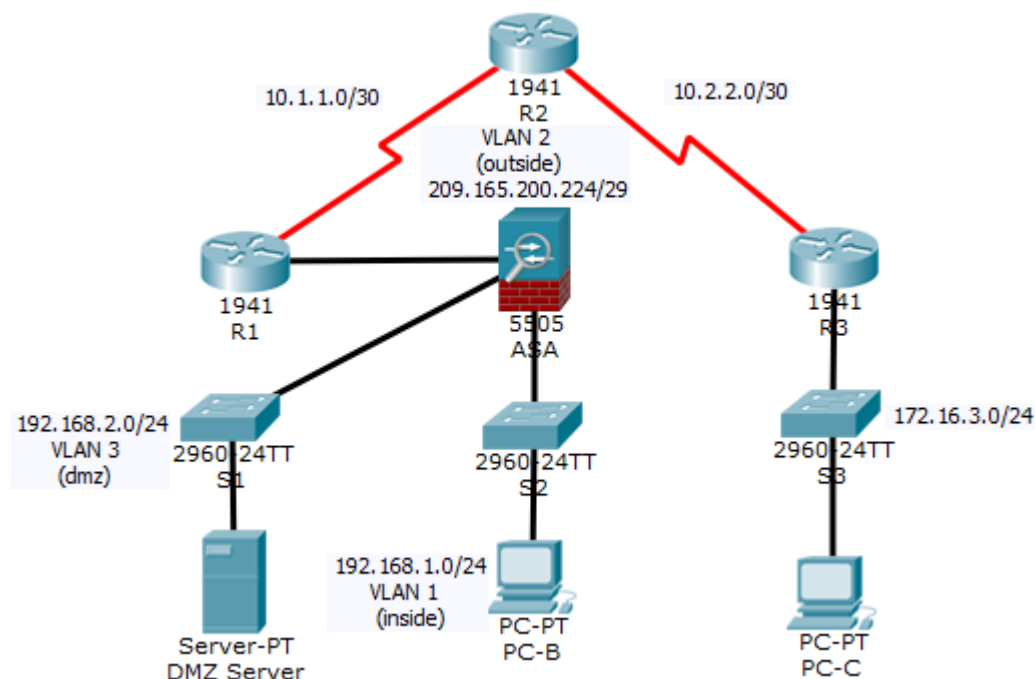


## Packet Tracer - Configuring ASA Basic Settings and Firewall Using CLI Topology



**NOTE:** I've added a Packet Tracer exercise file called Exercise – Configuring ASA to help!

## IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

## Objectives

- Verify connectivity and explore the ASA
- Configure basic ASA settings and interface security levels using CLI
- Configure routing, address translation, and inspection policy using CLI
- Configure DHCP, AAA, and SSH
- Configure a DMZ, Static NAT, and ACLs

## Scenario

Your company has one location connected to an ISP. R1 represents Customer Premises Equipment (CPE) device managed by the ISP. R2 represents an intermediate Internet router. R3 represents an ISP that connects an administrator from a network management company, who has been hired to remotely manage your network. The ASA is an edge CPE security device that connects the internal corporate network and DMZ to the ISP while providing NAT and DHCP services to inside hosts. The ASA will be configured for management by an administrator on the internal network and by the remote administrator. Layer 3 VLAN interfaces provide access to the three areas created in the activity: Inside, Outside, and DMZ. The ISP assigned the public IP address space of 209.165.200.224/29, which will be used for address translation on the ASA.

All router and switch devices have been preconfigured with the following:

- Enable password:
- Console password:
- Admin username and password:

**Note:** This activity provides additional practice and simulates most of the ASA 5505 configurations. When compared to a real ASA 5505, there may be slight differences in command output or commands that are not yet supported in Packet Tracer.

## Part 1: Verify Connectivity and Explore the ASA

### Step 1: Verify connectivity.

The ASA is not currently configured. However, all routers, PCs, and the DMZ server are configured. Verify that PC-C can ping any router interface e.g R1 209.165.200.225.

PC-C is unable to ping the ASA (209.165.200.226), PC-B (192.168.1.3), or the DMZ server(192.168.2.3).

### Step 2: Determine the ASA version, interfaces, and license.

Use the **show version** command to determine various aspects of this ASA device.

To enter privileged mode of the ASA. Use the **enable** command to enter privileged mode on the ASA. Note: there is NO PASSWORD required to enter privileged mode. Press **ENTER/RETURN** key on keyboard to move from user to privileged mode.

### Step 3: Enter privileged mode.

- Use the **enable** command to enter privileged mode on the ASA. Enter privileged EXEC mode. **A password has not been set.** Press **Enter** when prompted for a password.

## Part 2: Configure ASA Settings and Interface Security Using the CLI

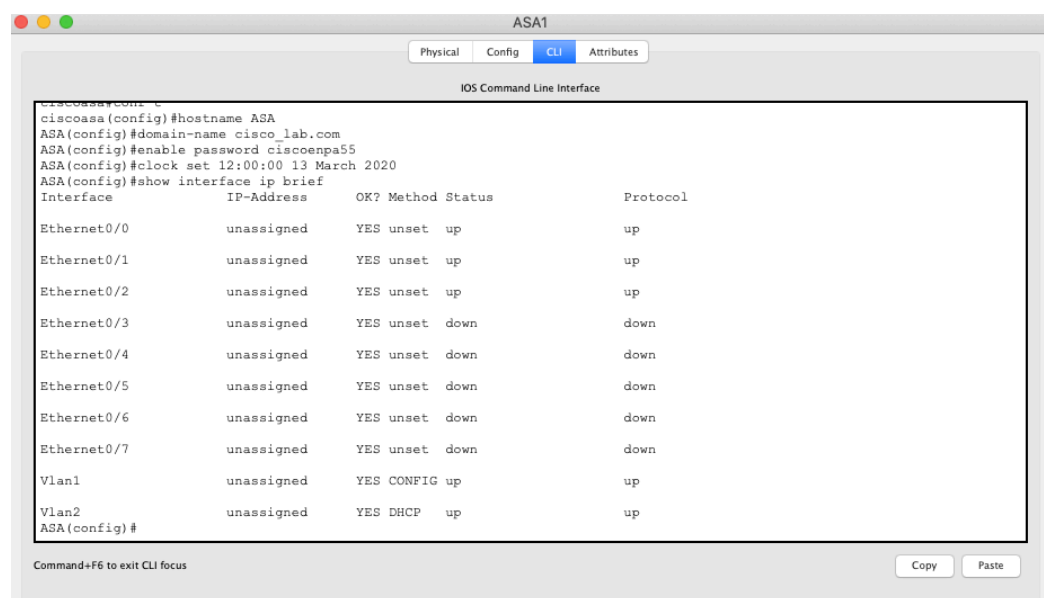
**Tip:** Many ASA CLI commands are similar to, if not the same, as those used with the Cisco IOS CLI. In addition, the process of moving between configuration modes and submodes is essentially the same.

