

CCNA ENSA

Lab 2

Team-No.:

Names: AKINSEYE FELIX SIMIDELE
ABIKOYE EMMANUEL

ENSA Module Group Exams

3 Network Security Concepts

4-5 ACL Concepts and ACL Configuration

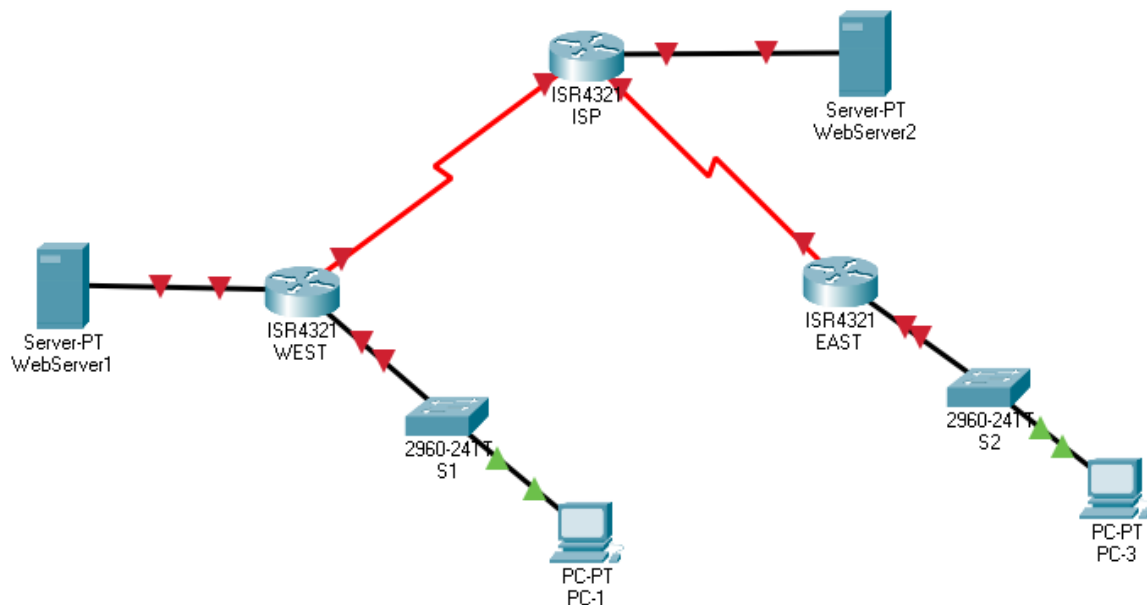
6 NAT for IPv4

7 WAN – PPP Connections

Network Address and Port Translation (NAPT)

Securing Networks with ACLs

WAN – PPP Connections



Homework

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?

1. The source IP address is permitted
2. Or the source IP address is denied

- 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
```

This allow icmp reply from any source ip address to the hosts inside the network address 192.168.10.0 with a subnet mask 255.255.255.0

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

This access list permit http traffic response from any source ip address to hosts inside the network address 192.168.10.0 with a subnet mask 255.255.255.0

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

This access list permit http encrypted(https) traffic response from any source address to hosts inside the network address 192.168.10.0 with a subnet mask 255.255.255.0

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

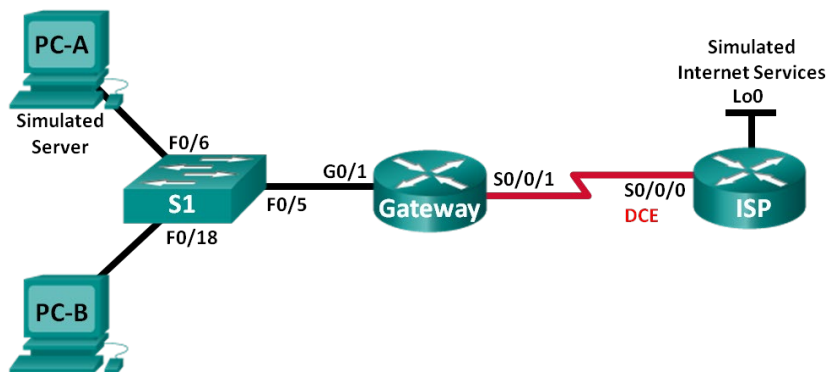
This access list permit 192.168.3.3 to send or have access to host 192.168.1.3 via telnet and ssh

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

```
R1 (config) # interface g0/0  
            # 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 since we have large number of ip addresses in the private network. It is almost impossible to match every host in a large network to global ip addresses because it will lead to depletion of the global ip addresses, and besides, it is very expensive to implement.

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

Which command creates a Dynamic NAT 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 interface gigabitEthernet 0/1 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?

