Troubleshooting Standard IPV4 ACLs

CIT 167

Chaz Davis

BCTC
Spring 2020

March 25, 2020

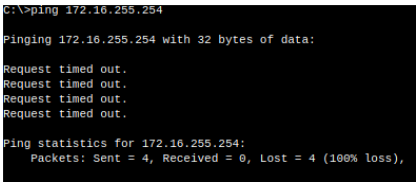
Part 1: Troubleshoot ACL Issue 1

i) Determine ACL problem

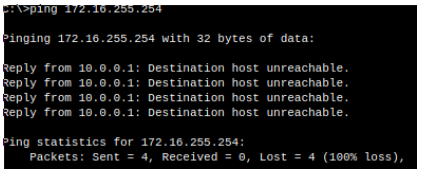
I realized that the Switches were misconfigured and had to reconnect them to the correct interfaces on the routers.

Now, the first step is to check if LAN1 is denied access to LAN2, so from L1 I will ping Server2. The successful output of that is in Fig. 1a on Pg. 1.

We are also told that Lan3 should have access to Lan2, so from L3 I will ping Server2. The ping was blocked by the router ,see Fig. 1b on Pg. 1. Which means that Lan1 has access to Lan2 and Lan3 is blocked from Lan3.



(a) L1 Pinging Server2



(b) L3 Pinging Server2

Figure 1: Assessing the Network configs for DENY-LAN1 on R1

ii) Implement a Solution

I logged into R1, I looked up the access tables, I went to `int g0/1` and ran `no ip access-group DENY-LAN1 out`. I then reconfigured DENY-LAN1 to say `20 permit any any` that way it would allow all other addresses. I then went to `int g0/1` and typed in `ip access-group DENY-LAN1 in`. See Fig. 2 on Pg. 2 for outputs.

iii) Verify that the problem is resolved and document the solution

I Verified the network connections by running a ping from L1 to Server2(Fig. 3a), and again from L3 to Server2(Fig. 3b).

```
R1>en
R1#show access-lists
Standard IP access list DENY-LAN1
    10 deny 10.0.0.0 0.255.255.255
    20 deny any
Standard IP access list DENY-L2
    10 permit any
    20 deny host 172.16.0.2
Standard IP access list PERMIT-L3
    10 permit host 192.168.0.2
```

(a) Configuring the ACL DENY-LAN1

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard DENY-LAN1
R1(config-std-nacl)#no 20
R1(config-std-nacl)#20 permit any
R1(config-std-nacl)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show access-lists
Standard IP access list DENY-LAN1
    10 deny 10.0.0.0 0.255.255.255
    20 permit any
Standard IP access list DENY-L2
    10 permit any
    20 deny host 172.16.0.2
Standard IP access list PERMIT-L3
    10 permit host 192.168.0.2

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1
R1(config-if)#ip access-group DENY-LAN1 in
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

(b) Output of the Access-lists

```
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 172.16.0.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is DENY-LAN1
  Proxy ARP is enabled
```

(c) G0/1 Configured with DENY-LAN1

Figure 2: Configuring the ACL for R1 DENY-LAN1

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(a) L1 Ping to Server2

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.

Ping statistics for 172.16.255.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(b) L3 Ping to Server2

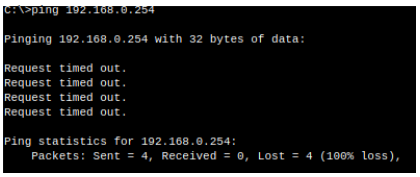
Figure 3: Verifying DENY-LAN1 Connections

Part 2: Troubleshoot ACL Issue 2

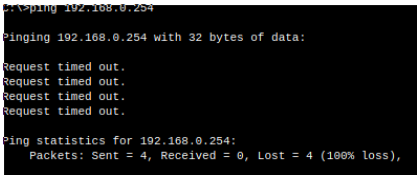
i) Determine the ACL problem

The second thing we are told is that L2 should have access to LAN3. But, that Lan2 shouldn't have access to Lan3. So, I will ping Server3 from L2. Next, I will ping Server3 from Server2. Both were unsuccessful. See Fig. 4a and Fig. 4b on Pg. 3 for those outputs.

Lastly, I ran the commands to show the output of access lists, to see how DENY-L2 was configured. See Fig. 1c.



