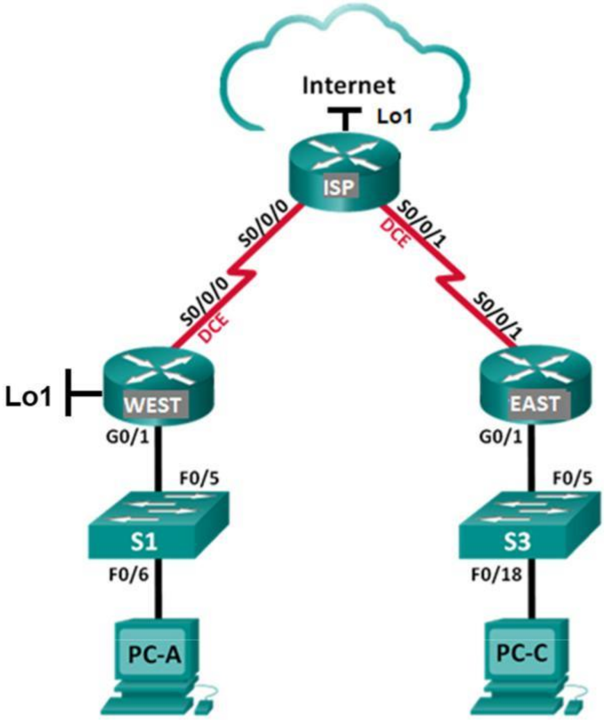
CCNA ENSA Lab 2

Team Members: Rubaiya Kabir Pranti

Network Address Translation (NAPT)

Securing Networks with ACLs WAN – PPP Connections



Homework / Lab Preparations

ENSA:	Modules 3 – 5 Exam: Network Security
	Modules 6 – 8 Exam: WAN Concepts
IN Course:	Chapters 5 (ACL, NAT)
	Chapter 6 (WAN, HDLC, PPP)
	Cisco IOS Commands

Lab Instructions

Task 1	Network Address and Port Translation (NAPT)
Task 2	Securing Networks with ACLs
Task 3	WAN – PPP Connections

Deliverables and Due Dates

Homework / Lab Preparation

Part 1: Cisco IOS Basic Configuration Commands

a. Read the **Lab Instructions** of this Lab

b. Check the **IOS Command List**, provided for the Labs and review configuration commands.

Part 2: Access Control Lists (ACL)

a. Standard Access Control Lists (ACLs)

If you apply a Standard ACL at an interface, what is tested by this standard ACL filter?
With standard ACL we can only filter at Layer 3 using the source IPv4 address only, so ACL will permit or deny a packet based only in IPv4 source address. In comparison to Extended ACL where source and destination IPv4 is filtered and also layer 4 using TCP and UDP ports.

b. Extended Access Control Lists (ACLs)

The following commands of an extended ACL on R1 are given, active on interface G0/0/0 direction is OUT. There is no other ACL with direction IN.

For each line, explain which filtering function is performed.

```
R1(config)#access-list 101 permit icmp any
                                       192.168.10.0 0.0.0.255 echo-reply
```

101 - access-list-number
permit icmp any - allow any host from source network to send icmp messages

192.168.10.0 0.0.0.255 - this will allow only hosts from this network to send echo-reply but not to request a ping

```
R1(config)#access-list 101 permit tcp any eq 80 192.168.10.0 0.0.0.255
```

101 - is the access-list-number.

permit tcp any eq 80 - this tells the router to allow any (from all hosts) packet which is using tcp as a transport protocol and port number 80. This identifies the source network. Port 80 is for http connection, www.

192.168.10.0 0.0.0.255 - this identifies the destination network

```
R1(config)#access-list 101 permit tcp any eq 443 192.168.1.0 0.0.0.255
```

101 - is the access-list-number.

permit tcp any eq 443 - this tells the router to allow any (from all hosts) packet which is using tcp as a transport protocol and port number 443. This identifies the source network. Port 443 is for https connection.

192.168.1.0 0.0.0.255 - this identifies the destination network

```
R1(config)#access-list 101 permit tcp host 192.168.3.3
                                      host 192.168.1.3 range 22 23
```

101 - access-list-number

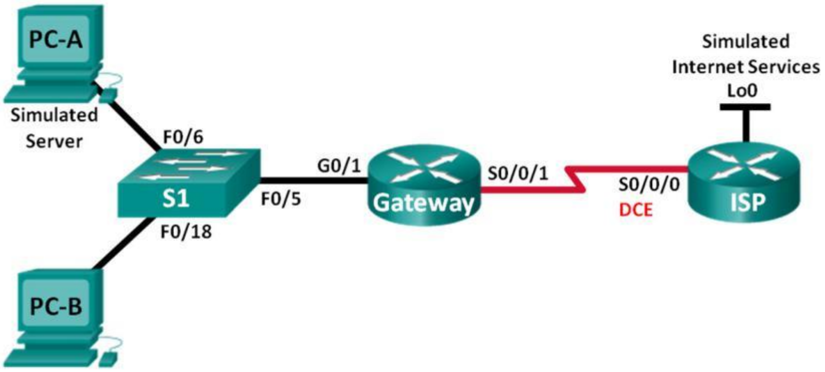
permit tcp host 192.168.3.3 host 192.168.1.3 range 22 23 - this will allow any packet which has the source ip address 192.168.3.3 and transport protocol tcp and a destination ip address 192.168.1.3 and the range of destination port numbers allowed are 22 and 23.

