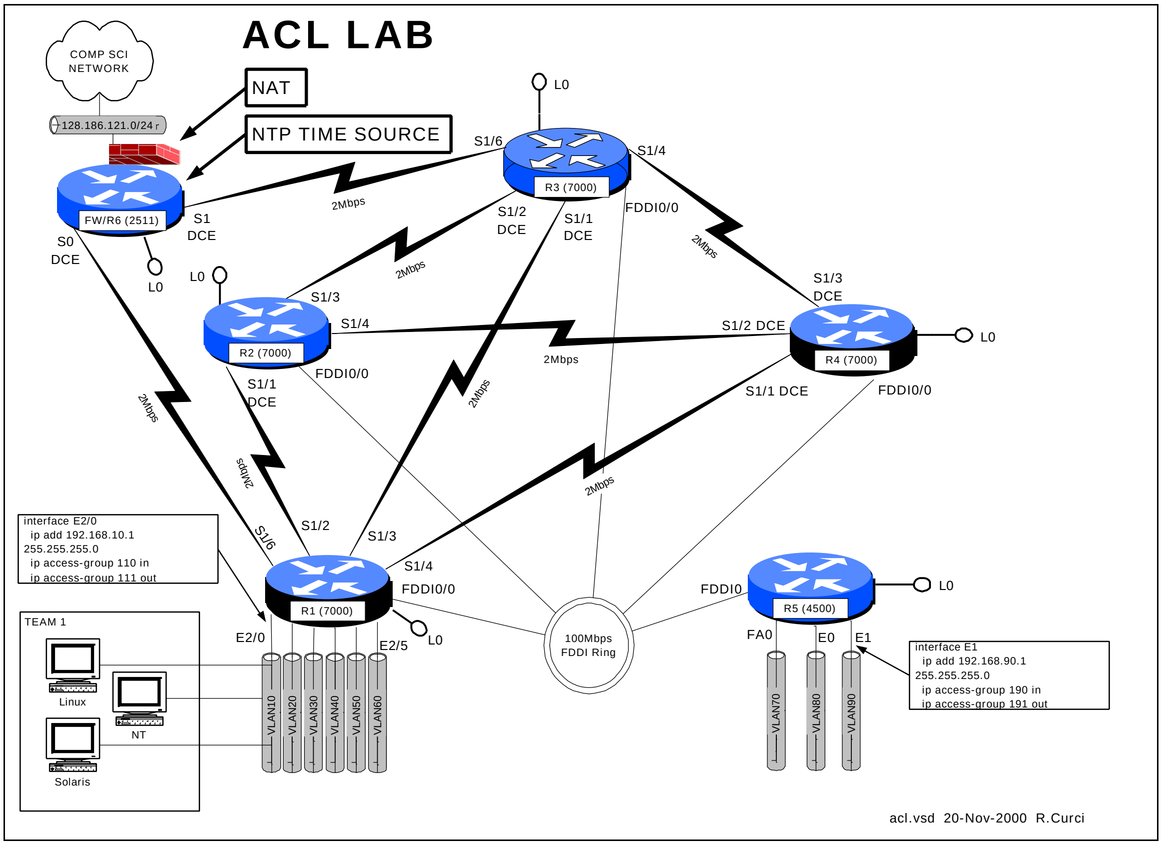
INTERNET TEACHING LAB: ACL LAB



```
interface E2/0
  ip add 192.168.10.1
255.255.255.0
  ip access-group 110 in
  ip access-group 111 out
```

```
interface E1
  ip add 192.168.90.1
255.255.255.0
  ip access-group 190 in
  ip access-group 191 out
```

acl.vsd 20-Nov-2000 R.Curci

Overview

Access Control Lists (ACLs) can be used to selectively block IP traffic to provide a rudimentary firewall. In this lab, you will be using Cisco extended IP access lists to secure your network.

PART1 – PC Setup

Linux and Solaris:

Configure your Linux system so that syslog messages received on facility “local7” should be logged to file /var/log/cisco.log at all severity levels including “debug”. You will need to create the log file, modify /etc/syslog.conf. By default, the syslog will not accept messages from the network which requires an optional flag when invoked. See the ‘man syslogd’ for more information. You will need to modify /etc/rc.d/init.d/syslog to include this flag when the daemon is invoked. You may find it useful to have a Linux window open to follow the log file with “linux# tail –f /var/log/syslog.log”.