(a) Pinging Server3 from L2



(b) Pinging Server3 from Server2

```
R1>en
R1#show access-lists
Standard IP access list DENY-LAN1
    10 deny 10.0.0.0 0.255.255.255
    20 permit any
Standard IP access list DENY-L2
    10 permit any
    20 deny host 172.16.0.2
Standard IP access list PERMIT-L3
    10 permit host 192.168.0.2
```

(c) DENY-L2 Access-list

Figure 4: Determining the problems in part 2

ii) Implement a Solution

I logged into R1, I looked up the access tables, I went to `int g0/2` and ran `no ip access-group DENY-L2 out`. I then reconfigured DENY-L2 to say `10 deny host 192.168.0.2 20 permit any` that way it would allow all other addresses. I then went to `int g0/1` and typed in `ip access-group DENY-L2 in`. See Fig. 5 on Pg. 4 for outputs.

iii) Verify that the problem is resolved and document the solution

I Verified the network connections by running a ping from L2 to Server3(Fig. 6a), and again from Server2 to Server3(Fig. 6b).

```
R1(config)#ip access-list standard DENY-L2
R1(config-std-nacl)#no 10
R1(config-std-nacl)#10 deny host 192.168.0.2
R1(config-std-nacl)#no 20
R1(config-std-nacl)#20 permit any
R1(config-std-nacl)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

(a) Configuring the ACL DENY-L2

```
R1#show access-lists
Standard IP access list DENY-LAN1
    10 deny 10.0.0.0 0.255.255.255
    20 permit any
Standard IP access list DENY-L2
    10 deny host 192.168.0.2
    20 permit any
Standard IP access list PERMIT-L3
    10 permit host 192.168.0.2
```

(b) Output of the Access-lists

```
GigabitEthernet0/2 is up, line protocol is up (connected)
  Internet address is 192.168.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is Deny-L2
  Proxy ARP is enabled
  Security level is default
```

(c) G0/2 Configured with DENY-L2

Figure 5: Configuring the ACL for R1 DENY-L2

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(a) L2 Ping to Server3

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

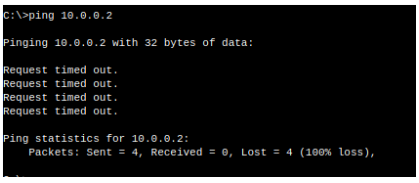
(b) Server2 Ping to Server3

Figure 6: Verifying DENY-L2 Connections

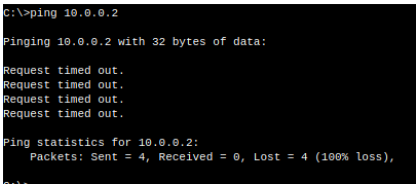
Part 3: Troubleshoot ACL Issue 3

i) Determine the ACL problem

Finally, we will test the connection to L1 and attempt to ping it both from L3, which it should have access to, and then from server3, which should not have access to it. You can see in Fig. 7 a and Fig. 7b on Pg. 5.



(a) Pinging L1 from L3



(b) Pinging L1 from Server3

```
R1#show ip int g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 10.0.0.1/8
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is PERMIT-L3
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
```

(c) Show ip int of g0/0 for PERMIT-L3

Figure 7: Checking original configuration of PERMIT-L3

ii) Implement a Solution

To fix the problem, I changed the access-list from incoming to an outgoing implementation. You can see in Fig. 8 a on Pg. 6.

We can now see the output of `show access-lists` (Fig. 8b) and `show ip int` (Fig. 8c).

iii) Verify that the problem is resolved and document the solution

We can now see based off of the configurations we've implemented that the ping from L3 to L1 is successful and that the ping from server3 to L1 is blocked at the router (Fig. 9).

Wrap-up

We can now see the ping's from each of the PC's to each of the servers, Fig. 10a through Fig. 10c on Pg. 7. We can see the final configurations of the interfaces, Fig. 11a through Fig. 11c on Pg. 8. And we can see the completion of activities, Fig. 12a through Fig. 12b on Pg. 8.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard PERMIT-L3
R1(config-std-nacl)#no 10
R1(config-std-nacl)#10 permit host 10.0.0.2
R1(config-std-nacl)#exit
R1(config)#int g0/0
R1(config-if)#no ip access-group PERMIT-L3 in
R1(config-if)#ip access-group PERMIT-L3 out
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

(a) Configuring and applying PERMIT-L3