c. How do you apply an ACL with number 199 at an interface G0/0 for incoming direction?

```
R1(config)# interface G0/0
R1(config-if) # ip access-group 199 in
```

Part 3: Network Address Translation (NAT)

a. **Static NAT**



See topology. Check the gateway router, Gateway router interface S0/0/1 is public IP address 12.5.3.5 / 30 and PC-A IP address is private IP address 10.5.3.5 / 24.

Configure a static NAT source mapping from IP 10.5.3.5 to IP 12.5.3.5 .

```
Gateway(config)# ip nat inside source static 10.5.3.5 12.5.3.5
```

Explain why this NAT solution does not solve NAT for all hosts in the private network.
Because static NAT is just a one-to-one mapping of private addresses to public addresses, and thus if we want to use static NAT an one-to-one mapping must be configured for each host in the private network

b. **Dynamic NAT with *Pooling* IP addresses**

See topology. Now, Gateway router serial interface S0/0/1 has IP address 209.165.201.18.

To map inside IP addresses to an outside IP address pool, an ACL is needed to catch all IP packets with inside IP addresses. Create a standard ACL no 1, which permits all IP packets from the IP source address range 10.5.3.0 / 24.

```
(config)# access-list 1 permit 10.5.3.0 0.0.0.255
```

Which command is used to configure a Dynamic NAT pool named “public_access” with IP addresses ranging from 209.165.200.242/27 to 209.165.200.254/27?

```
(config)# ip nat pool public_access 209.165.200.242 209.165.200.254 netmask
255.255.255.224
```

Which command creates a Dynamic NAT translation to the NAT pool “public_access”, and using the ACL 1 to permit IP addresses?

```
(config)#
ip nat inside source list 1 pool public_access
```

c. **Dynamic NAT with *Port Translation* (NAPT)**

Which command creates a Dynamic NAPT translation to outside interface S0/0/1 of Gateway router, and using the ACL 1 of previous task to permit IP addresses?

```
(config)# ip nat inside source list 1 pool public_access overload
```

Part 4: Point-to-Point Protocol (PPP)

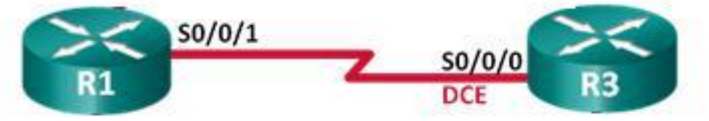
a. **PPP and PAP and CHAP**

What is the default encapsulation on serial links in Cisco routers? HDCL

Which IOS command switches the encapsulation on serial links from HDLC to PPP?

```
(config)# encapsulation ppp
```

Watch the following network. The R1 interface S0/0/1 has the IP address 10.3.3.1/30, and the R3 interface S0/0/0 has the IP address 10.3.3.2/30. The serial links are already up and running.



On R1, how to configure a PPP connection from R1 to R3 with CHAP authentication. Which commands are necessary for PPP configuration including usernames R1, and R3, and common password is **DNPRAK**?

```
(config)#
```

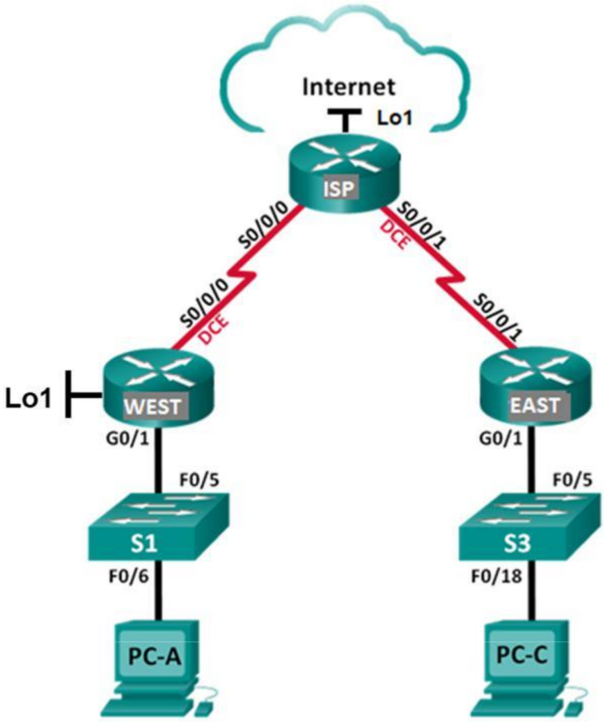
```
R1(config)# int s0/0/1
R1(config-if)# ip address 10.3.3.1 255.255.255.252
R1(config-if)# encapsulation ppp
R1(config-if)# ppp authentication chap
R1(config-if)# no shutdown
R1(config)# username R3 password DNPRAK

R3(config)# int s0/0/0
R3(config-if)# ip address 10.3.3.2 255.255.255.252
R3(config-if)# encapsulation ppp
R3(config-if)# ppp authentication chap
R3(config-if)# no shutdown
R3(config)# username R1 password DNPRAK
```

