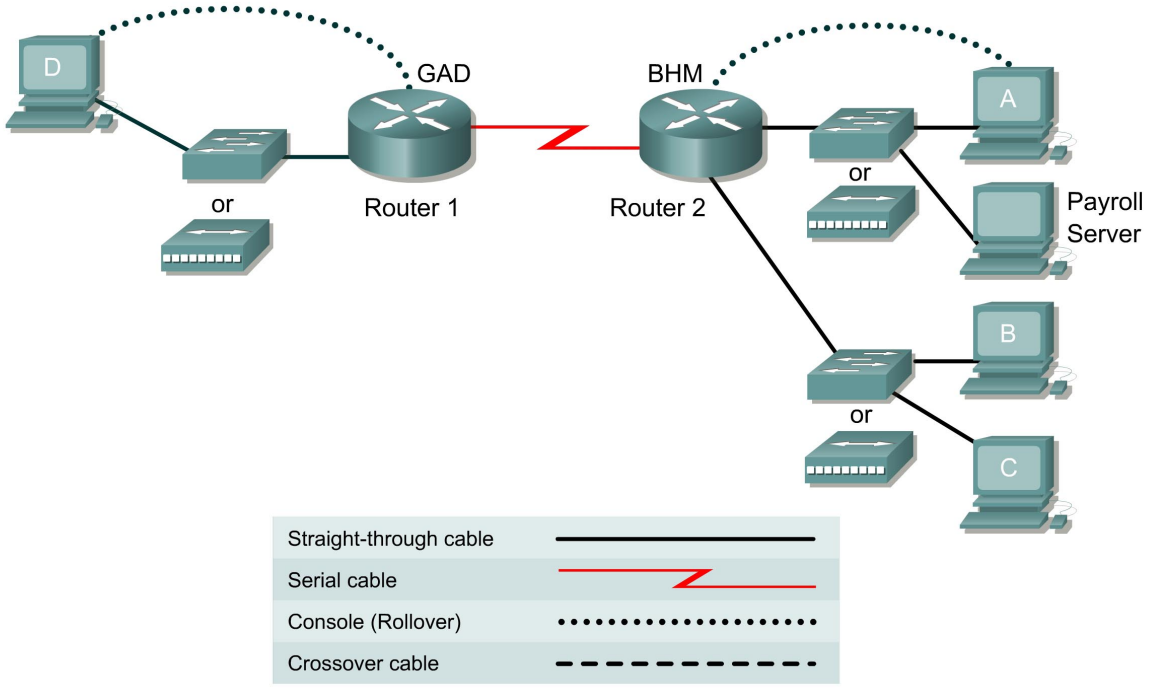
Lab 11.2.2b Simple Extended Access Lists



Router Designation	Router Name	Enable secret password	Enable, VTY and console password	Routing protocol	RIP network statements
Router 1	GAD	class	cisco	RIP	172.16.0.0
Router 2	BHM	class	cisco	RIP	192.168.1.0 172.16.0.0

Router Designation	Fast Ethernet 0 Address	Interface type Serial 0	Serial 0 Address	Fast Ethernet 1 Address	IP host table entries
Router 1	172.16.2.1/24	DTE	172.16.1.1/24		BHM
Router 2	192.168.1.17/28	DCE	172.16.1.2/24	192.168.1.33/28	GAD

Host	IP Address	Subnet Mask	Gateway
Payroll Server	192.168.1.18	255.255.255.240	192.168.1.17
A	192.168.1.19	255.255.255.240	192.168.1.17
B	192.168.1.34	255.255.255.240	192.168.1.33
C	192.168.1.35	255.255.255.240	192.168.1.33
D	172.16.2.2	255.255.255.0	172.16.2.1

Objective

In this lab, configuring extended access lists to filter network to network, host to network, and network to host traffic.

Scenario

A marketing company has two locations. The main site is in Birmingham (BHM) and the branch site is in Gadsden (GAD). The telecommunication administrator for both sites needs to plan and implement access control lists for security and performance. At the Birmingham site, there are two groups of network users. These groups are an Administrative group and a Production group and each are on separate networks. Both networks are interconnected with a router.

The Gadsden site is a stub network and only has a LAN connected to it.

Step 1 Basic Router and Host Configurations

a. Interconnect the routers and hosts as shown in the diagram. Configure all router basics such as hostname, enable password, telnet access, router interfaces. Use the preceding diagram and tables for reference.

Note: The BHM router requires two Ethernet interfaces.

b. The configurations on each router should be as follows:

```
BHM#show running-config

<Output Omitted>

hostname BHM
!
enable secret class
!
interface FastEthernet0/0
 ip address 192.168.1.17 255.255.255.240
!
interface Serial0
 ip address 172.16.1.2 255.255.255.0
 clock rate 56000
!
interface FastEthernet0/1
 ip address 192.168.1.33 255.255.255.240
!
router rip
 network 172.16.0.0
 network 192.168.1.0
!
line vty 0 4
 password cisco
 login
!
end


BHM#
GAD#show running-config

<Output Omitted>

!
hostname GAD
!
enable password class
```



```
!
interface FastEthernet0
 ip address 172.16.2.1 255.255.255.0
!
interface Serial0
 ip address 172.16.1.1 255.255.255.0
!
router rip
 network 172.16.0.0
!
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end

GAD#
```

c. Configure the hosts with the appropriate information using the information previously defined. Before applying any type of access list, it is important to verify reachability between systems.

