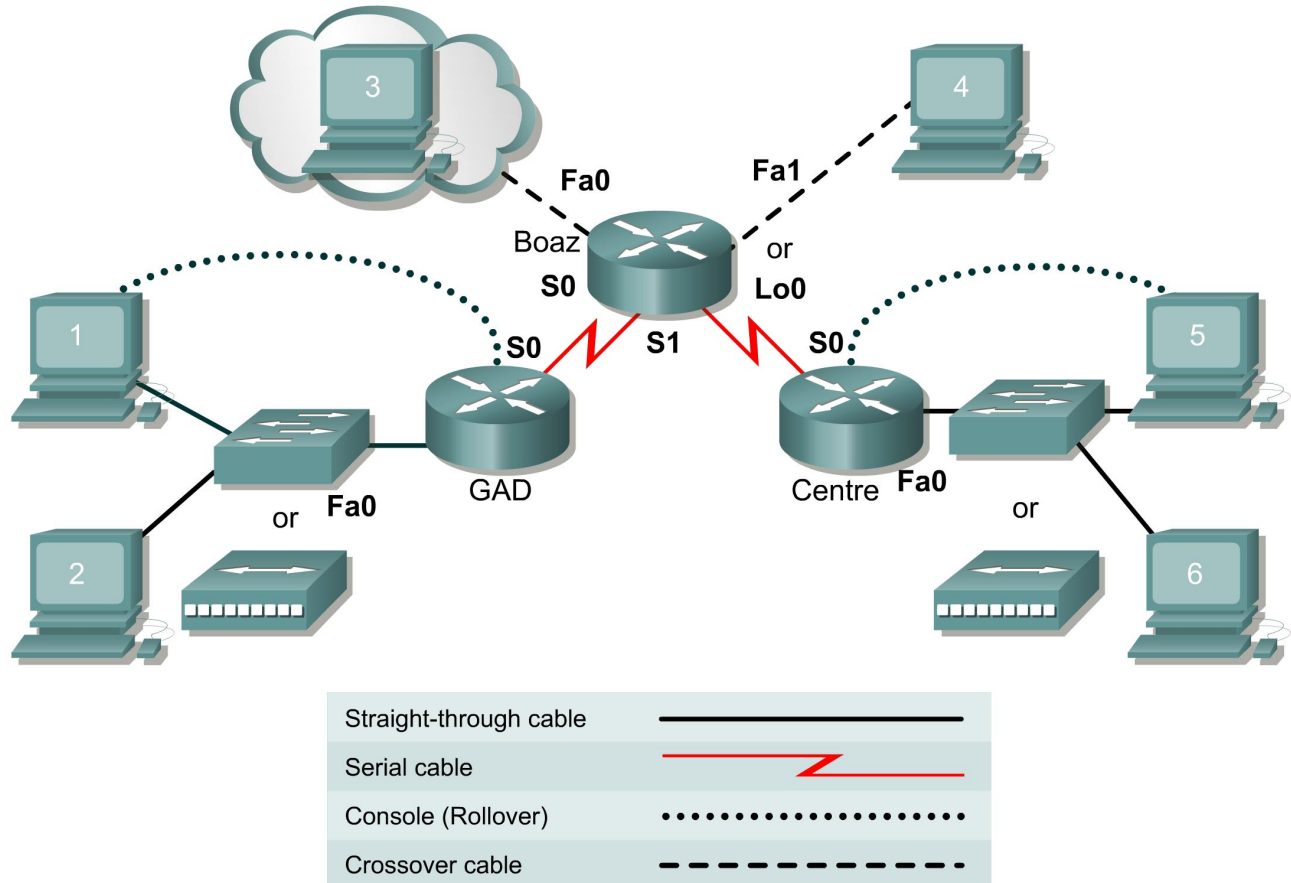




Lab 11.2.3c Multiple Access Lists Functions (Challenge Lab) – Instructor Version 2500



Router Name	Router Type	FA0 Address	FA1 Address	S0 Address	S1 Address	Subnet mask	Routing	Enable password	VTY password
<u>GAD</u>		<u>192.168.1.30</u> <u>/28</u>		<u>192.168.1.45</u> <u>/28</u>		<u>/28</u>	<u>RIP</u>		
<u>Boaz</u>		<u>10.3.3.1 /28</u>	<u>192.168.1.62</u> <u>/28</u>	<u>192.168.1.46</u> <u>/28</u>	<u>192.168.1.77</u> <u>/28</u>	<u>/28</u>	<u>RIP</u>		
<u>Centre</u>		<u>192.168.1.94</u> <u>/28</u>		<u>192.168.1.78</u> <u>/28</u>		<u>/28</u>	<u>RIP</u>		