Download and install NTP version 3 on your UNIX systems. Configure ntpd to use the R6 loopback0 port (192.168.66.6) as your time source. You can find the software at http://www.eecis.udel.edu/~ntp/.

Download and install Sendmail version 8 on your UNIX systems. Configure so that you can send e-mail between your two UNIX systems. You can find the latest software at http://www.sendmail.org.

Download and install the Apache web server. Configure a sample default web page. You can find the software at http://www.apache.org.

Download and install SSH client and server. You can find this at http://SL.us.fsu.edu or http://www.ssh.com.

NT 4.0 Server:

Install the Internet Information Server (IIS) version 4. If not already loaded, you will first need to install IIS version 2 from the NT 4.0 Server distribution CD-ROM. Afterwards, update the IIS server to version 4.0 using the Windows NT 4.0 Option Pack CD-ROM. Afterwards, be sure to reinstall the latest service pack (6a as of this writing). Create a sample default web page and verify you can access it from a web browser on another system.

Download and install an SSH client. You can find this at http://SL.us.fsu.edu or http://www.ssh.com.

PART2 – Baseline Configuration

Begin with the following baseline router configuration. You should be able to copy and paste the common configuration and router specific configuration into your router's configuration as appropriate.

```
COMMON:
service udp-small-servers
service tcp-small-servers
enable password cisco
no ip domain-lookup
no ip classless
logging buffered
snmp-server community public RO
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password cisco
 login

R1:
hostname r1
interface Loopback0
 ip address 192.168.11.1 255.255.255.0
 no shutdown
interface Fddi0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface Serial1/2
 description Link to R2 S1/1
 ip address 192.168.12.1 255.255.255.0
 bandwidth 2000
 no shutdown
interface Serial1/3
 description Link to R3 S1/1
 ip address 192.168.13.1 255.255.255.0
 bandwidth 2000
 no shutdown
interface Serial1/4
 description Link to R4 S1/1
 ip address 192.168.14.1 255.255.255.0
 bandwidth 2000
 no shutdown
```

```
interface Serial1/6
 description Link to R6 S0
 ip address 192.168.16.1 255.255.255.0
 bandwidth 2000
 no shutdown
interface E2/0
 description Vlan 10 to cat1 FA0/1
 ip address 192.168.10.1 255.255.255.0
 no shutdown
interface E2/1
 description Vlan 20 to cat1 FA0/2
 ip address 192.168.20.1 255.255.255.0
 no shutdown
interface E2/2
 description Vlan 30 to cat1 FA0/3
 ip address 192.168.30.1 255.255.255.0
 no shutdown
interface E2/3
 description Vlan 40 to cat1 FA0/4
 ip address 192.168.40.1 255.255.255.0
 no shutdown
interface E2/4
 description Vlan 50 to cat1 FA0/5
 ip address 192.168.50.1 255.255.255.0
 no shutdown
interface E2/5
 description Vlan 60 to cat1 FA0/6
 ip address 192.168.60.1 255.255.255.0
 no shutdown
router rip
 network 192.168.11.0
 network 192.168.12.0
 network 192.168.13.0
 network 192.168.14.0
 network 192.168.16.0
 network 192.168.1.0
 network 192.168.10.0
 network 192.168.20.0
 network 192.168.30.0
 network 192.168.40.0
 network 192.168.50.0
 network 192.168.60.0
```

R2:

```
hostname r2
interface Loopback0
 ip address 192.168.22.2 255.255.255.0
 no shutdown
interface Fddi0/0
 ip address 192.168.1.2 255.255.255.0
 no shutdown
interface Serial1/1
 description Link to R1 S1/2
 ip address 192.168.12.2 255.255.255.0
 bandwidth 2000
 clockrate 2000000
 no shutdown
interface Serial1/3
 description Link to R3 S1/2
 ip address 192.168.23.2 255.255.255.0
 bandwidth 2000
 no shutdown
interface Serial1/4
 description Link to R4 S1/2
 ip address 192.168.24.2 255.255.255.0
 bandwidth 2000
 no shutdown
router rip
 network 192.168.12.0
 network 192.168.22.0
 network 192.168.23.0
 network 192.168.24.0
 network 192.168.1.0
```