Verify reachability by pinging all systems and routers from each system.

d. All hosts should be able to ping each other and the router interfaces. If pings to some interfaces are not successful, the problem will need to be located and corrected. Always verify the Physical layer connections, as they seem to be the more common source of connectivity problems. Next, verify the router interfaces. Make sure they are not shutdown, improperly configured, and that RIP is correctly configured. Finally, remember that along with valid IP addresses, hosts must also have default gateways specified.

e. Now that the infrastructure is in place, it is time to begin securing the internetwork.

Step 2 Prevent the Production Users from Accessing the Gadsden Network

a. Company policy specifies that only the Administrative group should have access to the Gadsden site. The Production group should be restricted from accessing that network.

b. Configure an extended access list to allow the Administrative group access to the Gadsden site. The production group should not have access to the Gadsden site.

c. After careful analysis, it is decided that it would be best to use an extended access list and apply it to the outgoing S0 interface on the BHM router.

Note: Remember that when the access list is configured, each statement in the list is processed by the router in the order it was created. It is not possible to reorder an access list, skip statements, edit statements, or delete statements from a numbered access list. For this reason, it may be beneficial to create the access-list in a text editor such as Notepad and then paste the commands to the router, instead of being typed in directly on a router.

d. Enter the following:

```
BHM#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BHM(config)#access-list 100 deny ip 192.168.1.32 0.0.0.15 172.16.2.0
0.0.0.255
```

e. This statement defines an extended access list called “100”. It will deny ip access for any users on the 192.168.1.32 – 192.168.1.47 network if they are trying to access network 172.16.2.0. Although a less specific access list could be defined, this access list could allow the production users to access other sites (if available) through the S0 interface.

f. Remember that there is an implicit deny all at the of every access list. We must now make sure to let the administrative group access the Gadsden network. Although we could be more restrictive, we will simply let any other traffic through. Enter the following statement:

```
BHM(config)#access-list 100 permit ip any any
```

g. Now we need to apply the access list to an interface. We could apply the list to any incoming traffic going to the production network Fa0/1 interface. However, if there were a great deal of traffic between the administrative network and the production network, the router would have to check every packet. There is concern that this would add unwanted overhead to the router. Therefore the access list is applied to the any outgoing traffic going through the BHM router S0 interface.

Enter the following:

```
BHM(config)#interface s0
BHM(config-if)#ip access-group 100 out
```

h. Verify the syntax of the access-list with the **show running-config** command. The following lists the valid statements that should be in the configuration.

```
interface Serial0
 ip access-group 100 out

<Output Omitted>

access-list 100 deny   ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
access-list 100 permit ip any any
```

i. Another valuable command is the **show access-lists** command. The following is a sample output.

```
BHM#show access-lists
Extended IP access list 100
    deny ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
    permit ip any any
```

j. The **show access-lists** command also displays counters, indicating how many times the list has been used. No counters are listed here since we haven't attempted to verify it yet.

Note: Use the **clear access-list counters** command to restart the access list counters

k. Now test the access list by verifying reachability to the Gadsden network by the administrative and production hosts.

Can the production host (B) ping the Gadsden host (D)? No

Can the production host (C) ping the Gadsden host (D)? No

Can the administrative host (A) ping the Gadsden host (D)? Yes

Can the production host (B) ping the administration host (A)? Yes

Can the production host (B) ping the Gadsden router Serial interface? Yes

l. The production hosts (B) and (C) should be able to ping the administrative host (A) and Gadsden router Serial interface. However, they should not be able to ping the Gadsden host (D). The router should return a reply message to the host stating “Destination net unreachable”.

Issue the **show access-lists** command. How many matches are there? 8

Note: The **show access-lists** command displays the number of matches per line. Therefore the number of deny matches may seem odd until it is realized that the pings matched the deny statement and the permit statement.

m. To help understand how the access list is operating, keep periodically issuing the **show access-lists** command.