Host	IP Address	Subnet Mask	Gateway
<u>1</u>	<u>192.168.1.17</u>	<u>255.255.255.240</u>	<u>192.168.1.30</u>
<u>2</u>	<u>192.168.1.21</u>	<u>255.255.255.240</u>	<u>192.168.1.30</u>
<u>3</u>	<u>10.3.3.2</u>	<u>255.255.255.240</u>	<u>10.3.3.1</u>
<u>4</u>	<u>192.168.1.61</u>	<u>255.255.255.240</u>	<u>192.168.1.62</u>
<u>5</u>	<u>192.168.1.81 /28</u>	<u>255.255.255.240</u>	<u>192.168.1.94</u>
<u>6</u>	<u>192.168.1.85 /28</u>	<u>255.255.255.240</u>	<u>192.168.1.94</u>

This lab has MANY different possible solutions. This presents ONE possible solution.

Objective

Configure and apply an extended access control list to control Internet traffic using one or more routers.

Scenario

The company has a regional office, Boaz, that provides services to two branch offices, Gadsden and Centre. These offices each have a branch manager and several people responsible for providing customer services. There has been a significant amount of turnover by the service personnel. After a security audit, it was discovered that there are no network restrictions on the computers used by the service personnel.

The network infrastructure team leader wants a plan created and implemented to enforce network security to prevent access.

Infrastructure

Host #3 represents the Internet. An alternative is to use loopback 0 interface on Boaz and issue the `Boaz(config)#ip http server` command.

Host #4 represents an internal web server that has sensitive personnel and payroll information.

Host #4 will also represent the network administration computer

The lowest 4 host addresses in each subnet are all reserved for the branch managers' computers, hosts 1 and 5.

The router interfaces use highest addresses in the subnets.

The remaining address of the subnet in each branch is to be used for service personnel computers, hosts 2 and 6.

Step 1 Basic Router Interconnection

- Interconnect the routers as shown in the diagram.

Step 2 Internetwork Address Design

- Using a private class C IP address for the internal network, design and document the network. Complete the preceding charts and include the interface type and number, IP address, subnet

mask, and cable type. The “Internet” (cloud) network can be any private space address. Be sure that the address ranges assigned to the routers and hosts meet the criteria described in the infrastructure section above.

Step 3 Basic Router 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. Using the information previously created, setup the router configurations using RIP or IGRP and verify reachability by pinging all systems and routers from each system.

To simulate specific locations on the Internet, add the following configuration to the Boaz router.

```
Boaz (config) #interface loopback 1
Boaz (config-if) #ip address 192.168.255.1 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 2
Boaz (config-if) #ip address 192.168.255.2 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 3
Boaz (config-if) #ip address 192.168.255.3 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 4
Boaz (config-if) #ip address 192.168.255.4 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 5
Boaz (config-if) #ip address 192.168.255.5 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 6
Boaz (config-if) #ip address 192.168.255.6 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 7
Boaz (config-if) #ip address 192.168.255.7 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 8
Boaz (config-if) #ip address 192.168.255.8 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 9
Boaz (config-if) #ip address 192.168.255.9 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 10
Boaz (config-if) #ip address 192.168.255.10 255.255.255.255
Boaz (config-if) #exit
```

Add a network statement to the Boaz routing protocol to advertise this network.

```
Boaz (config-router) #network 192.168.255.0
```

Step 4 Client Configurations

- a. Configure the hosts with the appropriate information using the information previously defined.
[] Verify reachability by pinging all systems and routers from each system.
- b. On hosts 3 and 4 install and configure a Web server such as Tiny Web server.
(<http://www.simtel.net/pub/pd/13103.html>) (Host 3 to represent the Internet. Host 4 to represent internal web server that has sensitive personnel and payroll information.) (Host 4 can be the Loopback of the Boaz router)

- [] Verify that all systems can use a web browser to access the web pages of both the intranet server (host 4) and the Internet server (host 3).
- c. On host 3, install and configure a Telnet server such as TelnetXQ (http://www.datawizard.net/Free_Software/TelnetXQ_Free/telnetxq_free.htm).
 - [] Verify that all systems can Telnet to the Internet (host 3).
- d. Now that the infrastructure is in place, it is time to begin securing the internetwork.

