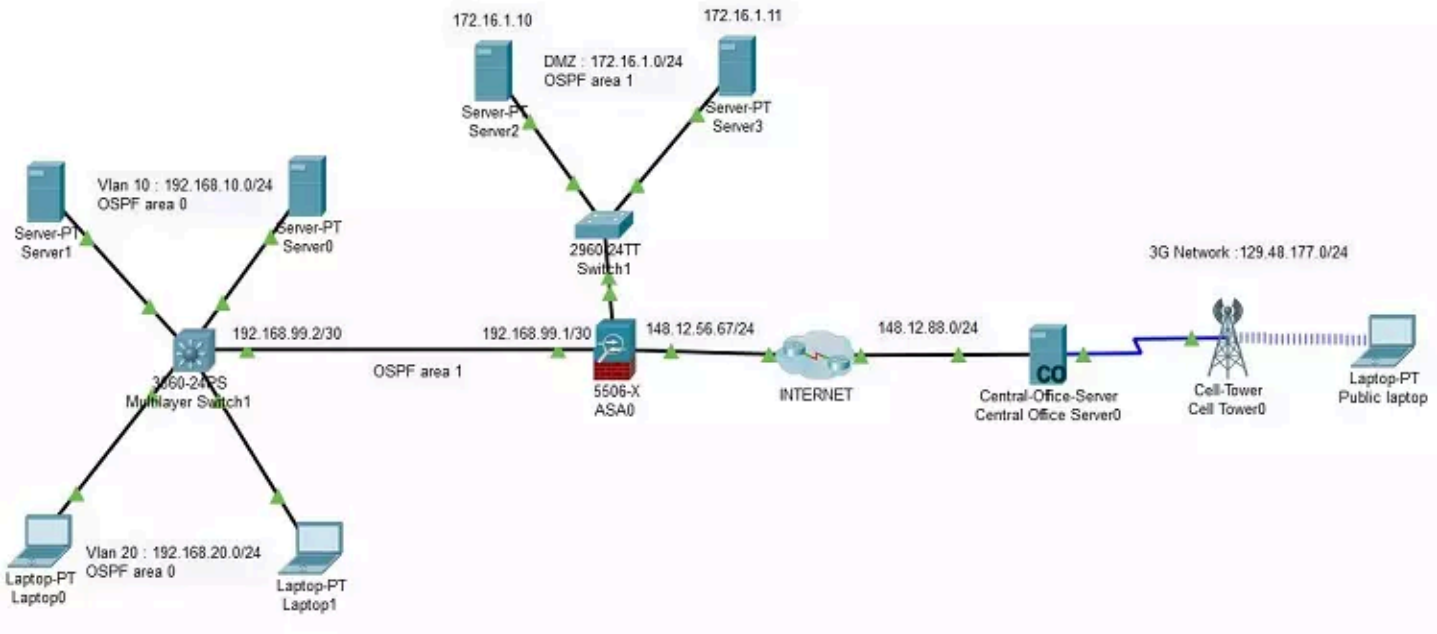
Network diagram

In this lab, the **AutoNAT feature of ASA 5506-X firewall** is used to configure the NAT rules that allow the hosts on the LAN segments to connect to the Internet. Network Address Translation is needed because these internal hosts use private IP addresses which are not routable on the Internet. Network Address Translation makes the addresses so that they look like the ASA's outside interface IP address. AutoNAT suits best if the ASA external IP changes frequently (DHCP).



Lab instructions

1. Configure NAT to allow LAN users to access the INTERNET

2. Configure NAT to allow DMZ servers to access the INTERNET

3. Configure inbound NAT rule to allow access to the 172.16.1.10 DMZ webserver from the Internet with 148.12.56.68 public IP address.

4. Configure ICMP rules to allow laptop1 to ping 148.12.56.1 internet router and any internet resource. An access-list, named OUTSIDE, will be configured to allow incoming echo-reply and unreachable ICMP replies

5.Configure the required access-lists on the internet facing interface to allow incoming trafic to the DMZ webserver

6.Test HTTP connectivity from the Public laptop to the DMZ webserver (http://148.12.56.68)

Lab Solution

1. Configure NAT to allow LAN users to access the INTERNET

AutoNAT configuration for the LAN subnet is done by creating a **network object** representing each LAN subnet. In each of these objects, a dynamic nat rule is configured to conduct Port Address Translation (PAT) on these clients as they pass from the inside to the outside interface.