### Step 1: Configure the hostname and domain name.

- Configure the ASA hostname as **ASA**.
- Configure the domain name as **ciscosecurity.com**

### Step 2: Configure the enable mode password.

Use the **enable password** command to change the privileged EXEC mode password to **ciscoenpa55**.



e.g. **NOTE:** in the example above I've used the domain name `cisco_lab.com` but you should use `ciscosecurity.com` – this will be required below in the SSH configuration.

### Step 3: Set the date and time.

Use the **clock set** command to manually set the date and time.

### Step 4: Configure the inside and outside interfaces.

Use the **show interface ip brief** command to see the state of the current interfaces.

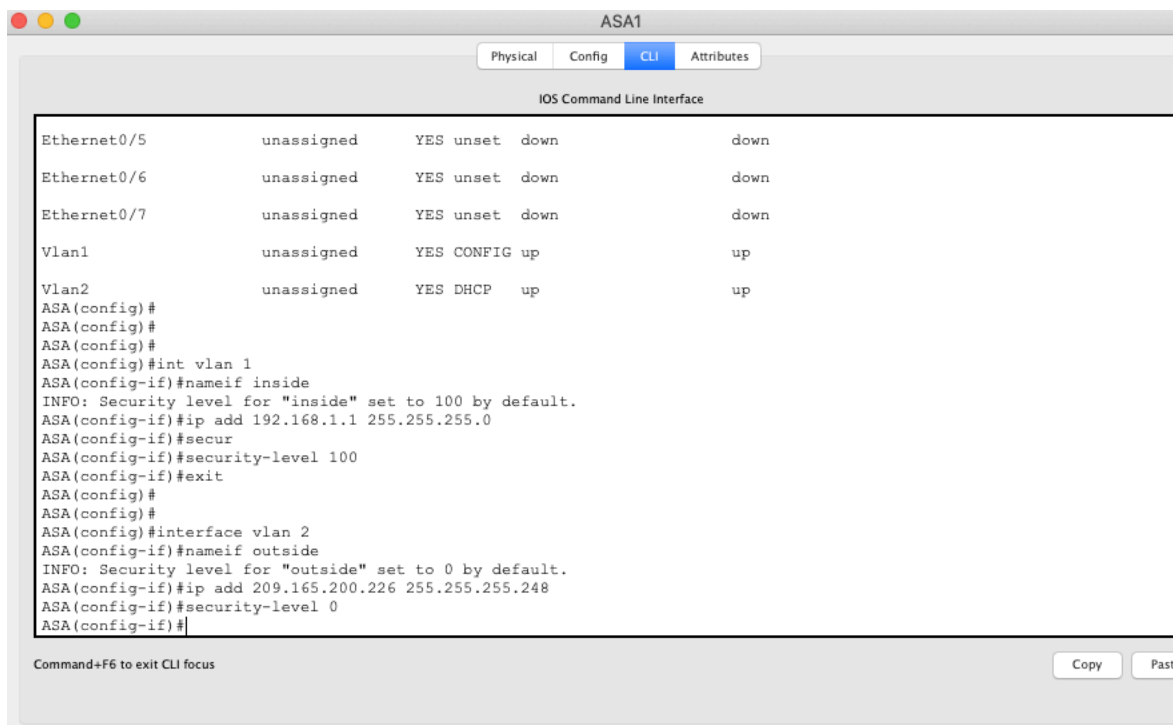
You will only configure the VLAN 1 (inside) and VLAN 2 (outside) interfaces at this time. The VLAN 3 (dmz) interface will be configured in Part 5 of the activity.

- Configure a logical VLAN 1 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100.

```
ASA(config)# interface vlan 1
ASA(config-if)# nameif inside
ASA(config-if)# ip address 192.168.1.1 255.255.255.0
ASA(config-if)# security-level 100
```

- Create a logical VLAN 2 interface for the outside network (209.165.200.224/29), set the security level to the lowest setting of 0, and enable the VLAN 2 interface.

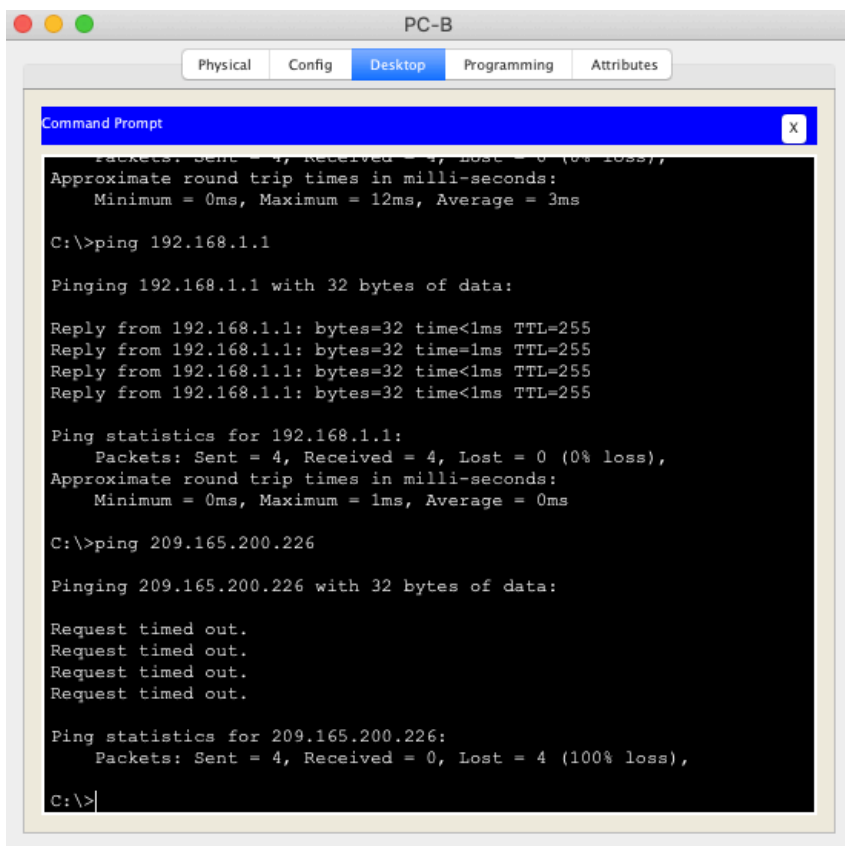
```
ASA(config-if)# interface vlan 2
ASA(config-if)# nameif outside
ASA(config-if)# ip address 209.165.200.226 255.255.255.248
ASA(config-if)# security-level 0
```