Describe the benefits of CHAP authentication versus PAP authentication.

CHAP is a stronger authentication method than PAP, because the secret is not transmitted over the link, and because it provides protection against repeated attacks during the life of the link. As a result, if both PAP and CHAP authentication are enabled, CHAP authentication is always performed first.

Task 1 – Network Address and Port Translation (NAPT)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	209.165.201.18	255.255.255.252	N/A
	Lo1 (simulated Webserver1)	10.0.1.1	255.255.255.0	N/A
ISP	Lo1 (simulated Webserver2)	209.165.200.225	255.255.255.224	N/A
	S0/0/0	209.165.201.17	255.255.255.252	N/A
	S0/0/1	209.165.203.21	255.255.255.252	N/A
EAST	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	209.165.203.22	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Note: Depending on the slot for the NIM-2T module, **serial interface names** will be different at the router in the lab.

Part 1: Build the Switched Network and Verify Connectivity

Step 1: Build the Topology.

a. Cable the network as shown in the topology.

b. Record the interfaces numbers in your local topology.

Step 2: Basic settings for each router.

a. Disable DNS lookup.

b. Configure the device name.

c. Assign **class** as the encrypted privileged EXEC mode password.

d. Assign **cisco** as console password, set console logging to synchronous mode, enable login.

e. Assign **cisco** as vty password, and enable login.

f. Encrypt plain text passwords.

Step 3: Ethernet and Serial Interface at each routers WEST, EAST, and ISP

a. Configure the Ethernet interfaces according to the Addressing Table and switch on the interfaces.

b. Configure the Serial interfaces according to the Addressing Table
- Set the clock rate for all DCE serial interfaces to **2 MHz,**
- (DCE or DTE V.35 interface mode can be checked by **show controllers serial <x/y/z>**)
- and switch-on interfaces.
Note: Depending on how you implemented the serial cable, DCE location may be flipped.

Step 4: Start Web Servers on router ISP and WEST with local user database.

a. Create a local user named **webuser** with an encrypted password of **webpass**.

```
ISP(config)# username webuser privilege 15 secret 0 webpass
```

b. Enable the HTTP server service on ISP and use the local user database.

```
ISP(config)# ip http server not successful in cisco pkt
ISP(config)# ip http authentication local not successful
```

```
for this reason, two separate web servers have configured
```

c. Repeat these steps with router WEST.

Step 5: Configure Default Routes at Router WEST and EAST

a. Create a static default route at router WEST using serial interface s0/0/0.

b. Create a static default route at router EAST using serial interface s0/0/1.

Step 6: Verify end-to-end connectivity.

a. Test connectivity by a ping from router WEST to Router ISP serial interface. Connectivity (y/n)? yes

b. Test connectivity by a ping from router WEST to Router EAST serial interface. Connectivity (y/n)?

yes

c. **Note**: Troubleshoot, if connectivity is not successful.

Part 2: Prepare for NAPT

Step 1: Configure the PC Hosts

Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 2: Verify LAN connectivity.

a. Test connectivity by a ping from PC-A to its default gateway. Successful (y/n)? yes

b. Try to ping Router EAST from PC-A. Why is it not working? no
Because there is no route configured in router ISP
Type escape sequence to abort.

Part 3: Dynamic NAPT for PC-A LAN

Step 1: Define an ACL that matches the LAN private IP addresses.

On router WEST, a standard ACL is used to allow the 192.168.1.0/24 network to be translated for NAT. Which command is required to define this ACL?

```
WEST(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 2: Define the NAT translation from inside source list to router outside interface.

To create an overload of mapped connections to one address plus port translation, the key word “overload” in the NAT translation rule is used.