The name of each interface, configured with **nameif**, is used in the AutoNAT command : **nat (inside,outside) dynamic interface**

```
object network LAN
 subnet 192.168.20.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

2. Configure NAT to allow DMZ servers to access the INTERNET

The same configuration as for the LAN subnet is done for the DMZ servers subnet. The source interface name is replaced by the DMZ named interface.

```
object network DMZ
 subnet 172.16.1.0 255.255.255.0
 nat (DMZ,outside) dynamic interface
```

3. Configure inbound NAT rule for 172.16.1.10 DMZ webserver access

The following NAT rule statically maps the DMZ 172.16.1.10 webserver address to the 148.12.56.68 external address. Rule is bi-directional.

```
object network webserver
 host 172.16.1.10
 nat (DMZ,outside) static 148.12.56.68
```

4. Configure ICMP rules

Configure an extended access-list with the required rules to accept incoming echo replies.

```
access-list OUTSIDE extended permit icmp any any echo-reply
access-list OUTSIDE extended permit icmp any any unreachable
```

5.Configure the required ACL to allow incoming trafic to the DMZ webserver

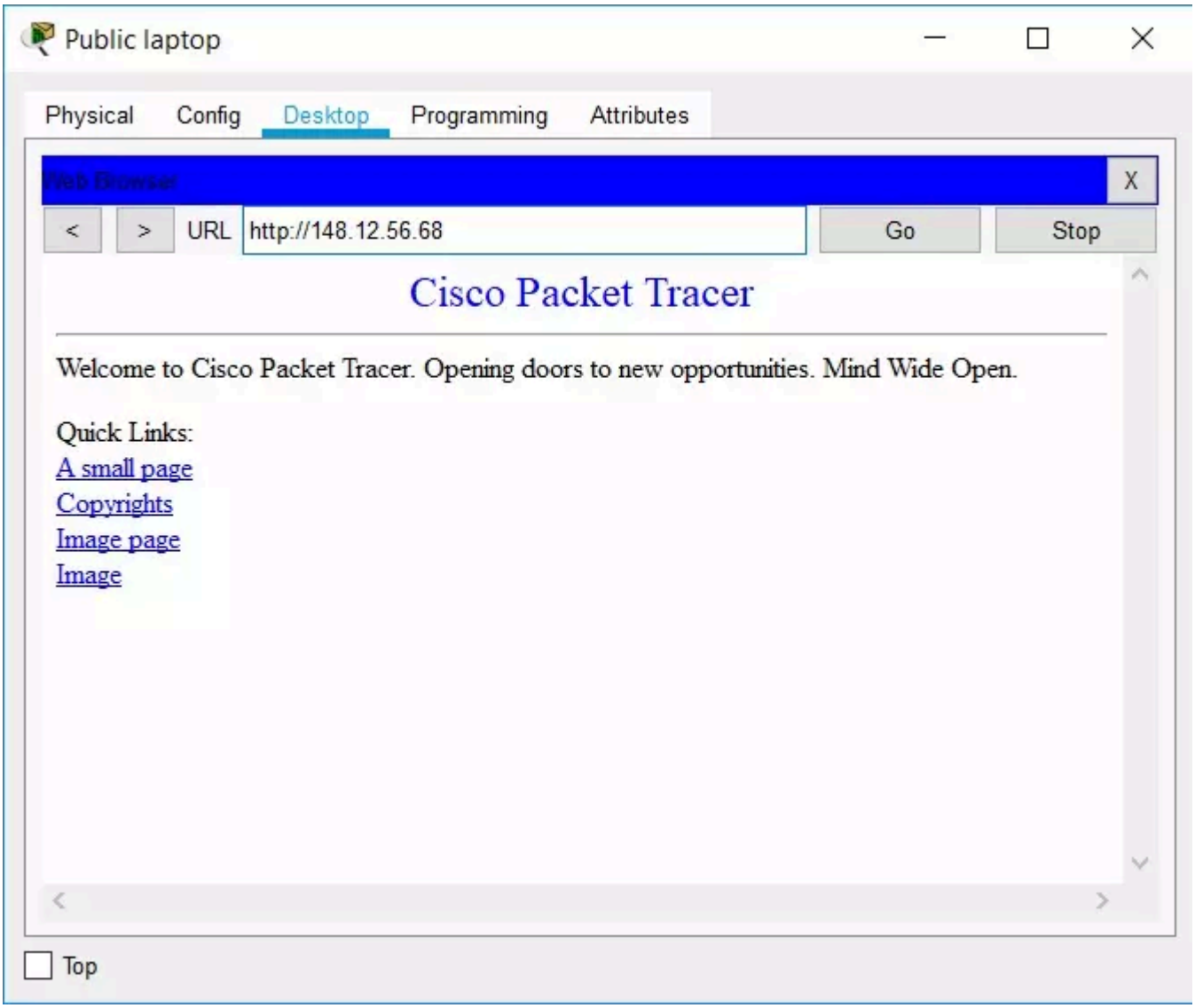
Complete the previous access-list with the rules to allow inbound HTTP trafic and apply the ACL to the outside interface.

