192.168.1.3	255.255.255.0	192.168.1.1
3	192.168.3.2	255.255.255.0	192.168.3.1
4	192.168.3.3	255.255.255.0	192.168.3.1

Objective

Plan, configure, and apply a standard ACL to permit or deny specific traffic and test the ACL to determine if the desired results were achieved.

Scenario

The company home office in Gadsden (GAD) provides services to branch offices such as the Birmingham (BHM) office. These offices have some minor security and performance concerns. A Standard ACL needs to be implemented as a simple and effective tool to control traffic

Infrastructure

Host #3 represents the kiosk station that needs to have its access limited to the local network.

Host #4 represents another host in the BHM office and the Loopback 0 interface on the GAD router represents the Internet.

Step 1 Basic Router Interconnection

- a. Interconnect the routers as shown in the diagram.

Step 2 Basic Configuration

- a. The router may contain configurations from a previous use. For this reason, erase the startup configuration and reload the router to remove any residual configurations. Refer to the table on the first page and setup the router and host configurations. Verify reachability by pinging all systems and routers from each system.
- b. To simulate the Internet, add the following configuration to the GAD router.

```
GAD(config)#interface loopback0
GAD(config-if)#address 172.16.1.1 255.255.255.0
GAD(config-if)#exit
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
GAD(config-if)#^z
```

Step 3 Establish Access List Requirements

- a. The kiosk station (host 3) needs to have its access limited to the local network. It is determined that a standard access list needs to be created to prevent traffic from this host from reaching any other networks. The access control list should block traffic from this host and not affect other traffic from this network. A standard IP ACL satisfies this requirement as it filters based on the source address to any destination.

What source address of the kiosk? [192.168.3.2](#)

Step 4 Plan the Access List Requirements

- a. As with any project, the most important part of the process is the planning. First, define the information needed to create the ACL. Remember that statements are added sequentially to an ACL. Therefore, the order of the statements needs to be planned carefully.
- b. It has been determined that this ACL will require 2 logical steps. Each of these steps can be accomplished with one statement each. As a planning tool, a text editor like Notepad can be used to organize the logic and then write the list. In the text editor enter the logic by typing:

```
! stop traffic from host 3

! permit all other traffic
```

- c. From this logic the actual ACL will be written. Using the tables below, document the information for each statement.

stop traffic from host 3			
List #	permit or deny	Source address	Wildcard mask
<u>1</u>	<u>Deny</u>	<u>192.168.3.2</u>	<u>0.0.0.0</u>

permit all other traffic			
List #	permit or deny	Source address	Wildcard mask
<u>1</u>	<u>Permit</u>	<u>0.0.0.0</u>	<u>255.255.255.255</u>

- d. What would be the result of not including a statement to permit all other source addresses?
Every packet going into that interface would be denied due to the implicit deny any any statement.
- e. What would be the result of reversing the order of the 2 statements in the list?
The ACL tests packets in the order in which the ACL was written. Therefore, if the packet is sent past the **permit any any** statement first, the deny statement does not take place.
- f. Why are both statements using the same ACL number?
They are both part of the incoming ACL. And since there are only two ACLs allowed per interface, the statements must be listed with each other in the same ACL.
- g. The final step in the planning process is to determine the best location for the access list and the direction the list should be applied. Examine the internetwork diagram and choose the appropriate interface and direction. Document this in the table below:

Router	Interface	Direction
<u>BHM</u>	<u>E0</u>	<u>in*</u>

Note:* This may also be applied to S0 out to stop traffic to the GAD.

Step 5 Write and Apply the ACL

- a. Using the previously constructed logic and information of the access list, complete the commands in the text editor. The list syntax should look similar to:

```
! stop traffic from host 3
  access-list # deny address wildcard
! permit all other traffic
  access-list # permit address wildcard
```

- b. Add to this text file the configuration statements to apply the list.
 The configuration statements take the form of:

```
interface type #/#
ip access-group # {in, out}
```

- c. Now the text file configuration needs to be applied to the router. Enter the configuration mode on the appropriate router and copy and paste the configuration. Observe the CLI display to ensure no errors were encountered.

Step 6 Verify the ACL

Now that the ACL is completed, the ACL needs to be confirmed and tested.