```
WEST(config)# ip nat inside source list 1 interface s0/1/0 overload
```

Step 3: Specify inside and outside interfaces.

PC1- LAN private IP addresses must be translated to a routable public IP address at router WEST. Issue the **ip nat inside** and **ip nat outside** commands to the correct interfaces.

Which interface is **ip nat inside**? interface g0/0/0

Which interface is **ip nat outside**? interface s0/1/0

Check NAT statistics (**show ip nat statistics**). Interface states correct (y/n)? yes

Step 4: Test the configuration.

a. From PC-A, ping the Webserver2. If the ping was unsuccessful, troubleshoot. it was successful

On the WEST router, display the NAT translation table (**show ip nat translation)**. Record the **inside local socket** mapped to **inside global**:

```
WEST#sh ip nat translation
      Pro Inside global Inside local Outside local Outside global
      icmp 209.165.201.18:5 192.168.1.3:5 209.165.200.225:5 209.165.200.225:5
      icmp 209.165.201.18:6 192.168.1.3:6 209.165.200.225:6 209.165.200.225:6
      icmp 209.165.201.18:7 192.168.1.3:7 209.165.200.225:7 209.165.200.225:7
       icmp 209.165.201.18:8 192.168.1.3:8 209.165.200.225:8 209.165.200.225:8
```

Why was a port number added to the translation entry, although ICMP does not use port numbers.?
Port numbers are used to uniquely identify each request (not device) that makes use of the service because a single device may have multiple requests and hence same IP.

b. From PC-C, ping the Webserver2. Why is the ping not successful?
Because of NAT. There is no address translation used therefore it will be unsuccessful.

Step 5: Verify the NAT overload configuration and NAT statistics.

a. Clear the NAT translations and statistics.

```
WEST# clear ip nat translation*

WEST# clear ip nat statistics
```

b. From PC-A, create a Telnet connection to the ISP router, serial interface s0/0/0, and display the NAT table on the WEST router. Record the inside local socket mapped to inside global:

```
WEST#sh ip nat translation
     Pro Inside global Inside local Outside local Outside global
     tcp 209.165.201.18:1025192.168.1.3:1025 209.165.201.17:22 209.165.201.17:22
     tcp 209.165.201.18:1026192.168.1.3:1026 209.165.201.17:22 209.165.201.17:22
     tcp 209.165.201.18:1027192.168.1.3:1027 209.165.201.17:22 209.165.201.17:22
```

Which protocol and ports were used in this translation?
tcp , port number 1025 ,1026,1027

c. From PC-A, open a browser and enter the IP address of Webserver2. Display the NAT table. Record protocol and Port used in this translation?
tcp.

Inside local: 192. 168.1.3:1028 Inside global: 209.165.201.18:1028

Outside local: 209.165.200.225:80 Outside global: 209.165.200.225:80

d. Display the NAT statistics and NAT table.

```
WEST# show ip nat statistics
```

How many active translations do you have? Total translations: 3 (0 static, 3 dynamic, 3 extended)

Part 4: Dynamic NAPT for PC-C LAN

Step 1: Create NAT translation in router EAST

a. Create Standard ACL for router EAST

```
EAST(config)# access-list 1 permit 192.168.3.0 0.0.0.255
```

b. Define the NAT translation from inside source list to router outside interface.