```
object network webserver-external-ip
 host 148.12.56.68

access-list OUTSIDE extended permit tcp any object webserver eq www
access-list OUTSIDE extended permit tcp any host 148.12.56.68 eq www

access-group ICMP-REPLY in interface outside
```

6.Test HTTP connectivity Internet to the DMZ webserver

Open a web browser on the "Public LAPTOP" located on the right of the network diagram.

The connection to http://148.12.56.67 should display the following welcome page.



ASA 5505 and 5506-X comparison

ASA 5506-X - Layer 3 interfaces

The new ASA 5506-X firewall provided in Packet Tracer 8.2 is configured with 8 layer 3 network interfaces. Each interface can be configured with it's own name and security level.

ASA 5506-X is configured with the Security Plus license by default which unlocks unlimited usage of the layer 3 physical interfaces, 30 vlans (50% more than ASA 5505), and 50 VPN peers (100% more than ASA 5505)

```
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 30             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Carrier                           : Disabled       perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 50             perpetual
Total VPN Peers                   : 50             perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
Shared License                    : Disabled       perpetual
Total UC Proxy Sessions           : 160            perpetual
Botnet Traffic Filter             : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has an ASA 5506 Security Plus license.
```

ASA 5505 - Vlan interfaces and basic license bundle problems with DMZ creation

The ASA 5505 firewall provided in Packet Tracer 7.1.1 was shipped and installed by default with the basic license bundle. The content of this license package is displayed below :

```
Licensed features for this platform:
Maximum Physical Interfaces : 8 perpetual
VLANs : 3 DMZ Restricted
Dual ISPs : Disabled perpetual
VLAN Trunk Ports : 0 perpetual
Inside Hosts : 10 perpetual
Failover : Disabled perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 10 perpetual
Total VPN Peers : 25 perpetual
```