Step 5 Secure the Intranet Server

- a. Host #4 represents an internal web server that has sensitive personnel and payroll information. The information on this server should be accessible ONLY by the branch managers. Access control list(s) should be created to secure this server so that only branch managers' machines have web access (http protocol) to this internal server
 - How many access control lists will be used? Four
 - Where will the access control list(s) will be applied? Loopback 0 on Boaz, the connection to the Internet, and Ethernet 0 at both branch offices.
 - Which direction will the access control list(s) will be applied?
In on Boaz and out at the branch offices.
 - For what reasons might it be better to use multiple access control lists?
Traffic is blocked before it gets to the destination.
 - For what reasons might it be better to use a single access control lists?
All of the internetwork is not under administrative control, therefore, control at the source is more efficient and secure.
- b. Using a text editor, such as Notepad, construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it into the router configuration and apply it to the appropriate interfaces.
- c. Confirm that the ACL is functioning properly:
 - [] Verify reachability by pinging all systems and routers from each system.
 - [] Verify that all computers systems can use a web browser to access the web pages on the Internet (any where except internal web server).
 - [] Verify that the service personnel computers CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server.

Step 6 Secure the Intranet Documents

- a. There is concern that internal policy and procedures documents are being shared outside of the company. To ensure that users in the internetwork cannot forward these documents, do not allow any Telnet or FTP access to the Internet.
 - Should a new ACL, or ACLs, be created or will the current list, or lists, be modified?
Yes, but the branch offices outbound E0 will also be modified.
 - If new list(s):
 - How many new access control lists will be created? One
 - Where will the new access control list(s) will be applied? Interface to the Internet on Boaz
 - Which direction will the new access control list(s) will be applied? Outbound

- b. Again, use a text editor, such as Notepad, to construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it to the router(s) and apply it to the appropriate interfaces.
- c. Confirm that the ACL is functioning properly:
 - [] Verify reachability by pinging all systems and routers from each system.
 - [] Verify that all computers systems can use a web browser to access the web pages on the Internet (any where except internal web server)
 - [] Verify that the service personnel computers CANNOT use a web browser to access (http protocol) the intranet server
 - [] Verify computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server
 - [] Verify that the computers CANNOT telnet to the Internet (host 3 and loopbacks interfaces on Boaz) but can telnet to the routers

Step 7 Deter Internet Abuse

- a. There have also been some complaints that employees have been abusing Internet access. They have been accessing sites with questionable content. To help stop this practice, do not allow any IP traffic from the internetwork to the following sites:

192.168.255.1
 192.168.255.4
 192.168.255.8
 192.168.255.9

Will new access control list(s) be created or will the current list(s) be modified?

If a new condition statement is created that permits or denies traffic, no statements added later will be checked. If additional statements are needed in an existing standard or extended ACL, the ACL must be deleted. Create a new ACL with the new condition statements.

If new list(s):

How many new access control lists will be created?

Access lists need to be removed and re-entered.

Where will the new access control list(s) will be applied?

Interfaces in step 6: Boaz Interface to Internet (Lo0 or E0) and E0 on branch routers.

Which direction will the new access control list(s) will be applied?

Outbound on Boaz, Incoming on branch routers.

- b. Again, use a text editor, such as Notepad, to construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it to the router(s) and apply it to the appropriate interfaces.
- c. Confirm that the ACL is functioning properly:
 - [] Verify service personnel computers CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers CANNOT telnet Internet (host 3 and loopbacks interfaces on Boaz) but can telnet to routers.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.1.

- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.4.
- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.8.
- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.9.
- [] Verify reachability by pinging all other systems and routers from each system.
- [] Verify all computers systems can use a web browser to access the other web pages on the Internet (host 3 and loopbacks interfaces on Boaz).

Step 8 Deter Denial of Service (DoS) Attacks

- a. In the last few weeks the company's internetwork has been the subject to numerous denial of service attacks. Most have taken the form of sending "Ping of Death" (oversized ICMP echo packets) or directed broadcasts (x.x.x.255). To help stop the "Ping of Death" attacks, do not allow any ICMP echo packets into the internetwork. Also to stop the directed broadcast, stop all IP packets from entering the internetwork addressed to the directed broadcast address.

Will new access control list(s) be created or will the current list(s) be modified?

Modify Boaz ACL on the interface connected to the Internet.

If new list(s):

How many new access control lists will be created?

Access lists need to be removed and re-entered.

Where will the new access control list(s) will be applied?

Boaz ACL on the interface connected to the Internet (Lo0 or E0).