```
EAST(config)# ip nat inside source list 1 interface s0/1/0 overload
```

c. Specify and configure inside and outside interfaces.

d. Check NAT statistics (**show ip nat statistics**). Interface states correct (y/n)? yes

Step 2: Test the configuration.

a. From PC-C, ping the Webserver2

On the Gateway router, display the NAT translation table (**show ip nat translation)**. Record the **inside local socket** mapped to **inside global**:

192.168.3.3:33 to 209.165.203.22:33

b. From PC-C, ping router WEST serial interface. Successful (y/n)? yes

c. Is a ping from PC-C to PC-A working now? Explain, why this still does not work. No it doesn`t work.

Reflection

1. Name advantages, which are given by NAT/NAPT.
1.Reuse of private IP addresses.
2.Enhancing security for private networks by keeping internal addressing private from the external network.
3.Connecting a large number of hosts to the global Internet using a smaller number of public (external) IP address

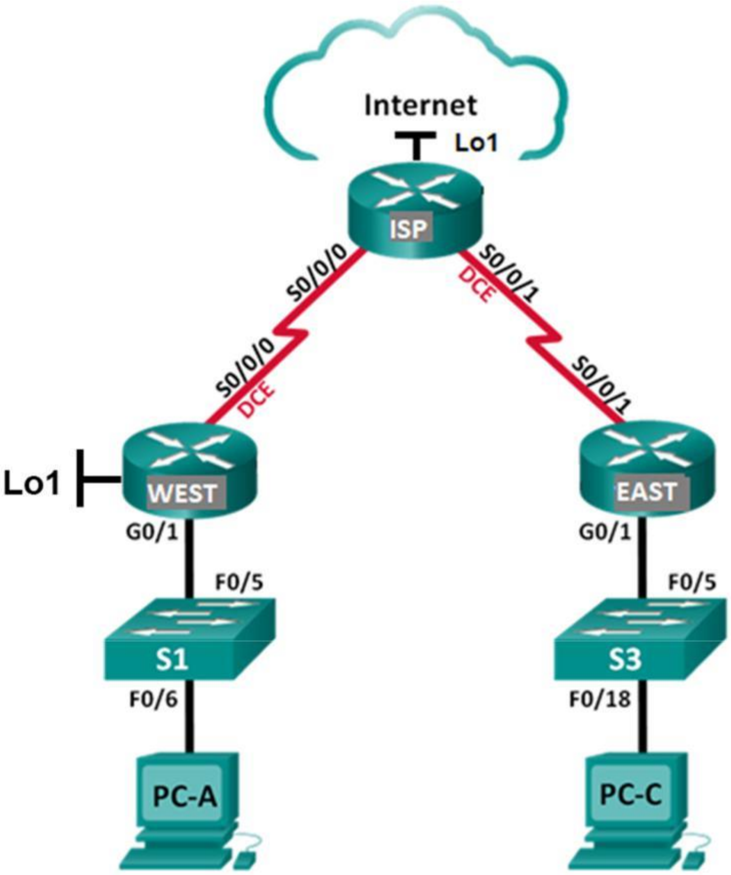
2. Why do we need port numbers in NAT translations?

We need port numbers because many local hosts with private IP addresses can be translated to a single public IP address and also many applications issued by a single host can be also translated to a single public IP address by using different port numbers. Thus each host and each application will not interfere with each other.

3. What are limitations of NAT?
It increases the delay of transaction between packets. End-to-end connectivity is lost.
TCP connections can be interrupted

Task 2 – Securing Networks with ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	209.165.201.18	255.255.255.252	N/A
	Lo1 (simulated Webserver1)	10.0.1.1	255.255.255.0	N/A
ISP	Lo1 (simulated Webserver2)	209.165.200.225	255.255.255.224	N/A
	S0/0/0	209.165.201.17	255.255.255.252	N/A
	S0/0/1	209.165.203.21	255.255.255.252	N/A
EAST	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	209.165.203.22	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Note: Proceed with the Topology and Addressing Table of Task 1

Part 1: Extended Numbered ACLs

Extended ACLs can filter traffic in many different ways. Extended ACLs can filter on source IP addresses, source ports, destination IP addresses, destination ports, as well as various protocols and services.

Step 1: Required Security Policies

Looking at the security policies listed, you will need at least two ACLs on two routers to fulfill the security policies.

Note: A best practice is to place Extended ACLs as close to the source as possible.

1. Allow **web traffic (http only)** originating from the **192.168.1.0/24 network** to go to any network. This rule must be implemented on which router? West
2. From PC-A, allow only a **Telnet** connection to serial interface S0/0/1 of router EAST. This rule must be implemented on which router? West
3. Allow **web traffic (http only)** originating from the **192.168.3.0/24 network** to access only the host of WebServer2. The 192.168.3.0/24 network should NOT be allowed to access any other network via the web. This rule must be implemented on which router? East

Step 2: Configure one numbered extended ACL for security policies 1 and 2.

a. Which router must be configured? West

b. Which filtering interface must be selected for our tasks? g0/0/0

c. In which direction is this ACL to be applied? inside to outside

d. What number range for extended ACLs maybe used? <100-199>

e. Configure the ACL. Use 100 for the ACL number.

To understand your ACL, set remarks, which work like inline comments in software coding.

```
(config)# access-list 100 remark Allow Web & Telnet Access
```

Which command must be used for **security policy 1**?

```
(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
```

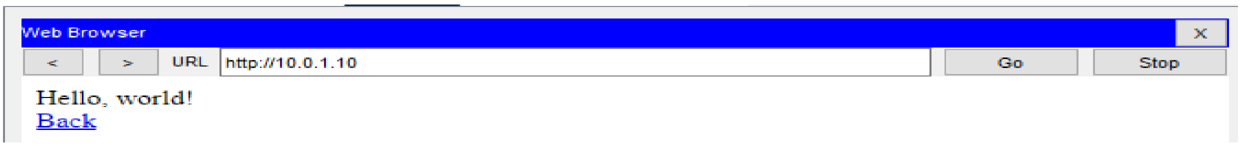
Which command must be used for **security policy 2**?

