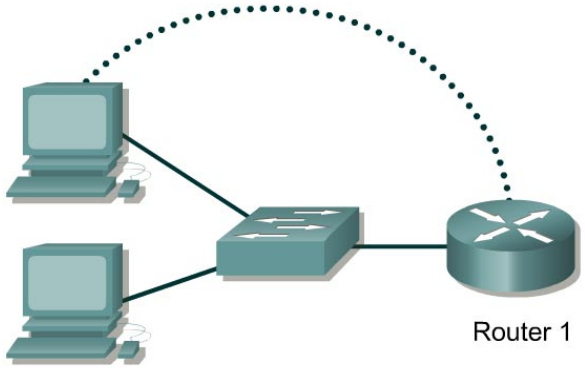
Lab 11.2.3a Configuring a Named Access List – Instructor Version 2500



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	
Console (Rollover)	
Crossover cable	

Objective

- Create a named 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.

 Copyright © 2003, Cisco Systems, Inc.

Step 1 Configure the hostname and passwords on the Gadsden router

a. On the Gadsden 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.

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 Prevent access to the Ethernet interface from the hosts

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

b. At the configuration prompt type the following command:

```
GAD(config)#ip access-list standard no_access
GAD(config-std-nacl)#deny 192.168.14.0 0.0.0.255
GAD(config-std-nacl)#permit any
```

c. Why is the third statement needed? This statement will deny traffic access from all addresses in the 192.168.14.0 network.

Step 6 Ping the router from the hosts

a. Were these pings successful? Yes

b. If they were, why? The ACLs were not applied to the interface yet.

Step 7 Apply the Access list to the interface

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

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

Step 8 Ping the router from the hosts

a. Were these pings successful? No

b. Why or why not? The ACL did not allow the ICMP request.

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

 Copyright © 2003, Cisco Systems, Inc.

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.

 Copyright © 2003, Cisco Systems, Inc.

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

 Copyright © 2003, Cisco Systems, Inc.

```
GAD#show running-config
Building configuration...

Current configuration : 638 bytes
!
version 12.2
!
hostname GAD
!
enable secret 5 $1$rzr7$l9H/aXmOyxeCAiPAUoGLq.
!
ip subnet-zero
!
interface Ethernet0
 ip address 192.168.14.1 255.255.255.0
 ip access-group no_access in
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
ip classless
no ip http server
!
!
ip access-list standard no_access
 deny   192.168.14.0 0.0.0.255
 permit any
!
line con 0
 password cisco
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end

GAD#show ip access-lists
Standard IP access list no_access
    deny   192.168.14.0, wildcard bits 0.0.0.255 (18 matches)
    permit any
```

 Copyright © 2003, Cisco Systems, Inc.

Hosts:

Host 1

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.14.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.14.1
```

Before grouping the access-list to the FA0 interface:

```
C:\>ping 192.168.14.1

Pinging 192.168.14.1 with 32 bytes of data:

Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

After grouping the access-list to the FA0 Interface:

```
C:\>ping 192.168.14.1

Pinging 192.168.14.1 with 32 bytes of data:

Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.

Ping statistics for 192.168.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

 Copyright © 2003, Cisco Systems, Inc.

Host 2

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.14.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.14.1
```

Before grouping the access-list to the E~~FA~~0 interface:

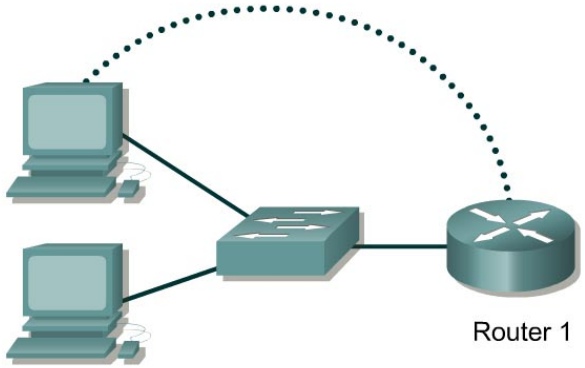
```
C:\>ping 192.168.14.1

Pinging 192.168.14.1 with 32 bytes of data:

Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

After grouping the access-list to the E~~FA~~0 Interface:

```
C:\>ping 192.168.14.1

Pinging 192.168.14.1 with 32 bytes of data:

Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.

Ping statistics for 192.168.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

 Copyright © 2003, Cisco Systems, Inc.

Lab 11.2.3a Configuring a Named Access List – 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

- Create a named 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.

 Copyright © 2003, Cisco Systems, Inc.

Step 1 Configure the hostname and passwords on the Gadsden router

a. On the Gadsden 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.

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 Prevent access to the Ethernet interface from the hosts

a. Create a named access list that will prevent access to FastEthernet 0 from the 192.168.14.0 network.

b. At the configuration prompt type the following command:

```
GAD(config)#ip access-list standard no_access
GAD(config-std-nacl)#deny 192.168.14.0 0.0.0.255
GAD(config-std-nacl)#permit any
```

c. Why is the third statement needed? This statement will deny traffic access from all addresses in the 192.168.14.0 network.

Step 6 Ping the router from the hosts

a. Were these pings successful? Yes

b. If they were, why? The ACLs were not applied to the interface yet.

Step 7 Apply the Access list to the interface

a. At the FastEthernet interface mode prompt type the following:

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

Step 8 Ping the router from the hosts

a. Were these pings successful? No

b. Why or why not? The ACL did not allow the ICMP request.

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

 Copyright © 2003, Cisco Systems, Inc.

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.

 Copyright © 2003, Cisco Systems, Inc.

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

 Copyright © 2003, Cisco Systems, Inc.

```
GAD#show running-config
Building configuration...

Current configuration : 638 bytes
!
version 12.2
!
hostname GAD
!
enable secret 5 $1$rzr7$l9H/aXmOyxeCAiPAUoGLq.
!
ip subnet-zero
!
interface FastEthernet0/0
 ip address 192.168.14.1 255.255.255.0
 ip access-group no_access in
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/1
 no ip address
 shutdown
!
ip classless
no ip http server
!
!
ip access-list standard no_access
 deny   192.168.14.0 0.0.0.255
 permit any
!
line con 0
 password cisco
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end

GAD#show ip access-lists
Standard IP access list no_access
    deny   192.168.14.0, wildcard bits 0.0.0.255 (18 matches)
    permit any
```

 Copyright © 2003, Cisco Systems, Inc.

Hosts:

Host 1

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.14.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.14.1
```

Before grouping the access-list to the FA0 interface:

```
C:\>ping 192.168.14.1

Pinging 192.168.14.1 with 32 bytes of data:

Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

After grouping the access-list to the FA0 Interface:

```
C:\>ping 192.168.14.1

Pinging 192.168.14.1 with 32 bytes of data:

Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.

Ping statistics for 192.168.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

 Copyright © 2003, Cisco Systems, Inc.

Host 2

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.14.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.14.1
```

Before grouping the access-list to the FA0 interface:

```
C:\>ping 192.168.14.1

Pinging 192.168.14.1 with 32 bytes of data:

Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255
Reply from 192.168.14.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

After grouping the access-list to the FA0 Interface:

```
C:\>ping 192.168.14.1

Pinging 192.168.14.1 with 32 bytes of data:

Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.
Reply from 192.168.14.1: Destination net unreachable.

Ping statistics for 192.168.14.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

 Copyright © 2003, Cisco Systems, Inc.