- a. The first step is to check the list to see if it was configured properly on the router. To check the ACL logic use the `show access-lists` command. Record the output.

```
BHM#show ip access-lists
Standard IP access list 1
    deny 192.168.3.2
    permit any
```

- b. Next, verify that the access list was applied to the proper interface and in the correct direction. To do this examine the interface with the `show ip interface` command. Look at the output from each interface and record the lists applied to the interface.

Interface E0

Outgoing access list is not set

Inbound access list is 1

```
Ethernet0 is up, line protocol is up
Internet address is 192.168.3.1/24
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
Multicast reserved groups joined: 224.0.0.9
Outgoing access list is not set
Inbound access list is 1
<output omitted>
```

- c. Finally, test the functionality of the ACL by trying to send packets from the source host and verify that is to be permitted or denied as appropriate. In this case, ping will be used to test this.

```
[ X ] verify that host 3 CAN ping host 4
[ X ] verify that host 3 CANNOT ping host 1
[ X ] verify that host 3 CANNOT ping host 2
[ X ] verify that host 3 CANNOT ping GAD Fa0/0E0
[ X ] verify that host 3 CANNOT ping GAD LO0
[ X ] verify that host 4 CAN ping host 1
[ X ] verify that host 4 CAN ping host 2
[ X ] verify that host 4 CAN ping GAD Fa0/0E0
[ X ] verify that host 4 CAN ping GAD LO0
```

Step 7 Document the ACL

- a. As a part of all network management, documentation needs to be created. Using the text file created for the configuration, add additional comments. This file should also contain output from the `show access-lists` and the `show ip interface` commands.
- b. The file should be saved with other network documentation. The file naming convention should reflect the function of the file and the date of implementation.

That should complete the ACL project.

```
! This is to stop access from the kiosk and is applied to Fa0 in  
access-list 1 deny 192.168.3.2  
access-list 1 permit any  
interface Ethernet0  
ip access-group 1 in
```

```
! access list applied to stop kiosk traffic  
Ethernet0 is up, line protocol is up  
Internet address is 192.168.3.1/24  
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  
Multicast reserved groups joined: 224.0.0.9  
Outgoing access list is not set  
Inbound access list is 1  
<output omitted>
```

```
BHM#show ip access-lists  
Standard IP access list 1  
deny 192.168.3.2  
permit any
```

- c. Once finished, erase the start-up configuration on routers, remove and store the cables and adapter. Also logoff and turn the router off.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If “class” does not work, ask the instructor for assistance.

Router>**enable**

At the privileged EXEC mode, enter the command **erase startup-config**.

Router#**erase startup-config**

The responding line prompt will be:

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

Press **Enter** to confirm.

The response should be:

Erase of nvram: complete

Now at the privileged EXEC mode, enter the command **reload**.

Router#**reload**

The responding line prompt will be:

System configuration has been modified. Save? [yes/no]:

Type **n** and then press **Enter**.

The responding line prompt will be:

Proceed with reload? [confirm]

Press **Enter** to confirm.

In the first line of the response will be:

Reload requested by console.

After the router has reloaded the line prompt will be:

Would you like to enter the initial configuration dialog? [yes/no]:

Type **n** and then press **Enter**.

The responding line prompt will be:

Press RETURN to get started!

Press **Enter**.

The router is ready for the assigned lab to be performed.

<u>Router Interface Summary</u>					
<u>Router Model</u>	<u>Ethernet Interface #1</u>	<u>Ethernet Interface #2</u>	<u>Serial Interface #1</u>	<u>Serial Interface #2</u>	<u>Interface #5</u>
<u>800 (806)</u>	<u>Ethernet 0 (E0)</u>	<u>Ethernet 1 (E1)</u>			
<u>1600</u>	<u>Ethernet 0 (E0)</u>	<u>Ethernet 1 (E1)</u>	<u>Serial 0 (S0)</u>	<u>Serial 1 (S1)</u>	
<u>1700</u>	<u>FastEthernet 0 (FA0)</u>	<u>FastEthernet 1 (FA1)</u>	<u>Serial 0 (S0)</u>	<u>Serial 1 (S1)</u>	
<u>2500</u>	<u>Ethernet 0 (E0)</u>	<u>Ethernet 1 (E1)</u>	<u>Serial 0 (S0)</u>	<u>Serial 1 (S1)</u>	
<u>2600</u>	<u>FastEthernet 0/0 (FA0/0)</u>	<u>FastEthernet 0/1 (FA0/1)</u>	<u>Serial 0/0 (S0/0)</u>	<u>Serial 0/1 (S0/1)</u>	

In order to find out exactly how the router is configured, look at the interfaces. This will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart does not include any other type of interface even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in IOS command to represent the interface.