- c. Use the following verification commands to check your configurations:
  - 1) Use the **show interface ip brief** command to display the status for all ASA interfaces. **Note:** This command is different from the IOS command **show ip interface brief**. If any of the physical or logical interfaces previously configured are not up/up, troubleshoot as necessary before continuing.  
**Tip:** Most ASA **show** commands, including **ping**, **copy**, and others, can be issued from within any configuration mode prompt without the **do** command.
  - 2) Use the **show ip address** command to display the information for the Layer 3 VLAN interfaces.
  - 3) Use the **show switch vlan** command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.

### Step 5: Test connectivity to the ASA.

- a. You should be able to ping from PC-B to the ASA inside interface address (192.168.1.1). If the pings fail, troubleshoot the configuration as necessary.
- b. From PC-B, ping the VLAN 2 (outside) interface at IP address 209.165.200.226. You should not be able to ping this address.
- c. Example:



The screenshot shows the PC-B Desktop tab in Packet Tracer. A Command Prompt window is open, displaying the results of two ping commands. The first command is `C:\>ping 192.168.1.1`, which shows successful connectivity with 4 packets sent and received, 0% loss, and an average round trip time of 3ms. The second command is `C:\>ping 209.165.200.226`, which shows that all four requests timed out, resulting in 100% loss.

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:

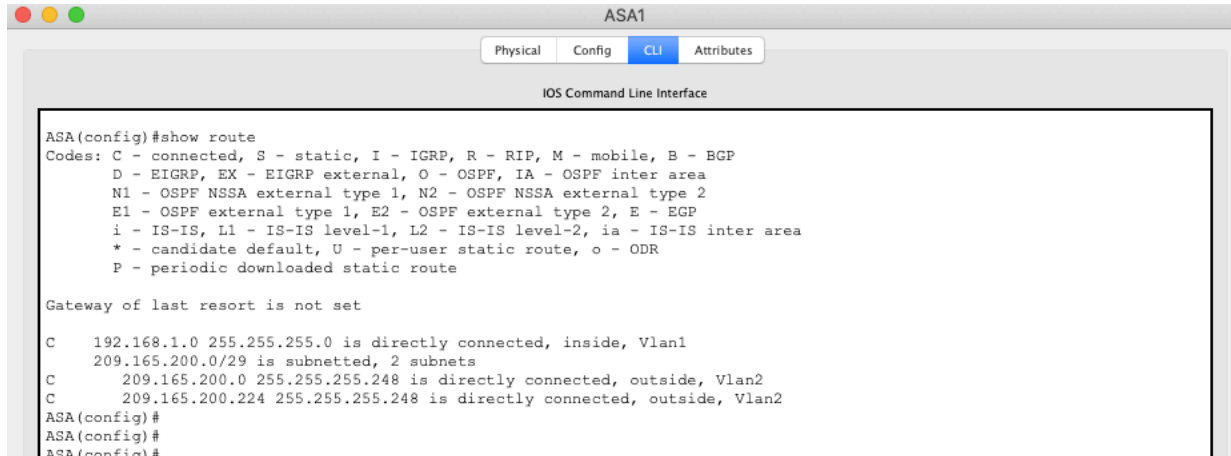
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.226:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

## Part 3: Configure Routing, Address Translation, and Inspection Policy Using the CLI

Before you configure the static default route, view the current routing table.



```
ASA1
Physical Config CLI Attributes
IOS Command Line Interface

ASA(config)#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
     209.165.200.0/29 is subnetted, 2 subnets
C      209.165.200.0 255.255.255.248 is directly connected, outside, Vlan2
C      209.165.200.224 255.255.255.248 is directly connected, outside, Vlan2
ASA(config)#
ASA(config)#
ASA(config)#
```

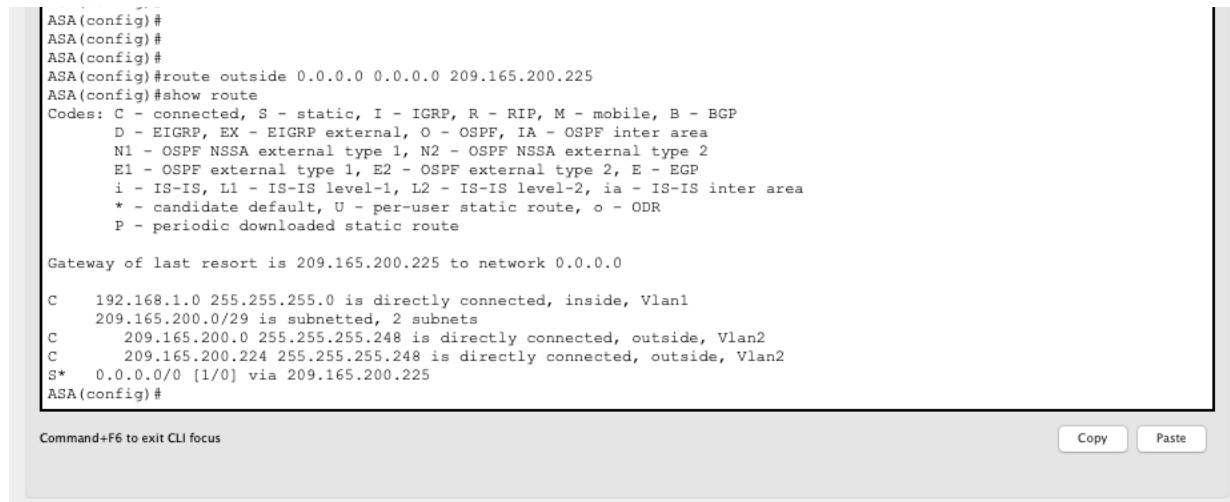
### Step 1: Configure a static default route for the ASA.

