



The purpose of this lab is to practice the syntax and logical sequencing involved with ACLs. It is not intended to require particularly challenging wild card masking. Most of the exercises are mirror images of each other because the lab is intended to be completed by two students working in a team, but each can design ACLs independently if desired.

Lab Setup

Cable the labs as shown in the diagram above. Ensure the routers are erased and then paste in the pre-made configurations found in p:\instructor files\spring 04 ACL. Log into the local lab account on the workstations and ensure they are set with correct IP information. Before proceeding with the lab, from the workstation command prompt, ping every router interface on both routers to ensure complete connectivity and proper configuration.

Why is it important to ensure connectivity before placing ACLs?

Standard ACLs

- Write and apply a standard ACL to that denies network 172.16.0.0 access to network 11.1.0.0.
- Write and apply a standard ACL to that denies network 172.30.0.0 access to network 10.1.0.0.

Assuming the ACLs are designed and placed properly, what behavior do you expect?

How should you test the ACLs to ensure they are working properly?

- Once you have verified the ACLs are working correctly, remove them both and re-write them to deny only the specific host addresses of the workstations in the respective networks. Apply and test the new ACLs. (hint: to properly test these, you will have to change the IP addresses on the workstations at some point.) Remove them both once they are verified.

Extended ACLs

- Write and apply an extended ACL that will permit Host B to ping only 11.1.0.1/24. Test the ACL and remove it once it is verified.
- Write and apply an extended ACL that will permit Host A to ping only 10.1.0.1/24. Test the ACL and remove it once it is verified.
- Write and apply an extended ACL that denies Host B telnet access to WEST, permits http access to EAST only through EAST's Serial interface, denies all access to the entire 172.30.0.0 network except for Host A, and permits anything else anywhere else. Apply, test, and remove this ACL before you apply and test the one listed directly below. The http portion of the ACL can be tested by opening a web browser and typing the IP address of the router into the search bar. If access is granted, the web interface of the router will display in the browser. Note: The router web interface is deactivated by default. The lab configurations enabled it for this lab.
- Write and apply an extended ACL that denies Host A telnet access to EAST, permits http access to WEST only through WEST's Serial interface, denies all access to the entire 172.16.0.0 network except for Host B, and permits anything else anywhere else.

Named ACLs

- Named ACLs are neat, but they will not work with some router applications. If students want practice with named ACL syntax, they can redo one of the above exercises as named ACLs instead of numbered ACLs.

Telnet Security

- Design and apply an ACL on each router that will lock down the telnet lines such that only Host A can telnet into EAST and only Host B can telnet into WEST.

```
!Config for ACL Lab Spring 04
!East router
!Written by Shannon Thomas
!14APR04
!Written for 2500 series routers
!will need to be modified for 1700 or 2600
```

```
enable
config t
hostname EAST
```

```
enable secret cisco
ip http server
Banner motd #
*****
EAST ROUTER
*****
#
line con 0
pass cisco
login
logging synch
line vty 0 4
pass cisco
login
logging synch

!create a logical interface to have more networks
!to test with ACLS
int lo0
ip add 11.1.0.1 255.255.255.0
no shut

!configure LAN default gateway
!on 1700 change line to "f0"
!on 2600 change line to "f0/0"
int e0
ip add 172.30.0.1 255.255.255.0
no shut

!configure wan link
!on 2600 change line to "s0/0"
int s0
ip add 192.168.1.2 255.255.255.0
clockrate 56000
no shut

!configure routing
router rip
network 192.168.1.0
network 172.30.0.0
network 10.200.0.0

end

write mem
!Config for ACL Lab Spring 04
```

```
!West router
!Written by Shannon Thomas
!14APR04
!Written for 2500 series routers
!will need to be modified for 1700 or 2600

enable
config t
hostname WEST
enable secret cisco
ip http server
Banner motd #
*****
WEST ROUTER
*****
#
line con 0
pass cisco
login
logging synch
line vty 0 4
pass cisco
login
logging synch

!create a logical interface to have more networks
!to test with ACLS
int lo0
ip add 10.1.0.1 255.255.255.0
no shut

!configure LAN default gateway
!on 1700 change line to "f0"
!on 2600 change line to "f0/0"
int e0
ip add 172.16.0.1 255.255.255.0
no shut

!configure wan link
!on 2600 change line to "s0/0"
int s0
ip add 192.168.1.1 255.255.255.0
clockrate 56000
no shut

!configure routing
```

```
router rip
network 192.168.1.0
network 172.16.0.0
network 11.1.0.0
```

```
end
```

```
copy run start
startup-config
```