--	--	--	--	--	--

BHM#show running-config
Building configuration...

Current configuration:

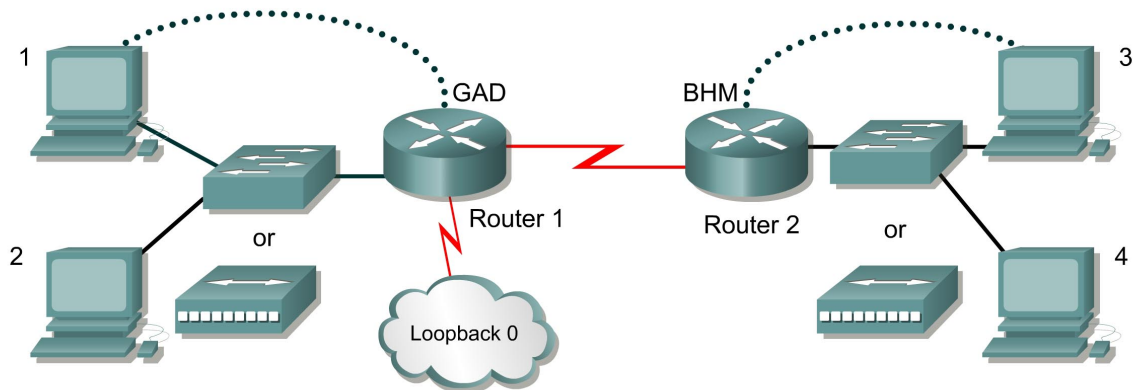
```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname BHM  
!  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
!  
process-max-time 200  
!  
interface Ethernet0  
 ip address 192.168.3.1 255.255.255.0  
 ip access-group 1 in  
 no ip directed-broadcast  
!  
interface Serial0  
 ip address 192.168.2.2 255.255.255.0  
 no ip directed-broadcast  
 no ip mroute-cache  
 no fair-queue  
 clockrate 64000  
!  
interface Serial1  
 no ip address  
 no ip directed-broadcast  
 shutdown  
!  
router rip  
 network 192.168.2.0  
 network 192.168.3.0  
!  
ip classless  
no ip http server  
!  
access-list 1 deny 192.168.3.2  
access-list 1 permit any  
!  
line con 0  
 transport input none  
line aux 0  
line vty 0 4  
!  
no scheduler allocate  
end
```

GAD#show running-config
Building configuration...

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname GAD  
!  
memory-size iomem 10  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
!  
process-max-time 200  
!  
interface Loopback0  
 ip address 172.16.1.1 255.255.255.0  
 no ip directed-broadcast  
!  
interface Ethernet0  
 ip address 192.168.1.1 255.255.255.0  
 no ip directed-broadcast  
!  
interface Serial0  
 ip address 192.168.2.1 255.255.255.0  
 no ip directed-broadcast  
 no ip mroute-cache  
 no fair-queue  
!  
interface Serial1  
 no ip address  
 no ip directed-broadcast  
 shutdown  
!  
router rip  
 network 172.16.0.0  
 network 192.168.1.0  
 network 192.168.2.0  
!  
ip classless  
no ip http server  
!  
!  
line con 0  
 transport input none  
line aux 0  
line vty 0 4  
!  
!  
no scheduler allocate  
end
```

Lab 11.2.1b Standard ACLs – Instructor Version 2600



Straight-through cable	—————
Serial cable	—————
Console (Rollover)	
Crossover cable	-----

Router Name	FA0/0 Address	Interface Type S0/0	S0/0 Address	LO0 Address	Routing	Enable password	VTY password
GAD	192.168.1.1 /24	DCE	192.168.2.1 /24	172.16.1.1 /24	RIP	cisco	class
BHM	192.168.3.1 /24	DTE	192.168.2.2 /24	--	RIP	cisco	class

Host	IP Address	Subnet Mask	Gateway
1	192.168.1.2	255.255.255.0	192.168.1.1
2	192.168.1.3	255.255.255.0	192.168.1.1
3	192.168.3.2	255.255.255.0	192.168.3.1
4	192.168.3.3	255.255.255.0	192.168.3.1

Objective

Plan, configure, and apply a standard ACL to permit or deny specific traffic and test the ACL to determine if the desired results were achieved.

Scenario

The company home office in Gadsden (GAD) provides services to branch offices such as the Birmingham (BHM) office. These offices have some minor security and performance concerns. A Standard ACL needs to be implemented as a simple and effective tool to control traffic

Infrastructure

Host #3 represents the kiosk station that needs to have its access limited to the local network.

Host #4 represents another host in the BHM office and the Loopback 0 interface on the GAD router represents the Internet.

Step 1 Basic Router Interconnection

- a. Interconnect the routers as shown in the diagram.

Step 2 Basic Configuration

- a. The router may contain configurations from a previous use. For this reason, erase the startup configuration and reload the router to remove any residual configurations. Refer to the table on the first page and setup the router and host configurations. Verify reachability by pinging all systems and routers from each system.
- b. To simulate the Internet, add the following configuration to the GAD router.