Configure a default static route on the ASA outside interface to enable the ASA to reach external networks.

- Create a “quad zero” default route using the **route** command, associate it with the ASA outside interface, and point to the R1 G0/0 IP address (209.165.200.225) as the gateway of last resort.

```
ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

- Issue the **show route** command to verify the static default route is in the ASA routing table.



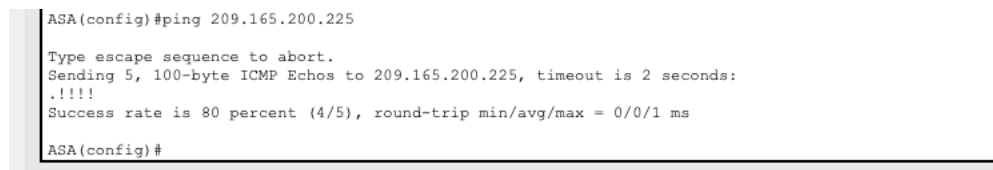
```
ASA(config)#
ASA(config)#
ASA(config)#
ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
ASA(config)#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

C    192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
     209.165.200.0/29 is subnetted, 2 subnets
C      209.165.200.0 255.255.255.248 is directly connected, outside, Vlan2
C      209.165.200.224 255.255.255.248 is directly connected, outside, Vlan2
S*    0.0.0.0/0 [1/0] via 209.165.200.225
ASA(config)#
```

c.

- Verify that the **ASA** can ping the R1 S0/0/0 IP address 10.1.1.1. If the ping is unsuccessful, troubleshoot as necessary.



```
ASA(config)#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

ASA(config)#
```

### Step 2: Configure address translation using PAT and network objects.

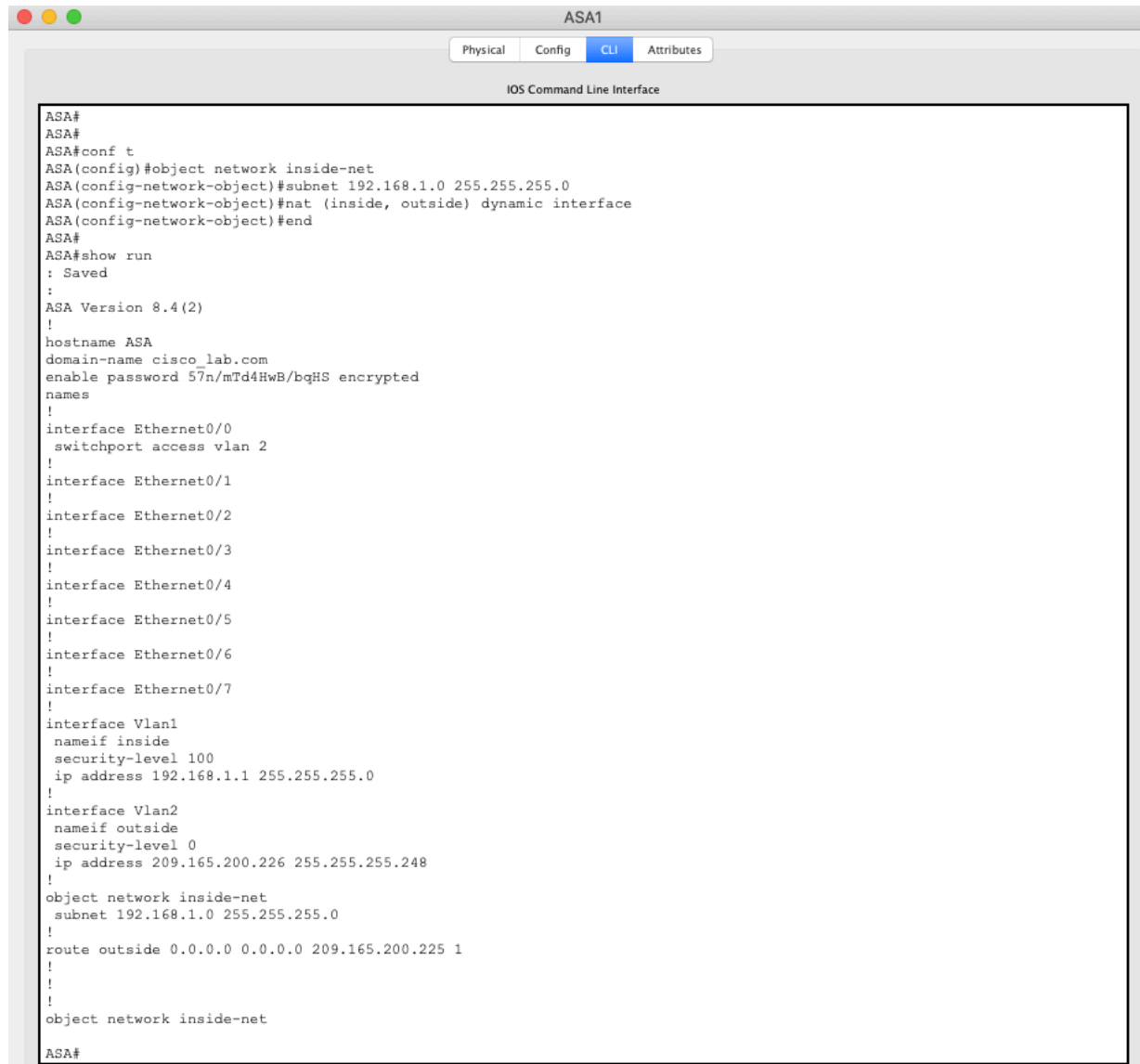
- Create network object **inside-net** and assign attributes to it using the **subnet** and **nat** commands.