```
(config)# access-list 100 permit tcp host 192.168.1.3 host 209.165.203.22 eq 23
```

f. Configure ACL 100 and Apply ACL 100 to the correct interface.
WEST, g0/0/0 in

Step 3: Verify ACL 100.

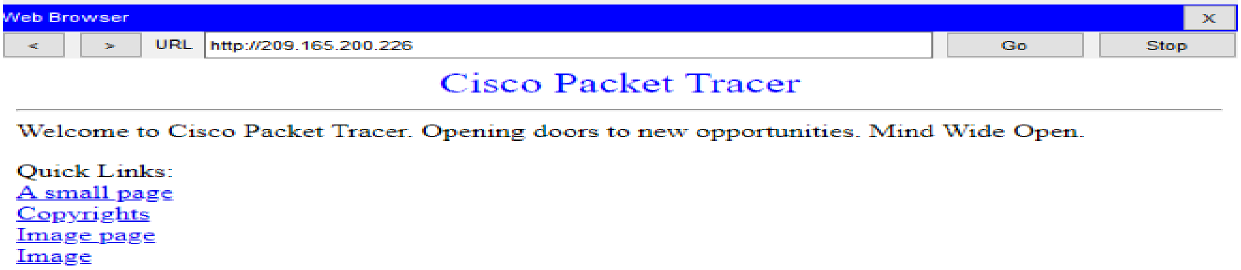
a. Open up a web browser on PC-A, and access WebServer1 http://10.0.1.1. It should be successful; troubleshoot, if not. **the webserver1 is configured with 10.0.1.10**



http://10.0.1.10

Hello, world!
Back

b. Open up a web browser on PC-A, and access WebServer2 http://209.165.200.225. It should be successful; troubleshoot, if not. **the webserver2 is configured with 209.165.200.226**



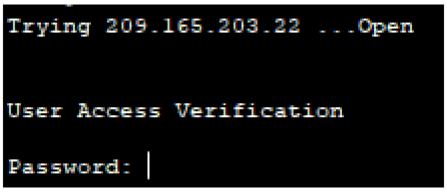
http://209.165.200.226

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

c. Establish a Telnet connection from PC-A to router EAST using the destination IP address of EAST serial interface S0/0/1. It should be successful; troubleshoot, if not. **yes**



```
Trying 209.165.203.22 ...Open


User Access Verification

Password:
```

d. Establish a Telnet connection from PC-A to router ISP, any IP address. It should fail; troubleshoot, if not.

d. From privileged EXEC mode prompt on WEST, issue the **show access-lists**

command. How many ACLs are active? 2 access-lists.

Is there any explicit **deny any any**? Discuss why or why not? No its not, because we didn`t write that when configuring the access list

e. From the PC-A command prompt, issue a ping to IP address of WebServer2. Explain your results.
it has to be destination unreachable. This is because we filtered the traffic now and ping is an icmp message and only web traffic and telnet traffic are allowed. Thus ping is not allowed or does not pass through g0/0/0. but showing successful.

Part 2: Extended Named ACLs

Step 1: Configure a named extended ACL

a. Configure the security policy 3. on router EAST. The name of the ACL is WEB-POLICY.

```
(config)# ip access-list extended WEB-POLICY
```

Which command must be used for security policy 3, to allow web access from network 192.168.3.0/24?

```
(config-ext-nacl)#permit tcp 192.168.3.0 0.0.0.255 host 209.165.200.226 eq 80
```

Is it necessary to explicitly block web traffic to other networks? No

b. Apply ACL WEB-POLICY to the **correct interface** and in **correct direction** on router EAST.

Step 2: Verify Named ACL WEB-POLICY.

a. Open a web browser on PC-C and access the WebServer2 (http://209.165.200.226).
It should be successful; troubleshoot, if not. It is successful

b. From PC-C access the WebServer1 (http://10.0.1.1).
unsuccessful

It should fail, troubleshoot, if not.

c. At router EAST command prompt use the **show ip interface g0/…** command for the active Ethernet interface. What information of ACLs is listed in this context?

```
EAST# sh access-lists
        Standard IP access list 1
        10 permit 192.168.3.0 0.0.0.255 (28 match(es))
        Extended IP access list WEB-POLICY
        10 permit tcp 192.168.3.0 0.0.0.255 host 209.165.200.225 eq www
```

d. From a PC-C command prompt, ping PC-A. This should fail. Explain why. There are 2 reasons for it.
It failed. Destination host unreachable.
because on both routers West and East there are access-lists that prevent these two hosts from communicating with each other

Part 3: Modify and Verify Extended ACLs

Because of the ACLs applied on router WEST and EAST, no pings or any other kind of traffic is allowed from PC-A LAN or PC-C LAN.

Management has decided that ICMP echo request and echo reply traffic between PC-A LAN and WebServer1 LAN should be allowed. You must modify the ACL on router WEST.

Step 1: Modify ACL 100 on router WEST.

PPP From WEST privileged EXEC mode, issue the **show access-lists** command. Check the line numbers in this access list! How many lines are there? 2 lines (one was extra)

a. Enter global configuration mode and modify the ACL on WEST.

```
WEST(config)# ip access-list extended 100
WEST(config-ext-nacl)# 30 permit icmp 192.168.1.0
0.0.0.255
                                          10.0.1.0 0.0.0.255 echo
WEST(config-ext-nacl)# 40 permit icmp 192.168.1.0 0.0.0.255
                                          10.0.1.0 0.0.0.255 echo-reply
WEST(config-ext-nacl)# end
```

Explain, which effect this changes will have: now we are allowed to ping from PC A and send echo replies from PC A lan to 10.0.1.0 lan

c. Issue the **show access-lists** command.

Where did the new line that you just added appear in ACL 100?

