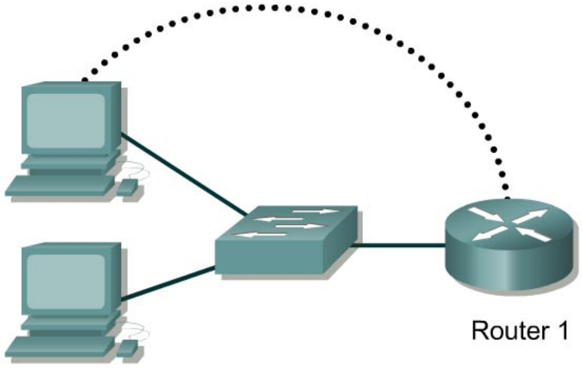
Lab 11.2.2a Configuring Extended Access Lists – Instructor Version 2500



Router Designation	Router Name	FA0/0 Address	Subnet mask	Enable Secret password	Enable/VTY/ Console passwords
Router 1	GAD	192.168.14.1	255.255.255.0	class	cisco

Straight-through cable	────────
Serial cable	────Z────
Console (Rollover)	••••••••••••••••••••
Crossover cable	– – – – – – – – – –

Objective

- Configure, and apply an extended ACL to permit or deny specific traffic.
- Test the ACL to determine if the desired results were achieved.

Background/Preparation

Cable a network similar to the one in the diagram. Any router that meets the interface requirements displayed on the above diagram, such as 800, 1600, 1700, 2500, 2600 routers, or a combination, may be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce a slightly different output. The following steps are intended to be executed on each router unless specifically instructed otherwise.

Start a HyperTerminal session as performed in the Establishing a HyperTerminal session lab.

> **Note:** Go to the erase and reload instructions at the end of this lab. Perform those steps on the router in this lab assignment before continuing.

Step 1 Configure the hostname and passwords on the GAD router

a. On the GAD router, enter the global configuration mode and configure the hostname as shown in the chart. Then configure the console, virtual terminal and enable passwords. Configure the ~~Fast~~Ethernet interface on the router according to the chart.

b. Allow HTTP access by issuing the **`ip http server`** command in global configuration mode.

Step 2 Configure the hosts on the Ethernet segment

a. Host 1

IP address	192.168.14.2
Subnet mask	255.255.255.0
Default gateway	192.168.14.1

b. Host 2

IP address	192.168.14.3
Subnet mask	255.255.255.0
Default gateway	192.168.14.1

Step 3 Save the configuration information from the privileged EXEC command mode

```
GAD#copy running-config startup-config
```

Step 4 Confirm connectivity by pinging the default gateway from both hosts

a. If the pings are not successful, correct the configuration and repeat until they are successful.

Step 5 Connect to the router using the Web browser

a. From a host, connect to the router using a Web browser to ensure that the Web server function is active.

Step 6 Prevent access to HTTP (port 80) from the Ethernet interface hosts

a. Create an access list that will prevent Web browsing access to ~~Fast~~Ethernet 0 from the 192.168.14.0 network.

b. At the router configuration prompt type the following commands:

```
GAD(config)#access-list 101 deny tcp 192.168.14.0 0.0.0.255 any eq 80
GAD(config)#access-list 101 permit ip any any
```

c. Why is the second statement needed?

There is an implicit deny any any at the end of every ACL and no traffic would pass.

Step 7 Apply the access list to the interface

a. At the ~~Fast~~Ethernet 0 interface mode prompt type:

```
GAD(config-if)#ip access-group 101 in
```

Step 8 Ping the router from the hosts

a. Were these pings successful? Yes

b. If they were, why? Because ICMP is not blocked

Step 9 Connect to the router using the web browser

a. Was the browser able to connect? No

Step 10 Telnet to the router from the hosts

a. Were you able to Telnet successfully? Yes

b. Why or why not? Telent uses TCP port 23 not TCP port 80 which is the port that was blocked on the ACL. Therefore, all other IP traffic should be permitted.

Upon completion of the previous steps, logoff by typing **exit**. Turn the router off.