```
ASA(config)# object network inside-net
```

```
ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
```

```
ASA(config-network-object)# nat (inside,outside) dynamic interface
ASA(config-network-object)# end
```

Example:



```
ASA1
Physical Config CLI Attributes
IOS Command Line Interface

ASA#
ASA#
ASA#conf t
ASA(config)#object network inside-net
ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)#nat (inside, outside) dynamic interface
ASA(config-network-object)#end
ASA#
ASA#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ASA
domain-name cisco_lab.com
enable password 57n/mTd4HwB/bqHS encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
object network inside-net
 subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
!
!
object network inside-net
ASA#
```

- b. The ASA splits the configuration into the object portion that defines the network to be translated and the actual **nat** command parameters. These appear in two different places in the running configuration. Display the NAT object configuration using the **show run** command.
- c. From PC-B attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. **The pings should fail.**
- d. Issue the **show nat** command on the ASA to see the translated and untranslated hits. Notice that, of the pings from PC-B, four were translated and four were not. The outgoing pings (echos) were translated and sent to the destination. The returning echo replies were blocked by the firewall policy. You will configure the default inspection policy to allow ICMP in Step 3 of this part of the activity.

e.

```
ASA#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
   translate_hits = 4, untranslate_hits = 4
```

### Step 3: Modify the default MPF application inspection global service policy.

For application layer inspection and other advanced options, the Cisco MPF is available on ASAs.

The Packet Tracer **ASA device does not have an MPF policy map in place by default**. As a modification, we can create the default policy map that will perform the inspection on inside-to-outside traffic. When configured correctly only traffic initiated from the inside is allowed back in to the outside interface. You will need to add ICMP to the inspection list.

- a. Create the class-map, policy-map, and service-policy. Add the inspection of ICMP traffic to the policy map list using the following commands:

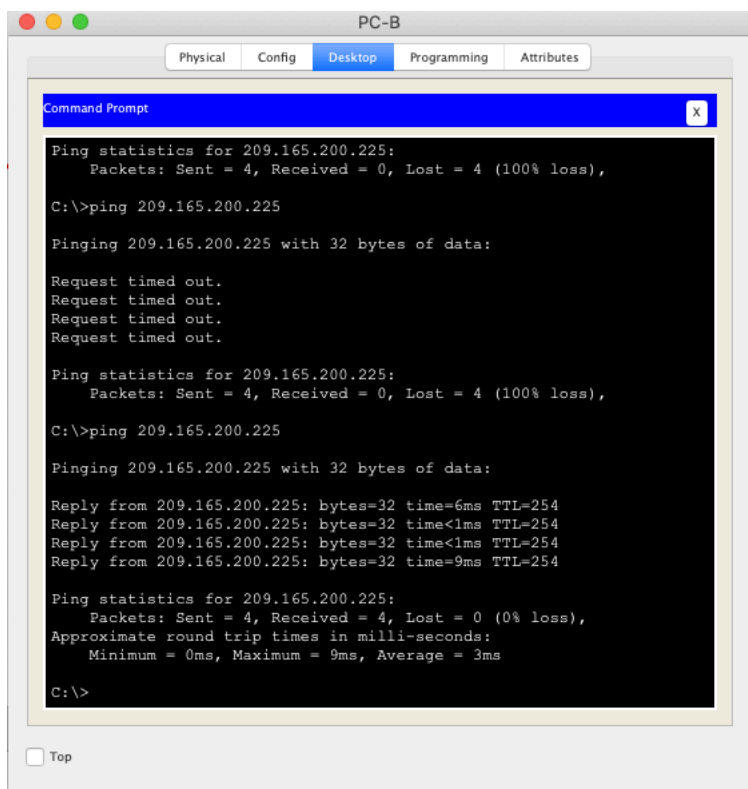
```
ASA(config)# class-map inspection_default
ASA(config-cmap)# match default-inspection-traffic
ASA(config-cmap)# exit
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# inspect icmp
ASA(config-pmap-c)# exit
ASA(config)# service-policy global_policy global
```

```
ASA#
ASA#conf t
ASA(config)#class-map inspection_default
ASA(config-cmap)#match default-inspection-traffic
ASA(config-cmap)#exit
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect ?

mode commands/options:
  dns
  ftp
  h323
  http
  icmp
  tftp
ASA(config-pmap-c)#inspect icmp
ASA(config-pmap-c)#exit
ASA(config)#service-policy global_policy global
ASA(config)#
```

- b. From PC-B, attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should be successful this time because ICMP traffic is now being inspected and legitimate return traffic is being **allowed**. If the pings fail, troubleshoot your configurations.



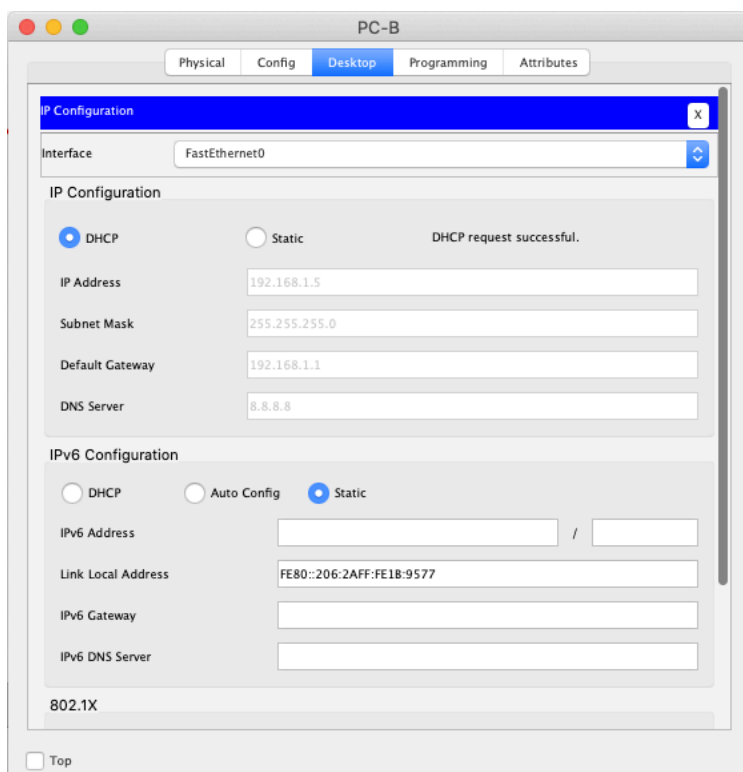


C.

## Part 4: Configure DHCP, AAA, and SSH

### Step 1: Configure the ASA as a DHCP server.

- Configure a DHCP **address pool** and enable it on the ASA inside interface.  
`ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside`
- (Optional) **Specify the IP address of the DNS server** to be given to clients.  
`ASA(config)# dhcpd dns 8.8.8.8 interface inside`
- Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside).  
`ASA(config)# dhcpd enable inside`
- Change PC-B from a static IP address to a DHCP client, and verify that it receives IP addressing information. Troubleshoot, as necessary to resolve any problems.



e.

### Step 2: Configure AAA to use the local database for authentication.

- Define a local user named **admin** by entering the **username** command. Specify a password of **adminpa55**.