```
WEST#sh access-lists
Standard IP access list 1
10 permit 192.168.1.0 0.0.0.255 (34 match(es))
Extended IP access list 100
10 permit tcp 192.168.1.0 0.0.0.255 any eq www
20 permit tcp host 192.168.1.3 host 209.165.203.22 eq telnet
30 permit icmp 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255 echo
40 permit icmp 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255 echo-reply
```

Step 2: Verify modified ACLs.

a. From PC-A, ping WebServer1. Were the pings successful (y/n)? yes It should be successful; troubleshoot, if not.

b. From PC-A, ping router WebServer2. It should fail; troubleshoot, if not. it's showing successful

c. Why did the ACLs work immediately for the ICMP messages, when you changed it?
because the access lists are already linked to the West router interface and the changes are directly saved and applied.

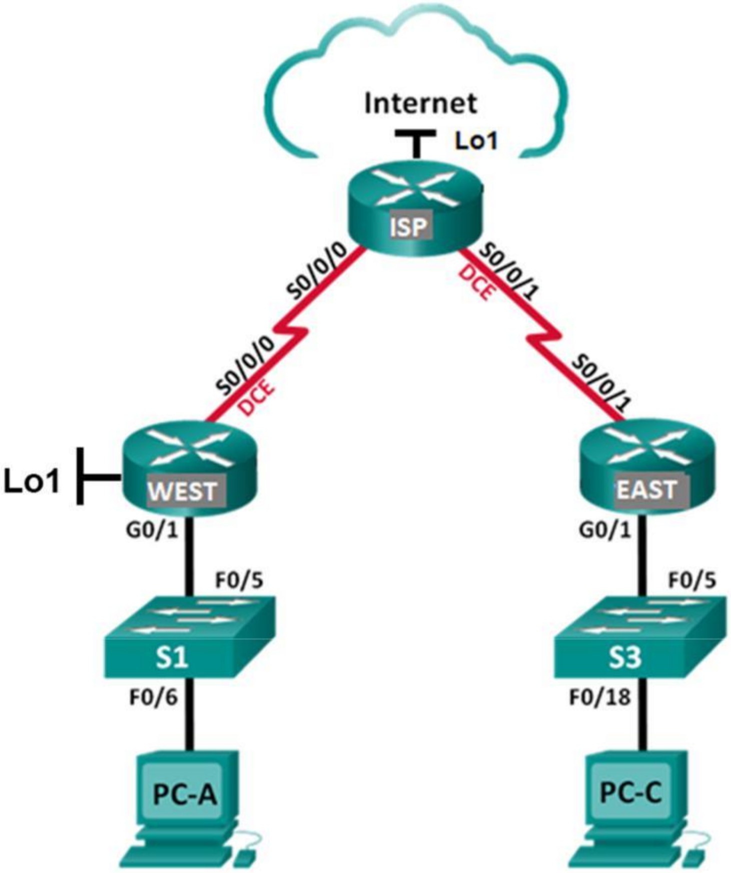
d. For which action would you need line 40 in ACL 100?
to respond to any ping request

Reflection

1. Why is it required to plan and test ACLs carefully and precise?
 Because if not done right there will be no connectivity and for example the access lists must be applied in the right order so we don`t deny connectivity to other routers or hosts
2. Which advantages are given by Standard ACLs?
 We can filter traffic based on source networks and hosts. They are easier to implement than extended access-lists
3. Which advantages are given by Extended ACLs?
 The ability to filter packets based on source address, destination address, protocol and port number. This gives greater flexibility to the system administrator in designing the network

Task 3 – WAN – PPP Connections

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	209.165.201.18	255.255.255.252	N/A
	Lo1 (simulated Webserver1)	10.0.1.1	255.255.255.0	N/A
ISP	Lo1 (simulated Webserver2)	209.165.200.225	255.255.255.224	N/A
	S0/0/0	209.165.201.17	255.255.255.252	N/A
	S0/0/1	209.165.203.21	255.255.255.252	N/A
EAST	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	209.165.203.22	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Note: Proceed with the Topology and Addressing Table of Task 1

Part 1: PPP Encapsulation

Step 1: Display the default serial encapsulation.

On router WEST, issue **show interfaces serial** *interface-id* to display the current serial encapsulation.

Record is the default serial encapsulation for a Cisco router: HDLC

Record the default MTU size for this interface: 1500 bytes

Step 2: Change the serial encapsulation to PPP.

a. At router WEST change the encapsulation of the serial interface s0/0/0 from HDLC to PPP without authentication.

Record the line status and line protocol for the serial interface (show ip interface brief): Why did the status of the interface change? Encapsulation PPP
because it's a different encapsulation on ISP router

b. Change the encapsulation from HDLC to PPP without authentication at serial interface S0/0/0 of router ISP. Check the serial interface S0/0/0 on router ISP with **show interfaces s0/0/0**.

b. Which PPP protocols are running? Encapsulation PPP

c. Check connectivity from router WEST to Router ISP serial interface. Connectivity (y/n)? no

Step 3: Inspect PPP connection establishment

a. Prepare PPP between router ISP and router EAST. Configure the interface S0/0/1 of ISP for PPP encapsulation.

b. Prepare PPP encapsulation at router EAST. Configure the interface S0/0/1 of EAST for PPP encapsulation.

- Test connectivity by pinging ISP router. Connectivity (y/n)? yes

Step 4: Phases of PPP connections.

a. At router EAST issue the **debug ppp** commands at the command prompt of router EAST to observe the process, which is associated with authentication.