Erasing and reloading the router

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

```
Router>enable
```

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

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.

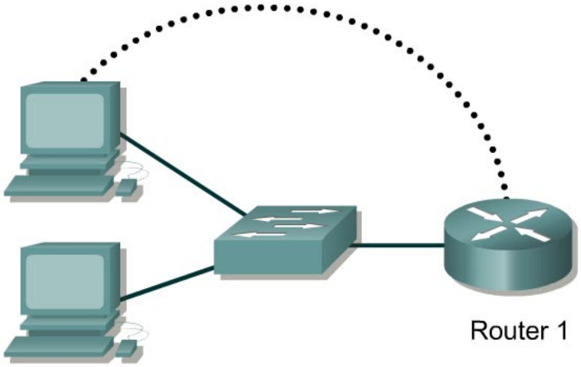
<table>
<tr><th colspan="6">Router Interface Summary</th></tr>
<tr><th>Router Model</th><th>Ethernet Interface #1</th><th>Ethernet Interface #2</th><th>Serial Interface #1</th><th>Serial Interface #2</th><th>Interface #5</th></tr>
<tr><td>800 (806)</td><td>Ethernet 0 (E0)</td><td>Ethernet 1 (E1)</td><td></td><td></td><td></td></tr>
<tr><td>1600</td><td>Ethernet 0 (E0)</td><td>Ethernet 1 (E1)</td><td>Serial 0 (S0)</td><td>Serial 1 (S1)</td><td></td></tr>
<tr><td>1700</td><td>FastEthernet 0 (FA0)</td><td>FastEthernet 1 (FA1)</td><td>Serial 0 (S0)</td><td>Serial 1 (S1)</td><td></td></tr>
<tr><td>2500</td><td>Ethernet 0 (E0)</td><td>Ethernet 1 (E1)</td><td>Serial 0 (S0)</td><td>Serial 1 (S1)</td><td></td></tr>
<tr><td>2600</td><td>FastEthernet 0/0 (FA0/0)</td><td>FastEthernet 0/1 (FA0/1)</td><td>Serial 0/0 (S0/0)</td><td>Serial 0/1 (S0/1)</td><td></td></tr>
<tr><td colspan="6">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.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

```
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
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
!
process-max-time 200
!
interface Ethernet0
 ip address 192.168.14.1 255.255.255.0
 ip access-group 101 in
 no ip directed-broadcast
!
interface Serial0
 ip address 192.168.2.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
ip http server
!
access-list 101 deny   tcp 192.168.14.0 0.0.0.255 any eq www
access-list 101 permit ip any any
!
line con 0
 password cisco
 login
 transport input none
line aux 0
line vty 0 4
password cisco
 login
!
no scheduler allocate
end
```

CISCO NETWORKING ACADEMY PROGRAM

Lab 11.2.2a Configuring Extended Access Lists – Instructor Version 2600



Router Designation	Router Name	FA0/0 Address	Subnet mask	Enable Secret password	Enable/VTY/ Console passwords
Router 1	GAD	192.168.14.1	255.255.255.0	class	cisco

Straight-through cable	————————
Serial cable	————⚡————
Console (Rollover)	••••••••••••••••••••
Crossover cable	– – – – – – – – – – –

Objective

- Configure, and apply an extended ACL to permit or deny specific traffic.
- Test the ACL to determine if the desired results were achieved.

Background/Preparation

Cable a network similar to the one in the diagram. Any router that meets the interface requirements displayed on the above diagram, such as 800, 1600, 1700, 2500, 2600 routers, or a combination, may be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce a slightly different output. The following steps are intended to be executed on each router unless specifically instructed otherwise.

Start a HyperTerminal session as performed in the Establishing a HyperTerminal session lab.

> **Note:** Go to the erase and reload instructions at the end of this lab. Perform those steps on the router in this lab assignment before continuing.