Which direction will the new access control list(s) will be applied? Incoming

- b. Again, use a text editor, such as Notepad, to construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it to the router(s) and apply it to the appropriate interfaces.
- c. Confirm that the ACL is functioning properly:
 - [] Verify service personnel computers CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers CANNOT telnet Internet (host 3 and loopbacks interfaces on Boaz) but can telnet to routers.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.1.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.4.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.8.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.9.
 - [] Verify that all computers systems can use a web browser to access the other web pages on the Internet (host 3 and loopbacks other interfaces on Boaz).
 - [] Verify that host 3 CANNOT successfully ping anything in the internetwork.
 - [] Verify that the systems can successfully ping to the other internet hosts.

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

Step 9 Stop Telnet into the Routers

- a. There have also been some attempts to telnet into the routers from both inside and outside the internetwork. The only host that should have telnet access to the routers is the network administration computer. To stop telnet access to the routers create an access control list and apply it to the VTY lines of the routers that will permit only the network administration computer to telnet.

What type of access list will be used? standard

What command will be used to apply the list to the VTY lines? access-class

- b. Use a text editor, such as Notepad, to construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it to the router(s) and apply it to the VTY lines.
- c. Confirm that the ACL is functioning properly:
 - [] Verify that the service personnels' computers CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers CANNOT telnet Internet (host 3 and loopbacks interfaces on Boaz) but can telnet to routers.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.1.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.4.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.8.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.9.
 - [] Verify that all computers systems can use a web browser to access the other web pages on the Internet (host 3 and loopbacks other interfaces on Boaz).
 - [] Verify that host 3 CANNOT successfully ping anything in the internetwork.
 - [] Verify that systems can successfully ping to the other internet hosts.
 - [] Verify that systems can successfully ping host 3.
 - [] Verify that the network administration computer (host 4) can telnet to all of the routers.
 - [] Verify that other internal computers CANNOT telnet to any of the routers.
 - [] Verify that other external computers (host 3) CANNOT telnet to any of the routers.

Step 10 Verify the Access Lists

- a. Now that the access lists have been applied, they need to be verified.

First, verify what lists have been defined. From a CLI session on one of the routers with access lists, display the access lists with the `Boaz#show ip access-lists` command. Record the information about one of the access lists.

```
ip access-list extended 100
remark Apply outbound to Boaz E1 or inbound to the LAN interfaces of
the branch offices
remark permit the branch managers hosts to access internal web server
permit tcp 192.168.1.0 0.0.0.243 host 192.168.1.61 eq www
deny tcp 192.168.1.0 0.0.0.0 host 192.168.1.61 eq www
remark let the rest go
permit ip any any
```

```
ip access-list extended 101
remark apply outbound to Boaz E0 or inbound on all the LAN interfaces
of the branch offices
remark stop worstations from FTP and telnet to the internet
deny tcp 192.168.1.0 0.0.0.255 any eq ftp
deny tcp 192.168.1.0 0.0.0.255 any eq telnet
remark let the rest go
permit ip any any
```

```
ip access-list extended 102
remark apply inbound to Boaz s0 and s1 interfaces
remark deter internet abuse
deny ip any host 192.168.255.1
deny ip any host 192.168.255.4
deny ip any host 192.168.255.8
deny ip any host 192.168.255.9
remark let the rest go
permit ip any any
```

```
ip access-list extended 103
remark apply inbound to Boaz E0
remark do not allow any ICMP echo packets
deny icmp any any echo
remark stop the directed broadcast
deny ip any host 192.168.1.255
remark let the rest go
permit ip any any
```

```
ip access-list standard 1
remark apply to vty lines on all routers
```

```
permit host
192.168.1.61
```

What does the “(# matches)” in the output represent?

The packets that matched a line of an ACL are noted.

- b. Next, confirm which access list is applied to each interface. This is done from the terminal session of one of the routers with access lists, with the Boaz#`show ip interface` command. Look at the output from each interface and record the lists applied to each interface.