R3:

```
hostname r3
interface Loopback0
 ip address 192.168.33.3 255.255.255.0
 no shutdown
interface Fddi0/0
 ip address 192.168.1.3 255.255.255.0
 no shutdown
interface Serial1/0
 description Link to self
 no ip address
 bandwidth 2000
 no shutdown
interface Serial1/1
 description Link to R1 S1/3
 ip address 192.168.13.3 255.255.255.0
 bandwidth 2000
 clockrate 2000000
 no shutdown
interface Serial1/2
 description Link to R2 S1/3
 ip address 192.168.23.3 255.255.255.0
 bandwidth 2000
 clockrate 2000000
 no shutdown
interface Serial1/3
 description Link to self
 no ip address
 bandwidth 2000
 clockrate 2000000
 no shutdown
interface Serial1/4
 description Link to R4 S1/3
 ip address 192.168.34.3 255.255.255.0
 bandwidth 2000
 no shutdown
interface Serial1/6
 description Link to R6 S1
 ip address 192.168.36.3 255.255.255.0
 bandwidth 2000
 no shutdown
router rip
 network 192.168.33.0
 network 192.168.13.0
 network 192.168.23.0
 network 192.168.34.0
 network 192.168.36.0
 network 192.168.1.0
```

R4:

```
hostname r4
interface Loopback0
 ip address 192.168.44.4 255.255.255.0
 no shutdown
interface Fddi0/0
 description Link to R5 FDDI0
 ip address 192.168.1.4 255.255.255.0
 no shutdown
interface Serial1/1
 description Link to R1 S1/4
 ip address 192.168.14.4 255.255.255.0
 bandwidth 2000
 clockrate 2000000
 no shutdown
interface Serial1/2
 description Link to R2 S1/4
 ip address 192.168.24.4 255.255.255.0
 bandwidth 2000
 clockrate 2000000
 no shutdown
interface Serial1/3
 description Link to R3 S1/4
 ip address 192.168.34.4 255.255.255.0
 bandwidth 2000
 clockrate 2000000
 no shutdown
router rip
 network 192.168.44.0
 network 192.168.14.0
 network 192.168.24.0
 network 192.168.34.0
 network 192.168.1.0
```

R5:

```
hostname r5
interface loopback0
 ip address 192.168.55.5 255.255.255.0
 no shutdown
interface FastEthernet0
 description Vlan70 to cat1 FA0/7
 ip address 192.168.70.1 255.255.255.0
 media-type 100BaseX
 no shutdown
interface Ethernet0
 description Vlan80 to cat1 FA0/8
 ip address 192.168.80.1 255.255.255.0
 media-type 10BaseT
 no shutdown
interface Ethernet1
 description Vlan90 to cat1 FA0/9
 ip address 192.168.90.1 255.255.255.0
 media-type 10BaseT
 no shutdown
interface Fddi0
 description Link to R4 FDDI0/0
 ip address 192.168.1.5 255.255.255.0
 no keepalive
 no shutdown
router rip
 network 192.168.55.0
 network 192.168.70.0
 network 192.168.80.0
 network 192.168.90.0
 network 192.168.1.0
```

PART3 – NTP and SYSLOG

Configure your router to sync its clock using the network time protocol with the clock on router r6/fw. Use the r6 loopback0 address, 192.168.66.6. Use “show ntp association” and “show ntp status” to test. Configure your router for the appropriate timezone and daylight savings time with the “clock” configuration command. We are in the Eastern time zone which is –5 hours different than UTC/GMT and use EDT in the summer. Use the “show clock” command to verify you have it working correctly.

Now that you have an accurate clock, configure the router so that log messages and debug messages will prepend the local date, time, and timezone using the “service timestamp” configuration command.