```
GAD(config)#interface loopback0
GAD(config-if)#address 172.16.1.1 255.255.255.0
GAD(config-if)#exit
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
GAD(config-if)#^z
```

Step 3 Establish Access List Requirements

- a. The kiosk station (host 3) needs to have its access limited to the local network. It is determined that a standard access list needs to be created to prevent traffic from this host from reaching any other networks. The access control list should block traffic from this host and not affect other traffic from this network. A standard IP ACL satisfies this requirement as it filters based on the source address to any destination.

What source address of the kiosk? [192.168.3.2](#)

Step 4 Plan the Access List Requirements

- a. As with any project, the most important part of the process is the planning. First, define the information needed to create the ACL. Remember that statements are added sequentially to an ACL. Therefore, the order of the statements needs to be planned carefully.
- b. It has been determined that this ACL will require 2 logical steps. Each of these steps can be accomplished with one statement each. As a planning tool, a text editor like Notepad can be used to organize the logic and then write the list. In the text editor enter the logic by typing:

```
! stop traffic from host 3

! permit all other traffic
```

- c. From this logic the actual ACL will be written. Using the tables below, document the information for each statement.

stop traffic from host 3			
List #	permit or deny	Source address	Wildcard mask
<u>1</u>	<u>Deny</u>	<u>192.168.3.2</u>	<u>0.0.0.0</u>

permit all other traffic			
List #	permit or deny	Source address	Wildcard mask
<u>1</u>	<u>Permit</u>	<u>0.0.0.0</u>	<u>255.255.255.255</u>

- d. What would be the result of not including a statement to permit all other source addresses?
Every packet going into that interface would be denied due to the implicit deny any any statement.
- e. What would be the result of reversing the order of the 2 statements in the list?
The ACL tests packets in the order in which the ACL was written. Therefore, if the packet is sent past the **permit any any** statement first, the deny statement does not take place.
- f. Why are both statements using the same ACL number?
They are both part of the incoming ACL. Since there are only two ACLs allowed per interface, the statements must be listed with each other in the same ACL.
- g. The final step in the planning process is to determine the best location for the access list and the direction the list should be applied. Examine the internetwork diagram and choose the appropriate interface and direction. Document this in the table below:

Router	Interface	Direction
<u>BHM</u>	<u>FA0/0</u>	<u>in*</u>

Note: * This may also be applied to S0 out to stop traffic to GAD.

Step 5 Write and Apply the ACL

- a. Using the previously constructed logic and information of the access list, complete the commands in the text editor. The list syntax should look similar to:

```
! stop traffic from host 3
  access-list # deny address wildcard
! permit all other traffic
  access-list # permit address wildcard
```

- b. Add to this text file the configuration statements to apply the list.
The configuration statements take the form of:

```
interface type #/#
ip access-group # {in, out}
```

- c. Now the text file configuration needs to be applied to the router. Enter the configuration mode on the appropriate router and copy and paste the configuration. Observe the CLI display to ensure no errors were encountered.

Step 6 Verify the ACL

Now that the ACL is completed, the ACL needs to be confirmed and tested.

- a. The first step is to check the list to see if it was configured properly on the router. To check the ACL logic use the `show access-lists` command. Record the output.