```
ASA(config)# username admin password adminpa55
```

- Configure AAA to use the local ASA database for SSH user authentication.

```
ASA(config)# aaa authentication ssh console LOCAL
```

### Step 3: Configure remote access to the ASA.

The ASA can be configured to accept connections from a single host or a range of hosts on the inside or outside network. In this step, hosts from the outside network can only use SSH to communicate with the ASA. SSH sessions can be used to access the ASA from the inside network.

- Generate an RSA key pair, which is required to support SSH connections. Because the ASA device has RSA keys already in place, enter **no** when prompted to replace them.

```
ASA(config)# crypto key generate rsa modulus 1024
```

WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

```
Do you really want to replace them? [yes/no]: no
```

```
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
```

- Configure the ASA to allow SSH connections from any host on the inside network (192.168.1.0/24) and from the remote management host at the branch office (172.16.3.3) on the outside network. Set the SSH timeout to 10 minutes (the default is 5 minutes).

```
ASA(config)# ssh 192.168.1.0 255.255.255.0 inside
```

```
ASA(config)# ssh 172.16.3.3 255.255.255.255 outside
```

```
ASA(config)# ssh timeout 10
```

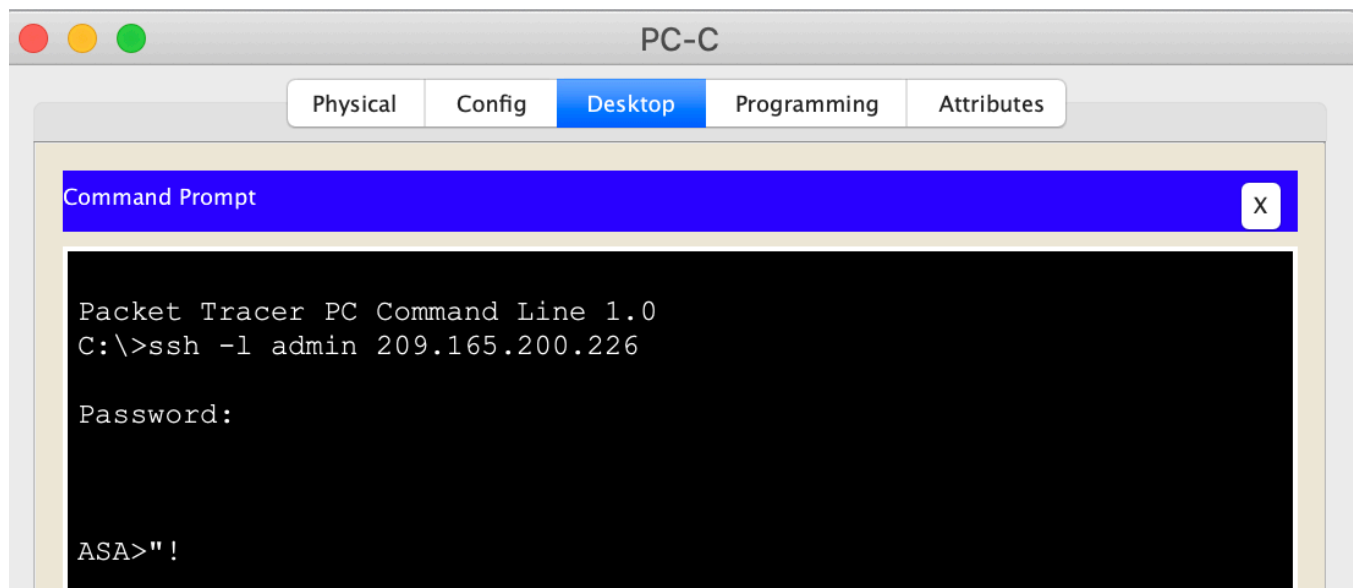
- c. Establish an SSH session from PC-C to the ASA (209.165.200.226). Troubleshoot if it is not successful.

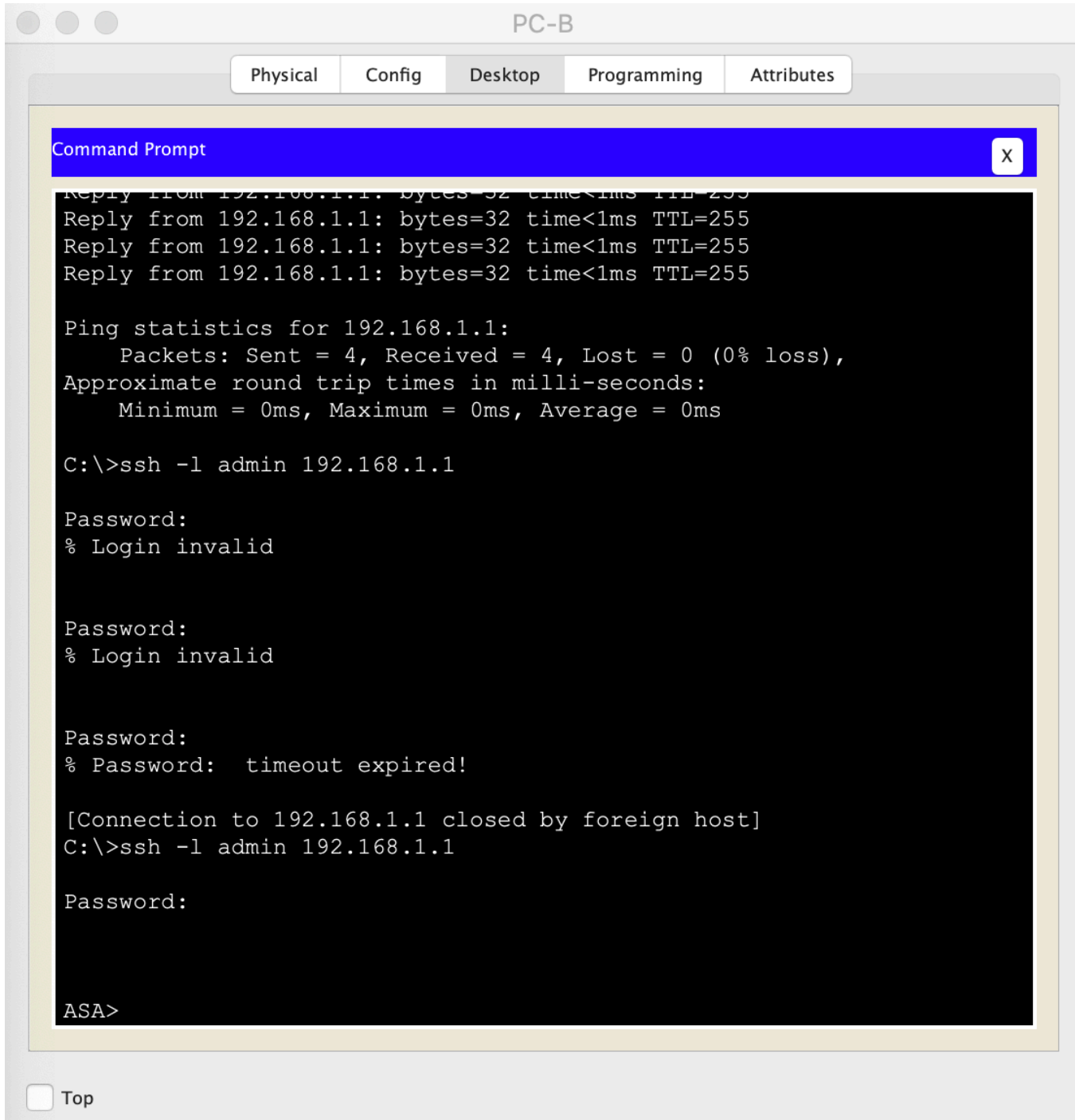
```
PC> ssh -l admin 209.165.200.226
```

- d. Establish an SSH session from PC-B to the ASA (192.168.1.1). Troubleshoot if it is not successful.