Interface E0

Outgoing access list is 101

Inbound access list is 102

Interface Lo0

Outgoing access list is 103

Inbound access list is 104

Interface S0

Outgoing access list is not set

Inbound access list is not set

Interface S1

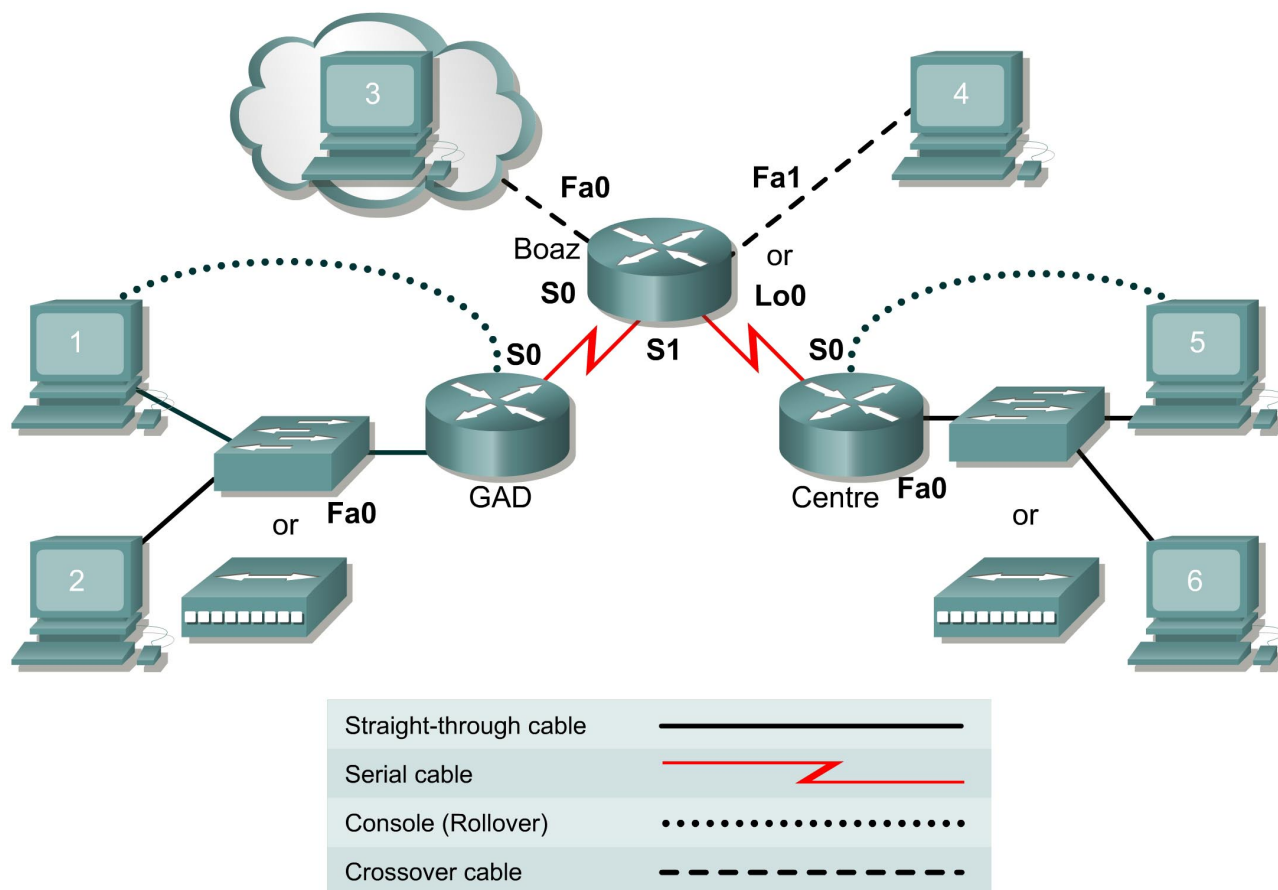
Outgoing access list is not set

Inbound access list is not set

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



Lab 11.2.3c Multiple Access Lists Functions (Challenge Lab) – Instructor Version 2600



Router Name	Router Type	FA0 Address	FA1 Address	S0 Address	S1 Address	Subnet mask	Routing	Enable password	VTY password
<u>GAD</u>		<u>192.168.1.30</u> <u>/28</u>		<u>192.168.1.45</u> <u>/28</u>		<u>/28</u>	<u>RIP</u>		
<u>Boaz</u>		<u>10.3.3.1 /28</u>	<u>192.168.1.62</u> <u>/28</u>	<u>192.168.1.46</u> <u>/28</u>	<u>192.168.1.77</u> <u>/28</u>	<u>/28</u>	<u>RIP</u>		
<u>Centre</u>		<u>192.168.1.94</u> <u>/28</u>		<u>192.168.1.78</u> <u>/28</u>		<u>/28</u>	<u>RIP</u>		

Host	IP Address	Subnet Mask	Gateway
<u>1</u>	<u>192.168.1.17</u>	<u>255.255.255.240</u>	<u>192.168.1.30</u>
<u>2</u>	<u>192.168.1.21</u>	<u>255.255.255.240</u>	<u>192.168.1.30</u>
<u>3</u>	<u>10.3.3.2</u>	<u>255.255.255.240</u>	<u>10.3.3.1</u>
<u>4</u>	<u>192.168.1.61</u>	<u>255.255.255.240</u>	<u>192.168.1.62</u>
<u>5</u>	<u>192.168.1.81 /28</u>	<u>255.255.255.240</u>	<u>192.168.1.94</u>
<u>6</u>	<u>192.168.1.85 /28</u>	<u>255.255.255.240</u>	<u>192.168.1.94</u>

This lab has many different possible solutions. This presents one possible solution.