Step 3 Allow a Production User Access to the Gadsden Network

a. A call is received from a user in the production group (B). They are responsible for exchanging certain files between the production network and the Gadsden network. The extended access list needs to be altered to allow them access to the Gadsden network, while denying everyone else on the production network.

b. Configure an extended access-list to allow that user access to Gadsden.

c. Unfortunately, it is not possible to reorder an access list, skip statements, edit statements, or delete statements from a numbered access list. With numbered access lists, any attempt to delete a single statement results in the entire list’s deletion.

d. Therefore the initial extended access list needs to be deleted and a new one created. To delete access-list 100, enter the following:

```
BHM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BHM(config)#no access-list 100
```

Verify that it has been deleted with the **show access-lists** command.

e. Now create a new extended access list. Always filter from the most specific to the most generic. Therefore the first line of the access list should allow the production host (B) access to the Gadsden network. The remainder of the access-list should be the same as the previous we had entered.

f. To filter the production host (B) the first line of the access list should be as follows:

```
BHM(config)#access-list 100 permit ip host 192.168.1.34 172.16.2.0
0.0.0.255
```

Therefore, the access list permits the production host (B) access to the Gadsden network.

g. Now deny all of the remaining production hosts access to the Gadsden network and permit any on else. Refer to the previous step for the next two lines of the configuration.

The **show access-list** command would display output similar to the following:

```
BHM#show access-lists
Extended IP access list 100
    permit ip host 192.168.1.34 172.16.2.0 0.0.0.255
    deny ip 192.168.1.32 0.0.0.15 172.16.2.0 0.0.0.255
    permit ip any any
BHM#
```

h. Now test the access list by verifying reachability to the Gadsden network by the administrative and production hosts.

Can the production host (B) ping the Gadsden host (D)? Yes

Can the production host (C) ping the Gadsden host (D)? No

The production host (B) should now be able to ping the Gadsden host (D). However, all other production hosts (C) should not be able to ping the Gadsden host (D). Again, the router should return a reply message to the host stating "Destination net unreachable" for host (C).

Step 4 Allow Gadsden Users Access to the Administration Payroll Server

a. The administration group houses the payroll server. Users from the Gadsden site need FTP and HTTP access the payroll server from time to time to upload and download payroll reports.

b. Configure an extended access-list to allow users from the Gadsden site FTP, HTTP access to the payroll server only. It is decided to also allow ICMP access for them to ping the server. Gadsden users should not be able to ping any other host on the Administration network.

c. We do not want unnecessary traffic between the sites therefore it is decided to configure an extended access list on the Gadsden router.

d. Anticipate that privileged EXEC access to GAD will be required occasionally. That is why Telnet access to it is configured. Otherwise travel would be required to the Gadsden site to configure it.

e. Telnet to the Gadsden router from the Birmingham router and enter enable mode. Troubleshoot as necessary.

Note: A common pitfall when configuring access lists on remote routers is to inadvertently "lock yourself" out. This is not a big problem when the router is physically located local. However, this could be a huge problem if the router is physically located in another geographical location.

f. For this reason, it is strongly suggest that the **`reload in 30`** command be issued on the remote router. This would automatically reload the remote router within 30 minutes of issuing the command. Therefore, if the administrator was locked out, it would eventually reload to the previous configuration, allowing access to the router again. Use `the` **`reload cancel`** command to deactivate the pending reload.

g. Configure an extended access list to allow FTP access to the payroll server. The access list statement should be similar to the following:

```
GAD(config)#access-list 110 permit tcp any host 192.168.1.18 eq ftp
```

This line will permit any host from the Gadsden network FTP access to the payroll server at address 192.168.1.18.

What could we have defined instead of using the keyword "any"?

Specific Port Number

What could we have defined instead of using the keyword "host"?

Subnet

What could we have defined instead of using the keyword "ftp"?

Another Service

h. Now configure the next line of the access list to permit HTTP access to the payroll server. The access list statement should be similar to the following:

```
GAD(config)#access-list 110 permit tcp any host 192.168.1.18 eq www
```


This line will permit any host from the Gadsden network FTP access to the payroll server at address 192.168.1.18.

What else could we have defined instead of using the keyword “www”?

Using a wildcard statement

i. Now configure the next line of the access list to permit ICMP access to the payroll server. The access list statement should be similar to the following:

```
GAD(config)#access-list 110 permit icmp any host 192.168.1.18
```

This line will permit any host from the Gadsden network to ping the payroll server at address 192.168.1.18.

j. Finally, no Gadsden user should be able access any other host on the Administration network. Although it is not required, it is always a good idea to include a deny statement. Adding the statement is a good reminder and makes it easier to “read” the access list. The access list statement should be similar to the following:

```
GAD(config)#access-list 110 deny ip any 192.168.1.16 0.0.0.15
```

k. Now we need to apply the access list to an interface. To reduce unwanted WAN traffic, it is decided to apply the access list to the any outgoing traffic going through the Gadsden routers S0 interface.

Enter the following:

```
GAD(config)#interface s0
GAD(config-if)#ip access-group 110 out
```

l. Now test the access list by verifying reachability to the payroll server by a Gadsden host (D).

Can the Gadsden host (D) ping the payroll server? Yes

Can the Gadsden host (D) ping the host (A)? No

The Gadsden host should be able to ping the payroll server only. The router should return the “Destination net unreachable” when it tries to ping the administrative host (D).

Step 5 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.

c. That should complete this extended ACL lab.

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