```
BHM#show ip access-lists
Standard IP access list 1
    deny   192.168.3.2
    permit any
```

- b. Next, verify that the access list was applied to the proper interface and in the correct direction. To do this examine the interface with the `show ip interface` command. Look at the output from each interface and record the lists applied to the interface.

Interface FA0/0

Outgoing access list is not set

Inbound access list is 1

```
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24
  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
  Multicast reserved groups joined: 224.0.0.9
  Outgoing access list is not set
  Inbound access list is 1
<output omitted>
```

- c. Finally, test the functionality of the ACL by trying to send packets from the source host and verify that is to be permitted or denied as appropriate. In this case, ping will be used to test this.

```
[ X ] verify that host 3 CAN ping host 4
[ X ] verify that host 3 CANNOT ping host 1
[ X ] verify that host 3 CANNOT ping host 2
[ X ] verify that host 3 CANNOT ping GAD Fa0/0
[ X ] verify that host 3 CANNOT ping GAD LO0
[ X ] verify that host 4 CAN ping host 1
[ X ] verify that host 4 CAN ping host 2
[ X ] verify that host 4 CAN ping GAD Fa0/0
[ X ] verify that host 4 CAN ping GAD LO0
```

Step 7 Document the ACL

- a. As a part of all network management, documentation needs to be created. Using the text file created for the configuration, add additional comments. This file should also contain output from the `show access-lists` and the `show ip interface` commands.
- b. The file should be saved with other network documentation. The file naming convention should reflect the function of the file and the date of implementation.

That should complete the ACL project.

```
! This is to stop access from the kiosk and is applied to Fa0 in  
access-list 1 deny 192.168.3.2  
access-list 1 permit any  
interface FastEthernet0/0  
ip access-group 1 in
```

```
! access list applied to stop kiosk traffic  
FastEthernet0/0 is up, line protocol is up  
Internet address is 192.168.3.1/24  
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  
Multicast reserved groups joined: 224.0.0.9  
Outgoing access list is not set  
Inbound access list is 1  
<output omitted>
```

```
BHM#show ip access-lists  
Standard IP access list 1  
deny 192.168.3.2  
permit any
```

- c. Once finished, erase the start-up configuration on routers, remove and store the cables and adapter. Also logoff and turn the router off.

BHM#show running-config
Building configuration...

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname BHM  
!  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
!  
process-max-time 200  
!  
interface FastEthernet0/0  
 ip address 192.168.3.1 255.255.255.0  
 ip access-group 1 in  
 no ip directed-broadcast  
!  
interface Serial0/0  
 ip address 192.168.2.2 255.255.255.0  
 no ip directed-broadcast  
 no ip mroute-cache  
 no fair-queue  
 clockrate 64000  
!  
interface Serial0/1  
 no ip address  
 no ip directed-broadcast  
 shutdown  
!  
router rip  
 network 192.168.2.0  
 network 192.168.3.0  
!  
ip classless  
no ip http server  
!  
access-list 1 deny 192.168.3.2  
access-list 1 permit any  
!  
line con 0  
 transport input none  
line aux 0  
line vty 0 4  
!  
no scheduler allocate  
end
```

GAD#show running-config
Building configuration...

Current configuration:

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname GAD  
!  
memory-size iomem 10  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
!  
process-max-time 200  
!  
interface Loopback0  
 ip address 172.16.1.1 255.255.255.0  
 no ip directed-broadcast  
!  
interface FastEthernet0/0  
 ip address 192.168.1.1 255.255.255.0  
 no ip directed-broadcast  
!  
interface Serial0/0  
 ip address 192.168.2.1 255.255.255.0  
 no ip directed-broadcast  
 no ip mroute-cache  
 no fair-queue  
!  
interface Serial0/1  
 no ip address  
 no ip directed-broadcast  
 shutdown  
!  
router rip  
 network 172.16.0.0  
 network 192.168.1.0  
 network 192.168.2.0  
!  
ip classless  
no ip http server  
!  
!  
line con 0  
 transport input none  
line aux 0  
line vty 0 4  
!  
!  
no scheduler allocate  
end
```