```
EAST# debug ppp negotiation
PPP protocol negotiation debugging is on
EAST# debug ppp packet
PPP packet display debugging is on
```

You will observe the debug PPP messages when traffic is flowing on the serial link.

b. Break the serial connection by returning the encapsulation to HDLC for interface s0/0/1 at the EAST router (**encapsulation hdlc**)

The serial connection to ISP has terminated, and the line protocol is down. (**sh ip int brief**)

The route to 209.165.201.16/30 and the static default route has been changed in the routing table. (**sh ip route**).

Does the PPP protocol stop trying to establish a PPP connection?

c. Observe the debug PPP messages as routers ISP and EAST re-establish a connection. Switch encapsulation to PPP again (**encapsulation PPP**).

Issue the **undebug all** (or **u all**) command at the command prompt of router EAST to turn off all debugging.

From the PPP debug messages, what phases did router EAST go through before the link is up with router ISP? there are continuous debug messages
Record the final PPP state:

```
Serial0/1/1 PPP: Phase is FORWARDING, Attempting Forward
Serial0/1/1 Phase is ESTABLISHING, Finish LCP
Serial0/1/1 Phase is UP
```

Part 2: PPP CHAP Authentication

Step 1: Configure PPP CHAP authentication between router ISP and EAST.

a. Following your homework prepare CHAP authentication on EAST.

- On router EAST configure a username **ISP** and password **cisco** for CHAP authentication.
- Configure the interface S0/0/1 on router EAST for CHAP authentication.

b. On router EAST start PPP debugging again to observe the process, which is associated with authentication.

```
EAST# debug ppp negotiation

EAST# debug ppp packet
```

c. On router ISP configure a username **EAST** and password **cisco** for CHAP authentication and configure the interface S0/0/1 on router ISP for CHAP authentication

d. Examine the debug PPP messages on router EAST during the negotiation with the ISP router.

When the link is up again, issue the **undebug all** (or **u all**) command on router EAST to turn off all debugging.

From the PPP debug messages, what phases did the EAST router go through before the link is up with the ISP router?

```
Serial0/1/1 PPP: I pkt type 0xc223, datagramsize 104
Serial0/1/1 PPP: O pkt type 0xc223, datagramsize 104
Serial0/1/1 PPP: I pkt type 0xc223, datagramsize 104
Serial0/1/1 IPCP: I CONFREQ [REQsent] id 1 len 10
Serial0/1/1 IPCP: O CONFACK [REQsent] id 1 len 10
```

Deliverables and Due Dates

Lab Teams

- This lab may be solved in teams of max. 2 students.
- Teams are grouped into 2 groups, which have different due dates and labs on site.

Module Group Exams

- Each team member must solve the requested **Module Group Exams** at least once **before** the lab date.

Lab Check

Before you start the lab work:

- Each participant prints these lab instructions to enter your **Homework / Lab Preparation** solution in advance and to complete answers during the lab work.
- All teams have to present and explain your **Homework / Lab Preparation** solution at of your lab date.

At the end of the lab:

- Each team presents the **Lab Solution** to the instructor and answers questions on topics of the lab.

Checkout

When your lab has been evaluated, clear your workplace.

1. Erase startup-configuration on routers and switches.

```
Routers# erase startup-config

Switches# delete vlan.dat

Switches# erase startup-config
```

2. Remove cabling in your lab.
3. If you are the last team this day, switch-off your PCs.

Due Dates

Group 1	Teams 1-10	Due Date
	ENSA Module Exams 1 – 2 **ENSA Module Exams 3 – 5** **ENSA Module Exams 6 – 8**	**Tuesday 31.5. – EOB**
	ENSA Lab2	**Wednesday 1.6. – 16:45**

Group 2	Teams 1-10	Due Date
	ENSA Module Exams 1 – 2 **ENSA Module Exams 3 – 5** **ENSA Module Exams 6 – 8**	**Tuesday 7.6. – EOB**
	ENSA Lab2	**Wednesday 8.6. – 16:45**