Step 1 Configure the hostname and passwords on the GAD router

a. On the GAD router, enter the global configuration mode and configure the hostname as shown in the chart. Then configure the console, virtual terminal and enable passwords. Configure the FastEthernet interface on the router according to the chart.

b. Allow HTTP access by issuing the **`ip http server`** command in global configuration mode.

Step 2 Configure the hosts on the Ethernet segment

a. Host 1

IP address	192.168.14.2
Subnet mask	255.255.255.0
Default gateway	192.168.14.1

b. Host 2

IP address	192.168.14.3
Subnet mask	255.255.255.0
Default gateway	192.168.14.1

Step 3 Save the configuration information from the privileged EXEC command mode

```
GAD#copy running-config startup-config
```

Step 4 Confirm connectivity by pinging the default gateway from both hosts

a. If the pings are not successful, correct the configuration and repeat until they are successful.

Step 5 Connect to the router using the Web browser

a. From a host, connect to the router using a Web browser to ensure that the Web server function is active.

Step 6 Prevent access to HTTP (port 80) from the Ethernet interface hosts

a. Create an access list that will prevent Web browsing access to FastEthernet 0 from the 192.168.14.0 network.

b. At the router configuration prompt type the following commands:

```
GAD(config)#access-list 101 deny tcp 192.168.14.0 0.0.0.255 any eq 80
GAD(config)#access-list 101 permit ip any any
```

c. Why is the second statement needed? There is an implicit deny any any at the end of every ACL and no traffic would pass.

Step 7 Apply the access list to the interface

a. At the FastEthernet 0 interface mode prompt type:

```
GAD(config-if)#ip access-group 101 in
```

Step 8 Ping the router from the hosts

a. Were these pings successful? Yes

b. If they were, why? Because ICMP is not blocked

Step 9 Connect to the router using the web browser

a. Was the browser able to connect? No

Step 10 Telnet to the router from the hosts

a. Were you able to Telnet successfully? Yes

b. Why or why not? Telent uses TCP port 23 not TCP port 80, which is the port that was blocked on the ACL. Therefore, all other IP traffic should be permitted.

Upon completion of the previous steps, logoff by typing **exit**. Turn the router off.

Erasing and reloading the router

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

```
Router>enable
```

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

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.

<table>
<tr><td colspan="6"><b>Router Interface Summary</b></td></tr>
<tr><td>Router Model</td><td>Ethernet Interface #1</td><td>Ethernet Interface #2</td><td>Serial Interface #1</td><td>Serial Interface #2</td><td>Interface #5</td></tr>
<tr><td>800 (806)</td><td>Ethernet 0 (E0)</td><td>Ethernet 1 (E1)</td><td></td><td></td><td></td></tr>
<tr><td>1600</td><td>Ethernet 0 (E0)</td><td>Ethernet 1 (E1)</td><td>Serial 0 (S0)</td><td>Serial 1 (S1)</td><td></td></tr>
<tr><td>1700</td><td>FastEthernet 0 (FA0)</td><td>FastEthernet 1 (FA1)</td><td>Serial 0 (S0)</td><td>Serial 1 (S1)</td><td></td></tr>
<tr><td>2500</td><td>Ethernet 0 (E0)</td><td>Ethernet 1 (E1)</td><td>Serial 0 (S0)</td><td>Serial 1 (S1)</td><td></td></tr>
<tr><td>2600</td><td>FastEthernet 0/0 (FA0/0)</td><td>FastEthernet 0/1 (FA0/1)</td><td>Serial 0/0 (S0/0)</td><td>Serial 0/1 (S0/1)</td><td></td></tr>
<tr><td colspan="6">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.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

```
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
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
!
process-max-time 200
!
interface FastEthernet0/0
 ip address 192.168.14.1 255.255.255.0
 ip access-group 101 in
 no ip directed-broadcast
!
interface Serial0/0
 ip address 192.168.2.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip classless
ip http server
!
access-list 101 deny   tcp 192.168.14.0 0.0.0.255 any eq www
access-list 101 permit ip any any
!
line con 0
 password cisco
 login
 transport input none
line aux 0
line vty 0 4
password cisco
 login
!
no scheduler allocate
end
```