Objective

Configure and apply an extended access control list to control Internet traffic using one or more routers.

Scenario

The company has a regional office, Boaz, that provides services to two branch offices, Gadsden and Centre. These offices each have a branch manager and several people responsible for providing customer services. There has been a significant amount of turnover by the service personnel. After a security audit, it was discovered that there are no network restrictions on the computers used by the service personnel.

The network infrastructure team leader wants a plan created and implemented to enforce network security to prevent access.

Infrastructure

Host #3 represents the Internet. An alternative is to use loopback 0 interface on Boaz and issue the `Boaz(config)#ip http server` command.

Host #4 represents an internal web server that has sensitive personnel and payroll information.

Host #4 will also represent the network administration computer

The lowest 4 host addresses in each subnet are all reserved for the branch managers' computers, hosts 1 and 5.

The router interfaces use highest addresses in the subnets.

The remaining address of the subnet in each branch is to be used for service personnel computers, hosts 2 and 6.

Step 1 Basic Router Interconnection

- Interconnect the routers as shown in the diagram.

Step 2 Internetwork Address Design

- Using a private class C IP address for the internal network, design and document the network. Complete the preceding charts and include the interface type and number, IP address, subnet mask, and cable type. The "Internet" (cloud) network can be any private space address. Be sure

that the address ranges assigned to the routers and hosts meet the criteria described in the infrastructure section above.

Step 3 Basic Router 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. Using the information previously created, setup the router configurations using RIP or IGRP and verify reachability by pinging all systems and routers from each system.

To simulate specific locations on the Internet, add the following configuration to the Boaz router.

```
Boaz (config) #interface loopback 0/1
Boaz (config-if) #ip address 192.168.255.1 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/2
Boaz (config-if) #ip address 192.168.255.2 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/3
Boaz (config-if) #ip address 192.168.255.3 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/4
Boaz (config-if) #ip address 192.168.255.4 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/5
Boaz (config-if) #ip address 192.168.255.5 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/6
Boaz (config-if) #ip address 192.168.255.6 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/7
Boaz (config-if) #ip address 192.168.255.7 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/8
Boaz (config-if) #ip address 192.168.255.8 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/9
Boaz (config-if) #ip address 192.168.255.9 255.255.255.255
Boaz (config-if) #exit
Boaz (config) #interface loopback 0/10
Boaz (config-if) #ip address 192.168.255.10 255.255.255.255
Boaz (config-if) #exit
```

Add a network statement to the Boaz routing protocol to advertise this network.

```
Boaz (config-router) #network 192.168.255.0
```

Step 4 Client Configurations

- a. Configure the hosts with the appropriate information using the information previously defined.
[] Verify reachability by pinging all systems and routers from each system.
- b. On hosts 3 and 4 install and configure a Web server such as Tiny Web server.
(<http://www.simtel.net/pub/pd/13103.html>) (Host 3 to represent the Internet. Host 4 to represent internal web server that has sensitive personnel and payroll information.) (Host 4 can be the Loopback of the Boaz router)

- [] Verify that all systems can use a web browser to access the web pages of both the intranet server (host 4) and the Internet server (host 3).
- c. On host 3, install and configure a Telnet server such as TelnetXQ (http://www.datawizard.net/Free_Software/TelnetXQ_Free/telnetxq_free.htm).
 - [] Verify that all systems can Telnet to the Internet (host 3).
- d. Now that the infrastructure is in place, it is time to begin securing the internetwork.

Step 5 Secure the Intranet Server

- a. Host #4 represents an internal web server that has sensitive personnel and payroll information. The information on this server should be accessible ONLY by the branch managers. Access control list(s) should be created to secure this server so that only branch managers' machines have web access (http protocol) to this internal server
 - How many access control lists will be used? Four
 - Where will the access control list(s) will be applied? Loopback 0/0 on Boaz, the connection to the Internet, and FastEthernet 0/0 at both branch offices.
 - Which direction will the access control list(s) will be applied?
In on Boaz and out at the branch offices
 - For what reasons might it be better to use multiple access control lists?
Traffic is blocked before it gets to the destination.
 - For what reasons might it be better to use a single access control lists?
All of the internetwork is not under administrative control, therefore, control at the source is more efficient and secure.
- b. Using a text editor, such as Notepad, construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it into the router configuration and apply it to the appropriate interfaces.
- c. Confirm that the ACL is functioning properly:
 - [] Verify reachability by pinging all systems and routers from each system.
 - [] Verify that all computers systems can use a web browser to access the web pages on the Internet (any where except internal web server).
 - [] Verify that the service personnel computers CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server.