```
R1#show access-lists
Standard IP access list DENY-LAN1
    10 deny 10.0.0.0 0.255.255.255
    20 permit any
Standard IP access list DENY-L2
    10 deny host 172.16.0.2
    20 permit any
Standard IP access list PERMIT-L3
    10 permit host 192.168.0.2
```

(b) show access-lists of PERMIT-L3

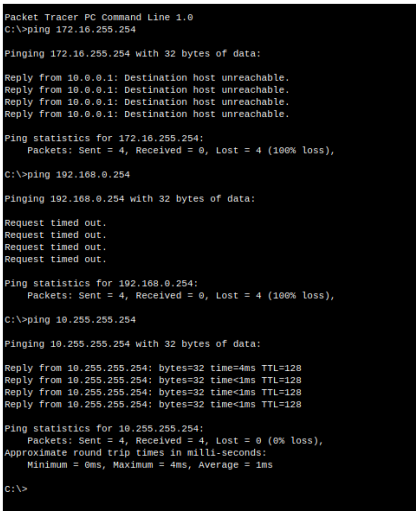
```
R1#show ip int g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 10.0.0.1/8
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is PERMIT-L3
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
```

(c) Show ip int of g0/0 with PERMIT-L3 applied

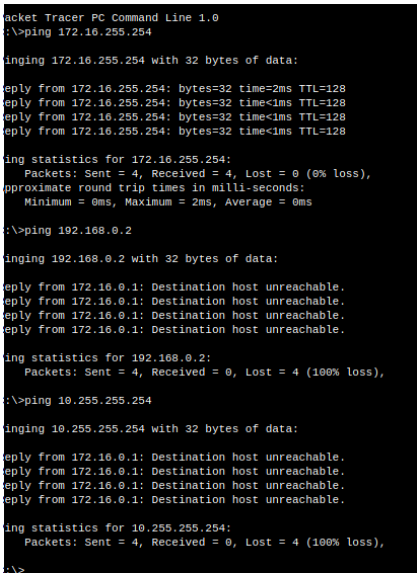
Figure 8: Configuring PERMIT-L3

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

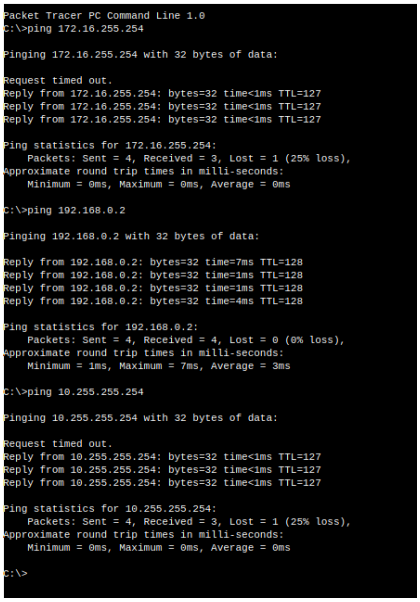
Figure 9: Server3 Blcoked pingin L1



(a) L1 Pinging Servers on the network

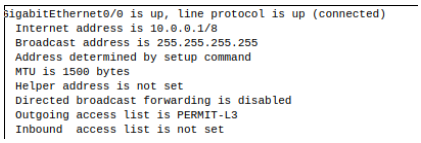


(b) L2 Pinging servers on the network

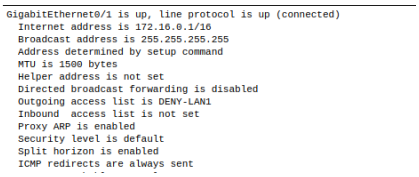


(c) L3 Pingin Servers on the network

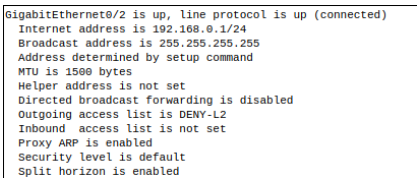
Figure 10: Wrap-up and overview



(a) Final Config of G0/0



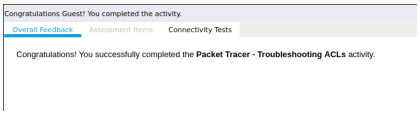
(b) Final Config for G0/1



(c) Final Config for G0/2

Figure 11: Final Configuration for the network interfaces

(a) Completion of activity



(b) Completion of activity

Figure 12: Completion of the Activity