```
PC> ssh -l admin 192.168.1.1
```

**Note:** if this doesn't work, ensure you have set the domain name as `ciscosecurity.com` in Part 2 above. Use the SSH command (shown below) from PC-B or PC-C.





**Note:** Ensure to use the correct password too!

### Part 5: Configure a DMZ, Static NAT, and ACLs

R1 G0/0 and the ASA outside interface already use 209.165.200.225 and .226, respectively. You will use public address 209.165.200.227 and static NAT to provide address translation access to the server.

### Step 1: Configure the DMZ interface VLAN 3 on the ASA.

- a. Configure DMZ VLAN 3, which is where the public access web server will reside. Assign it IP address 192.168.2.1/24, name it **dmz**, and assign it a security level of 70. Because the server does not need to initiate communication with the inside users, disable forwarding to interface VLAN 1.

```
ASA(config)# interface vlan 3
ASA(config-if)# ip address 192.168.2.1 255.255.255.0
ASA(config-if)# no forward interface vlan 1
ASA(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA(config-if)# security-level 70
```

- b. Assign ASA physical interface E0/2 to DMZ VLAN 3 and enable the interface.

```
ASA(config)# interface Ethernet0/2
ASA(config-if)# switchport access vlan 3
```

- c. Use the following verification commands to check your configurations:

- 1) Use the **show interface ip brief** command to display the status for all ASA interfaces.
- 2) Use the **show ip address** command to display the information for the Layer 3 VLAN interfaces.
- 3) Use the **show switch vlan** command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.

### Step 2: Configure static NAT to the DMZ server using a network object.

Configure a **network object named dmz-server** and assign it the static IP address of the DMZ server (192.168.2.3). While in object definition mode, use the **nat** command to specify that this object is used to translate a DMZ address to an outside address using static NAT, and **specify a public translated address** of 209.165.200.227.