Step 6 Secure the Intranet Documents

- a. There is concern that internal policy and procedures documents are being shared outside of the company. To ensure that users in the internetwork cannot forward these documents, do not allow any Telnet or FTP access to the Internet.
 - Should a new ACL, or ACLs, be created or will the current list, or lists, be modified?
Yes, but the branch offices outbound Fa0/0 will also be modified.
 - If new list(s):
 - How many new access control lists will be created? One
 - Where will the new access control list(s) will be applied? Interface to the Internet on Boaz
 - Which direction will the new access control list(s) will be applied? Outbound

- b. Again, use a text editor, such as Notepad, to construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it to the router(s) and apply it to the appropriate interfaces.
- c. Confirm that the ACL is functioning properly:
 - [] Verify reachability by pinging all systems and routers from each system.
 - [] Verify that all computers systems can use a web browser to access the web pages on the Internet (any where except internal web server)
 - [] Verify that the service personnel computers CANNOT use a web browser to access (http protocol) the intranet server
 - [] Verify computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server
 - [] Verify that the computers CANNOT telnet to the Internet (host 3 and loopbacks interfaces on Boaz) but can telnet to the routers

Step 7 Deter Internet Abuse

- a. There have also been some complaints that employees have been abusing Internet access. They have been accessing sites with questionable content. To help stop this practice, do not allow any IP traffic from the internetwork to the following sites:

192.168.255.1
 192.168.255.4
 192.168.255.8
 192.168.255.9

Will new access control list(s) be created or will the current list(s) be modified?

If a new condition statement is created that permits or denies traffic, no statements added later will be checked. If additional statements are needed in an existing standard or extended ACL, the ACL must be deleted. Create a new ACL with the new condition statements.

If new list(s):

How many new access control lists will be created?

Access lists need to be removed and re-entered.

Where will the new access control list(s) will be applied?

Boaz Interface to Internet (Lo0 or E0) and E0 on branch routers.

Which direction will the new access control list(s) will be applied?

Outbound on Boaz, Incoming on branch routers.

- b. Again, use a text editor, such as Notepad, to construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it to the router(s) and apply it to the appropriate interfaces.
- c. Confirm that the ACL is functioning properly:
 - [] Verify service personnel computers CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server.

- [] Verify that the computers CANNOT telnet Internet (host 3 and loopbacks interfaces on Boaz) but can telnet to routers.
- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.1.
- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.4.
- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.8.
- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.9.
- [] Verify reachability by pinging all other systems and routers from each system.
- [] Verify all computers systems can use a web browser to access the other web pages on the Internet (host 3 and loopbacks interfaces on Boaz).

Step 8 Deter Denial of Service (DoS) Attacks

- a. In the last few weeks the company's internetwork has been the subject to numerous denial of service attacks. Most have taken the form of sending "Ping of Death" (oversized ICMP echo packets) or directed broadcasts (x.x.x.255). To help stop the "Ping of Death" attacks, do not allow any ICMP echo packets into the internetwork. Also to stop the directed broadcast, stop all IP packets from entering the internetwork addressed to the directed broadcast address.

Will new access control list(s) be created or will the current list(s) be modified?

Modify Boaz ACL on the interface connected to the Internet.

If new list(s):

How many new access control lists will be created?

Access lists need to be removed and re-
entered.

Where will the new access control list(s) will be applied?

Boaz ACL on the interface connected to the Internet (Lo0 or
E0).

Which direction will the new access control list(s) will be applied?

Incoming

- b. Again, use a text editor, such as Notepad, to construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it to the router(s) and apply it to the appropriate interfaces.
- c. Confirm that the ACL is functioning properly:
 - [] Verify service personnel computers CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers CANNOT telnet Internet (host 3 and loopbacks interfaces on Boaz) but can telnet to routers.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.1.

- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.4.
- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.8.
- [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.9.
- [] Verify that all computers systems can use a web browser to access the other web pages on the Internet (host 3 and loopbacks other interfaces on Boaz).
- [] Verify that host 3 CANNOT successfully ping anything in the internetwork.
- [] Verify that the systems can successfully ping to the other internet hosts.
- [] Verify reachability by pinging all other systems and routers from each system.