Configure your router to generate SYSLOG messages to your Linux syslog server. Use the default “local7” facility and log all messages including those with severity level debug. You will need the “logging” and “logging trap” configuration commands. Verify your router settings with “show log”. Once you have it configured, turn on some debug messages such as “debug ntp packets” and verify you see the messages on your Linux syslog file /var/log/cisco.log. Remember to turn off debugging with “undebug all”.

PART4 – Access Control Lists

Extended IP access lists numbered between 100 through 199. Your team’s VLAN should connect to a router Ethernet or fast Ethernet port. Create two extended IP access lists and apply one to your ethernet port input and other to your ethernet port output as follows:

```
interface [ethernetX|fastethernetX]
  ip access-group XXX in
  ip access-group YYY out
```

Where XXX = (100 + 10 x TEAM) and YYY = (101 + 10 x TEAM):

TEAM	INPUT ACL	OUTPUT ACL
1	110	111
2	120	121
3	130	131
4	140	141
5	150	151
6	160	161
7	170	171
8	180	181
9	190	191

(The terms Input and Output are relative to your router's ethernet port. The terms "host" and "server" are synonymous in this context.)
Create two IP extended access lists for the input and output of your gateway router's ethernet interface to your team VLAN and apply to your ethernet or fast ethernet port with the following security policy:

Security Policy:

- Hosts on your VLAN should generally be able to access services outside your VLAN provided the services are not outside the FSU network. (FSU networks 128.186.0.0/16, 146.201.0.0/16, and 144.174.0.0/16 and RFC1918 private address space 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 should be permitted).
- Do not allow any spoofed packets into your VLAN.
- Allow all NETBIOS over TCP/IP traffic.
- Allow all DNS, NTP, TFTP, SNMP, SYSLOG, and RIP v1 datagrams. (Do not worry about SNMP traps or DNS zone transfers).
- Allow TCP DISCARD and TTCP/IPERF packets for testing.
- Allow all ICMP packets for testing.
- Allow all shell (ssh), and web (www/http) access to hosts on your VLAN (Do not worry about secure http).
- Allow e-mail access (smtp,pop3,imap) to only your Linux server.
- Allow TELNET access to your servers if sourced from a trusted group's VLAN. All even groups only trust each other. All odd groups only trust each other.
- Disallow any other TELNET access from unauthorized IP addresses
- Deny everything else.

- All disallowed traffic must be logged to your Linux host using syslog on file /var/log/cisco.log

You can find out TCP/IP port number assignments from the Internet Assigned Numbers Authority, http://www.isi.edu/in-notes/iana/assignments/port-numbers. The relevant assignments are also included in the table below.

service	**protocol**	**port**	**description**
discard	tcp	9	Bit Bucket/Discard Protocol for Testing
ssh	tcp	22	SSH Remote Login Protocol
telnet	tcp	23	Telnet
smtp	tcp	25	Simple Mail Transfer Protocol
dns	udp	53	Domain Name Server
tftp	udp	69	Trivial File Transfer Protocol
http/www	tcp	80	HyperText Transport Protocol (WWW)
pop3	tcp	110	Post Office Protocol version 3
ntp	udp	123	Network Time Protocol
netbios-ns	tcp	137	NETBIOS Name Service
netbios-ns	udp	137	NETBIOS Name Service
netbios-dgm	tcp	138	NETBIOS Datagram Service
netbios-dgm	udp	138	NETBIOS Datagram Service
netbios-ssn	tcp	139	NETBIOS Session Service
netbios-ssn	udp	139	NETBIOS Session Service
imap4	tcp	143	Internet Message Access Protocol
snmp	udp	161	Simple Network Management Protocol
syslog	udp	514	System Log Messages
rip	udp	520	Routing Information Protocol
ttcp/iperf	tcp	5001	Test TCP / IPERF Testing Protocol

Example of how to apply an access list to an ethernet interface and converting the policy into a detailed intermediate form before coding the access lists:

```
interface ethernet0
   ip address 192.168.10.1 255.255.255.0
   ip access-group 110 in
   ip access-group 111 out
```

Input access list 110:

1. Allow all traffic, provided the destination is in RFC1918 private address space or one of FSU’s three class B addresses:
   a. 192.168.0.0/16
   b. 172.16.0.0/12
   c. 10.0.0.0/8
   d. 128.186.0.0/16

    e. 146.201.0.0/16
    f. 144.174.0.0/16

2. Deny everything else and log it.

Output access list 111:

1. Allow all established TCP connections
2. Deny forged packets with IP source address on your VLAN and log it.
3. Allow all Microsoft NetBIOS name, datagram, and session traffic (137/udp, 138/udp, 139/udp, 137/tcp, 138/tcp, 139/tcp).
4. Allow all DNS,NTP,TFTP,SNMP,SYSLOG, and RIP datagrams (53/udp, 123/udp, 69/udp, 161/udp, 514/udp, 520/udp).
5. Allow TCP DISCARD and TTCP/IPERF packets (9/tcp, 5001/tcp).
6. Allow all ICMP packets.
7. Allow all TCP SSH and WWW to our VLAN. (22/tcp, 80/tcp)
8. Allow SMTP, POP3, and IMAP only to our Linux server (25/tcp, 110/tcp, 143/tcp).
9. Allow all TELNET (23/tcp) access from trusted VLAN IP addresses.
10. Deny all other (23/tcp) TELNET and log it.
11. Deny everything else and log it.

PART5 – Verification

Verify that your access lists are working. The following are some examples of tests that can be performed on the routers and Linux PC for partly testing out your access lists.

PING packets use ICMP protocol and should work from your PC to an FSU destination, but fail to an outside destination:

```
[curci@s1 curci]$ ping www.cnn.com.
PING cnn.com (207.25.71.24) from 192.168.10.2 : 56(84) bytes of data.
From 192.168.10.1: Packet filtered
From 192.168.10.1: Packet filtered
. . .
--- cnn.com ping statistics ---
5 packets transmitted, 0 packets received, +5 errors, 100% packet loss

[curci@s1 curci]$ ping nu.cs.fsu.edu
PING nu.cs.fsu.edu (128.186.121.10) from 192.168.10.2 : 56(84) bytes of
data.
64 bytes from nu  (128.186.121.10):icmp_seq=0 ttl=253 time=4.6 ms
64 bytes from nu  (128.186.121.10):icmp_seq=1 ttl=253 time=4.3 ms
64 bytes from nu  (128.186.121.10): icmp_seq=2 ttl=253 time=4.2 ms
--- nu.cs.fsu.edu ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 4.2/4.3/4.6 ms
[curci@s1 curci]$
```

Ping should also work from outside your Vlan from r6 to your Linux server:

```
fw/r6#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/12 ms
fw/r6#
```

Test NTP protocol by syncing Linux server clock to ntp server on r6 loopback address 192.168.66.6 using the ntpdate utility:

```
[root@s1 curci]# /usr/sbin/ntpdate -v 192.168.66.6
22 Nov 23:23:33 ntpdate[1826]: ntpdate 3-5.93e Fri Feb 18
                              18:55:19 EST 2000 (1)
22 Nov 23:23:33 ntpdate[1826]: adjust time server 192.168.66.6
                               offset 0.001193 sec
```

Test SNMP protocol by fetching the system.sysName.0 MIB variable from r6:

```
[root@s1 curci]# snmpget -v 1 192.168.66.6 public system.sysName.0
system.sysName.0 = fw/r6
```

Test DNS datagram traffic by fetching the SOA record for domain cs.fsu.edu from nu.cs.fsu.edu:

```
[root@s1 curci]# nslookup
> lserver nu.cs.fsu.edu.
Default Server:  nu.cs.fsu.edu
Address:  128.186.121.10

> set type=SOA
> cs.fsu.edu.

fsu.edu
        origin = dns1.fsu.edu
        mail addr = hostmaster.acns.fsu.edu
        serial = 2000112203
        refresh = 3600 (1H)
        retry   = 1200 (20M)
        expire  = 604800 (1W)
        minimum ttl = 86400 (1D)
>
```

From Linux PC, test iperf client using discard TCP port 9 on r6:

```
[root@s1 curci]# iperf -c 192.168.66.6 -p 9
------------------------------------------------------------
Client connecting to 192.168.66.6, TCP port 9
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.10.2 port 2690 connected with 192.168.66.6 port 9
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.3 sec   1.5 MBytes   1.1 Mbits/sec
[root@s1 curci]#
```