```
ASA(config)# object network dmz-server
ASA(config-network-object)# host 192.168.2.3
ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
ASA(config-network-object)# exit
```

### Step 3: Configure an ACL to allow access to the DMZ server from the Internet.

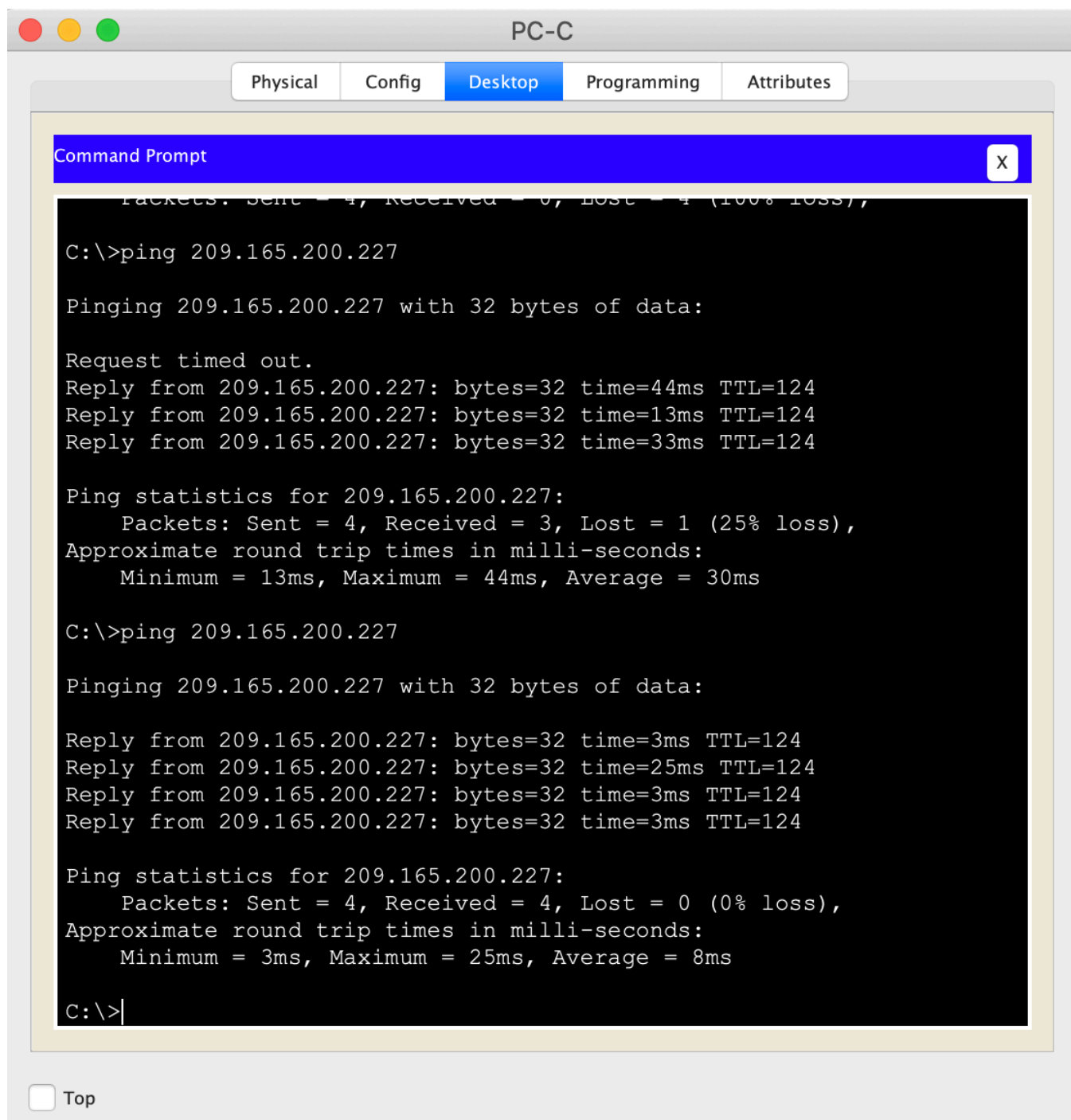
Configure a **named access list OUTSIDE-DMZ** that permits the TCP protocol on port 80 from any external host to the internal IP address of the DMZ server. Apply the access list to the ASA outside interface in the "IN" direction.

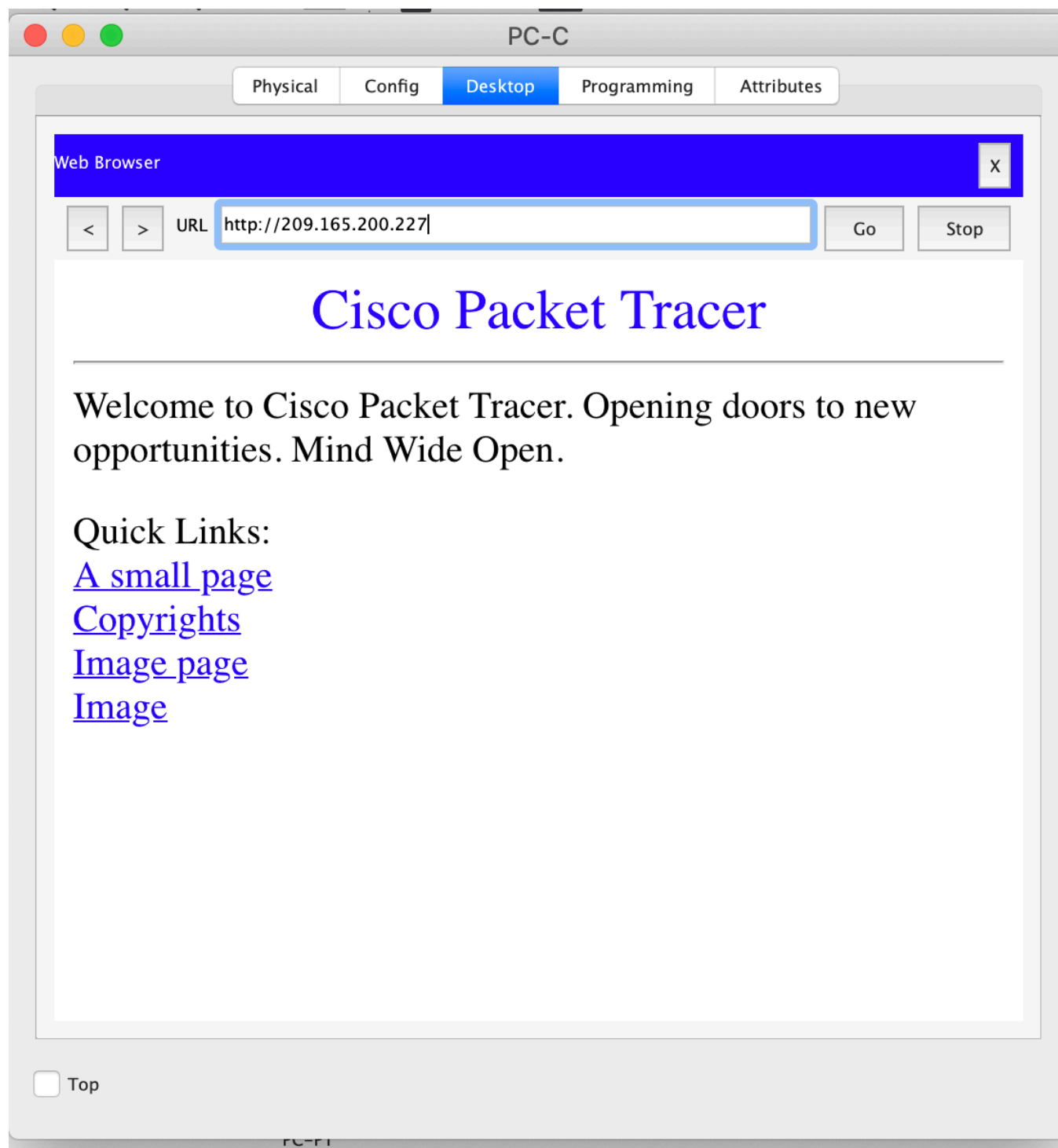
```
ASA(config)# access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
ASA(config)# access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
ASA(config)# access-group OUTSIDE-DMZ in interface outside
```

**Note:** Unlike IOS ACLs, the ASA ACL permit statement must permit access to the internal private DMZ address. **External hosts access the server using its public static NAT address, the ASA translates it to the internal host IP address, and then applies the ACL.**

### Step 4: Test access to the DMZ server.

Test outside access to the DMZ - launch a ping test to the DMZ server to check for connectivity. Then, try and get to the web server from PC-C.





**Step 5: Check results. Well done!**

References: Cisco Networking Academy - Please note this exercise has been modified from the original to add in extra step by step images.