```
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual

This platform has a Base license.
```

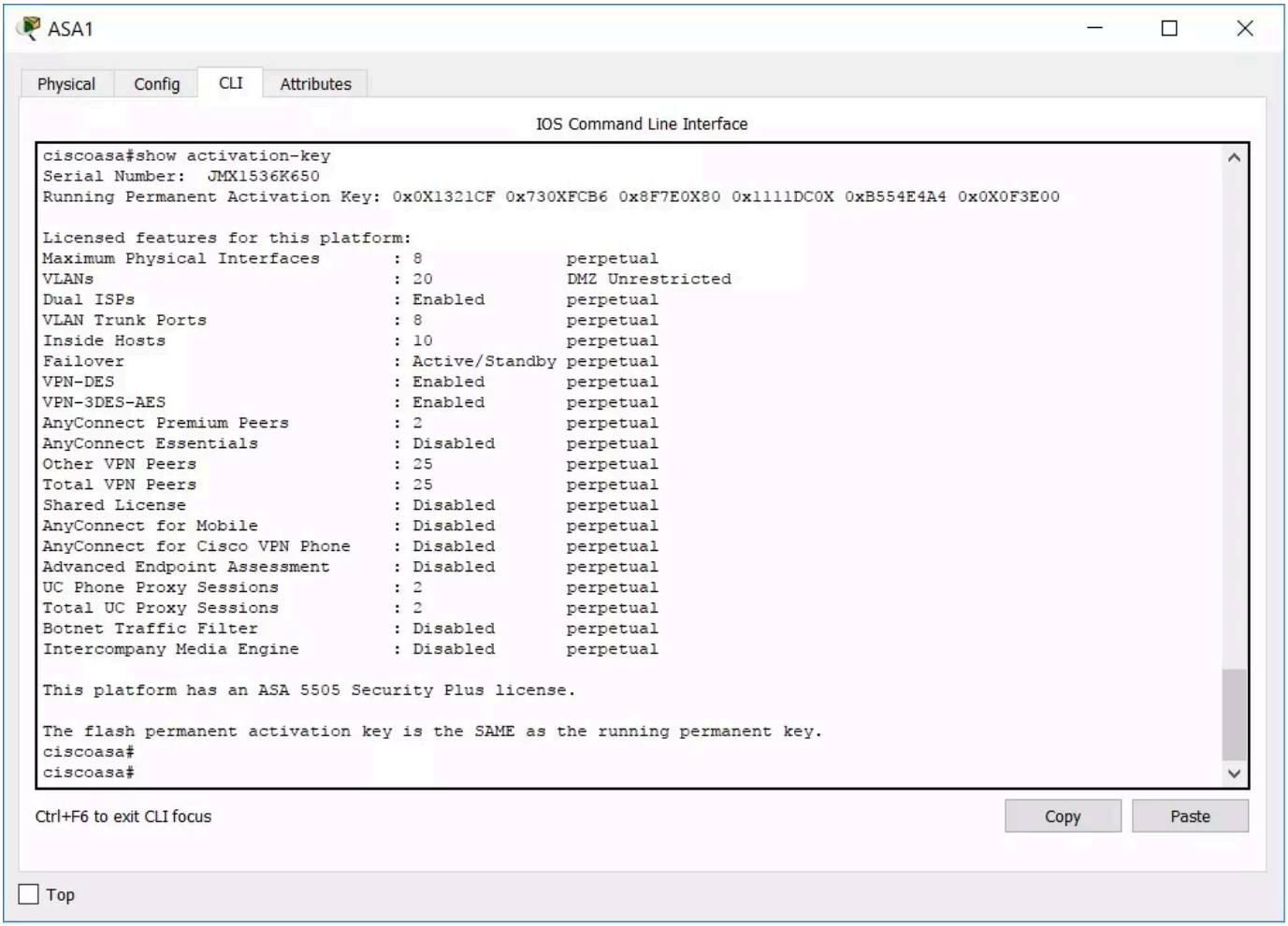
The ASA 5505 is configured by default with 2 vlans :

- VLAN 1 : Inside VLAN (interfaces E0/1 -> E0/7)
- VLAN 2 : Outside VLAN (interface E0/0)

If you try to configure a third vlan to host your DMZ,the ASA device will return the following error because of the limited licence :
ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s) with nameif already configured.

You have to limit communications between two vlan interfaces to make the creation of the third vlan interface possible. This can be done for example using the command **no forward interface vlan 1** on the "interface vlan 3" to deny communications betwen the inside network and the DMZ

The "security plus" license bundle which remove this limitation in the ASA 5505 (available from Packet Tracer 7.1.1) and can be unlocked with the **activation-key 0x1321CF73 0xFCB68F7E 0x801111DC 0xB554E4A4 0x0F3E008D** command. Up to 20 vlans can now be configured in the ASA 5505.


ASA1
Physical
Config
CLI
Attributes
IOS Command Line Interface
ciscoasa#show activation-key
Serial Number: JMX1536K650
Running Permanent Activation Key: 0x0X1321CF 0x730XFCB6 0x8F7E0X80 0x1111DC0X 0xB554E4A4 0x0X0F3E00
Licensed features for this platform:
Maximum Physical Interfaces : 8 perpetual
VLANs : 20 DMZ Unrestricted
Dual ISPs : Enabled perpetual
VLAN Trunk Ports : 8 perpetual
Inside Hosts : 10 perpetual
Failover : Active/Standby perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 25 perpetual
Total VPN Peers : 25 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
This platform has an ASA 5505 Security Plus license.
The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
ciscoasa#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top