From the Linux PC, test access to an outside FSU web page http://www.cs.fsu.edu/~curci:

```
[root@s1 curci]# telnet www.cs.fsu.edu 80
Trying 128.186.121.41...
Connected to xi.cs.fsu.edu.
Escape character is '^]'.
GET /~curci/

<html>
<head><title>Ray Curci Home Page</title></head>
<body>Ray Curci Home Page   16-Nov-2000</p>
I am presently working on an MS degree in the FSU Computer
Network and Systems Administration track.
</body></html>
Connection closed by foreign host.
[root@s1 curci]#
```

Your team VLAN should connect to an ethernet port on either r1 or r5. If you go to r1 or r5, whichever does not connect to your VLAN, you can execute TELNET sourced from a trusted and untrusted group to verify the access list. For example, I am on team 1 served from router r1 interface ethernet 2/0, and my Linux server is at IP address 192.168.10.2. (Vlan10). If try to telnet to my Linux PC from r5 and source from team 8's untrusted ethernet port Ethernet0 it should fail, but work if sourced from team 9's trusted ethernet port Ethernet1, it should work and I will see the login prompt:

```
(Sourced from r5 Ethernet0, ip address 192.168.80.1 (untrusted))
r5#telnet 192.168.10.2 /source-interface Ethernet0
Trying 192.168.10.2 ...
% Destination unreachable; gateway or host down

(Sourced from r5 Ethernet1, ip address 192.168.90.1 (trusted))
r5#telnet 192.168.10.2 /source-interface Ethernet1
Trying 192.168.10.2 ... Open

Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.14-5.0 on an i586
login:
```

My my Linux syslog server in logfile /var/log/cisco.log, the denied telnet attempt from 192.168.80.1 appears. There are four fields in this message (1) time/date stamp prepended by the Linux syslogd program, (2) IP address of device that sent the message, r1's ethernet 2/0 port, prepended by Linux syslogd, (3) time/date stamp prepended by router r1, and (4) the log message itself indicating a denied TCP packet from 192.168.80.1 port 11000 to 192.168.10.2 port 23 (telnet port):

```
Nov 22 23:43:54 192.168.10.1 63: Nov 22 23:43:53 EST:
  %SEC-6-IPACCESSLOGP: list 111 denied
  tcp 192.168.80.1(11000) -> 192.168.10.2(23), 1 packet
```

From outside, I should be able to access the WWW server on my Linux system (192.168.10.2) or NT system at 192.168.10.3:

```
fw/r6#telnet 192.168.10.2 80
Trying 192.168.10.2, 80 ... Open
GET /
<html><head><title>S1 Sample WWW Page</title></head><body>
```

```
<h1>S1 Sample WWW Page</h1>
<hr>This is a test WWW page on server S1 Linux Redhat 6.2 Server
<hr></body></html>
[Connection to 192.168.10.2 closed by foreign host]

fw/r6#telnet 192.168.10.3 80
Trying 192.168.10.3, 80 ... Open
GET /
<html><head><title>S2 Sample WWW Page</title></head>
<body><h1>S2 Sample WWW Page</h1><hr>
This is a test WWW page on server S2 Windows NT 4.0 Server
<hr></body></html>
[Connection to 192.168.10.3 closed by foreign host]
fw/r6#
```

From outside on r6, I should be able to access my Linux system 192.168.10.2 with SMTP e-mail:

```
fw/r6#telnet 192.168.10.2 25
Trying 192.168.10.2, 25 ... Open
220 s1.egghead.net ESMTP Sendmail 8.9.3/8.9.3; Wed, 22 Nov 2000 23:50:05
-0500
quit
221 s1.egghead.net closing connection
[Connection to 192.168.10.2 closed by foreign host]
```

Here is an excerpt from “show access-list 111”. Note that some lines have been matched and the number of matches are displayed:

```
r1# show access-list 111
. . .
    permit udp any eq domain any (79 matches)
    permit udp any any eq ntp (8 matches)
. . .
```