Step 9 Stop Telnet into the Routers

- a. There have also been some attempts to telnet into the routers from both inside and outside the internetwork. The only host that should have telnet access to the routers is the network administration computer. To stop telnet access to the routers create an access control list and apply it to the VTY lines of the routers that will permit only the network administration computer to telnet.
 What type of access list will be used? standard
 What command will be used to apply the list to the VTY lines? access-class
- b. Use a text editor, such as Notepad, to construct the logic of the access list(s) and then type the proper commands. When the list is properly constructed, paste it to the router(s) and apply it to the VTY lines.
- c. Confirm that the ACL is functioning properly:
 - [] Verify that the service personnels' computers CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers from the Internet (host 3) CANNOT use a web browser to access (http protocol) the intranet server.
 - [] Verify that the computers CANNOT telnet Internet (host 3 and loopbacks interfaces on Boaz) but can telnet to routers.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.1.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.4.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.8.
 - [] Verify that the computers CANNOT telnet, use a web browser to access, nor ping 192.168.255.9.
 - [] Verify that all computers systems can use a web browser to access the other web pages on the Internet (host 3 and loopbacks other interfaces on Boaz).
 - [] Verify that host 3 CANNOT successfully ping anything in the internetwork.
 - [] Verify that systems can successfully ping to the other internet hosts.
 - [] Verify that systems can successfully ping host 3.
 - [] Verify that the network administration computer (host 4) can telnet to all of the routers.
 - [] Verify that other internal computers CANNOT telnet to any of the routers.

[] Verify that other external computers (host 3) CANNOT telnet to any of the routers.

Step 10 Verify the Access Lists

- a. Now that the access lists have been applied, they need to be verified.

First, verify what lists have been defined. From a CLI session on one of the routers with access lists, display the access lists with the `Boaz#show ip access-lists` command. Record the information about one of the access lists.

```
ip access-list extended 100  
remark Apply outbound to Boaz Fa1 or inbound to the LAN interfaces of  
the branch offices  
remark permit the branch managers hosts to access internal web server  
permit tcp 192.168.1.0 0.0.0.243 host 192.168.1.61 eq www  
deny tcp 192.168.1.0 0.0.0.0 host 192.168.1.61 eq www  
remark let the rest go  
permit ip any any
```

```
ip access-list extended 101  
remark apply outbound to Boaz fa0 or inbound on all the LAN interfaces  
of the branch offices  
remark stop worstations from FTP and telnet to the internet  
deny tcp 192.168.1.0 0.0.0.255 any eq ftp  
deny tcp 192.168.1.0 0.0.0.255 any eq telnet  
remark let the rest go  
permit ip any any
```

```
ip access-list extended 102  
remark apply inbound to Boaz s0 and s1 interfaces  
remark deter internet abuse  
deny ip any host 192.168.255.1  
deny ip any host 192.168.255.4  
deny ip any host 192.168.255.8  
deny ip any host 192.168.255.9  
remark let the rest go  
permit ip any any
```

```
ip access-list extended 103  
remark apply inbound to Boaz fa0  
remark do not allow any ICMP echo packets  
deny icmp any any echo  
remark stop the directed broadcast  
deny ip any host 192.168.1.255  
remark let the rest go  
permit ip any any
```

```
ip access-list standard 1  
remark apply to vty lines on all routers  
permit host 192.168.1.61Extended IP access list 100  
permit ip host 10.0.0.2 172.16.2.0 0.0.0.255 (4 matches)  
deny ip 192.168.1.1 0.0.0.15 172.16.2.0 0.0.0.255 (8 matches)  
deny ip 192.168.1.4 0.0.0.15 172.16.2.0 0.0.0.255 (8 matches)  
deny ip 192.168.1.8 0.0.0.15 172.16.2.0 0.0.0.255 (8 matches)  
deny ip 192.168.1.9 0.0.0.15 172.16.2.0 0.0.0.255 (8 matches)  
permit ip any any (66 matches)
```

What does the “(# matches)” in the output represent?

The packets that matched a line of an ACL are noted.

- b. Next, confirm which access list is applied to each interface. This is done from the terminal session of one of the routers with access lists, with the Boaz#**show ip interface** command. Look at the output from each interface and record the lists applied to each interface.

Interface Fa0/0

Outgoing access list is 101

Inbound access list is 102

Interface Lo0/0

Outgoing access list is 103

Inbound access list is 104

Interface S0/0

Outgoing access list is not set

Inbound access list is not set

Interface S0/1

Outgoing access list is not set

Inbound access list is not set

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