Cisco HDLC is the default encapsulation types for serial links interfaces

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)#
```

```
(config)# int s0/0/1
```

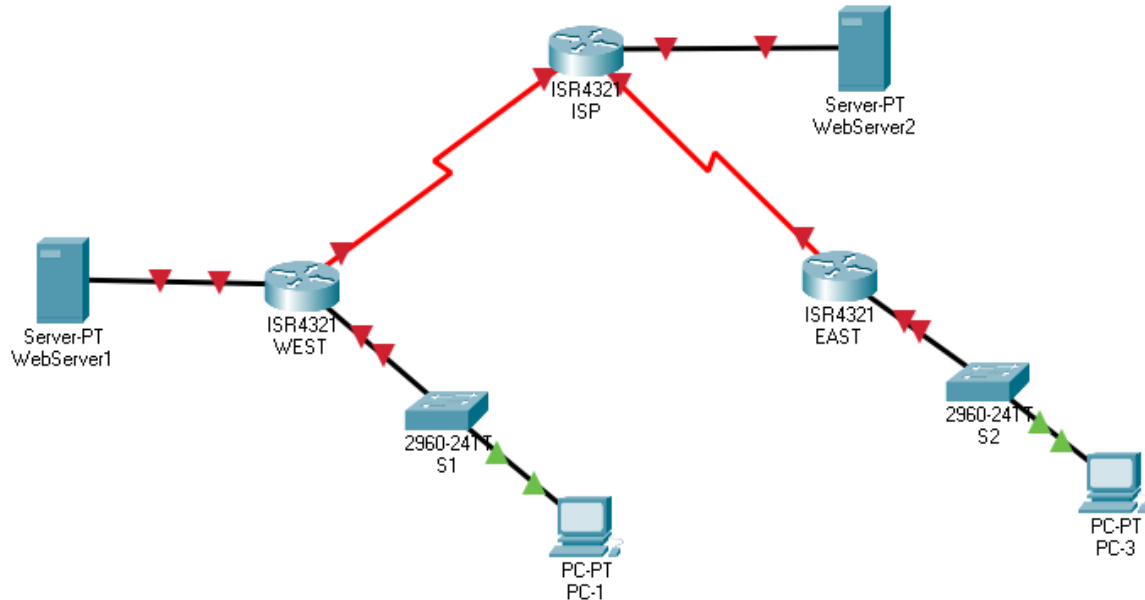
```
config)# interface s0/0/1
config-if)# encapsulation ppp
config-if)# exit
config)# username R1 password DNPRAK
config)# interface s0/0/1
config-if)# ppp authentication chap
```

Describe the benefits of CHAP authentication versus PAP authentication.

1. Encrypted username and password are usually transmitted in CHAP, but they transmitted in clear text in PAP
2. CHAP can do repeated middle session authentications, whereas, PAP cannot do.
3. Only the username is transmitted through the link in CHAP, but both username and password through the link in PAP
4. Authentication is done on both sides in CHAP. but in PAP, authentication is done only at the source side.
5. CHAP is more secured because the actual password is never transmitted through the link, but in PAP, password is transmitted without encryption.

Task 1 – Network Address and Port Translation (NAPT)

Topology



Addressing Table



| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|------------|-----------|-----------------|-----------------|-----------------|
| WEST | G0/0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| | G0/0/1 | 10.0.1.1 | 255.255.255.0 | N/A |
| | S0/1/0 | 209.165.201.18 | 255.255.255.252 | N/A |
| ISP | G0/0/0 | 209.165.200.225 | 255.255.255.224 | N/A |
| | S0/1/0 | 209.165.201.17 | 255.255.255.252 | N/A |
| | S0/1/1 | 209.165.203.21 | 255.255.255.252 | N/A |
| EAST | G0/0/0 | 192.168.3.1 | 255.255.255.0 | N/A |
| | S0/1/0 | 209.165.203.22 | 255.255.255.252 | N/A |
| PC-1 | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-3 | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 |
| WebServer1 | NIC | 10.0.1.10 | 255.255.255.0 | 10.0.1.1 |
| WebServer2 | NIC | 209.165.200.226 | 255.255.255.224 | 209.165.200.225 |

Note: Depending on the slot in which you implemented the NIM-2T module, serial interface names may be different.

Part 1: Build the Switched Network and Verify Connectivity

Step 1: Build topology in Packet Tracer.

COVID-19 Version: Build topology in **Packet Tracer**. Use and re-label the following devices:

- Build the network with ISR4321 router, 2960 switches, PCs and Servers in Packet Tracer. Rename the devices.
- Cable the network according to the topology with straight-through TP cables .
- Implement NIM-2T modules at each router, and connect these interfaces by serial cables. .
- We will use the CLI window of the network devices directly for configurations.

Step 2: Basic settings for each router.

- Disable DNS lookup.
- Configure the device name.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as console password, set console logging to synchronous mode, enable login.
- Assign **cisco** as vty password, and enable login.
- Encrypt plain text passwords.

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

- Configure the Ethernet interfaces according to the Addressing Table and switch on the interfaces.
 - 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: Configure Default Routes at Router WEST and EAST

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

Step 5: Verify end-to-end connectivity.

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

Note: Troubleshoot, if connectivity is not successful.

Part 2: Prepare for NAPT

Step 1: Configure the PC Hosts, Webserver1 and Webserver2

Assign IP addresses and default gateways to the PCs and Webserver1 according to the Addressing Table.

Step 2: Verify LAN connectivity.

- Test connectivity by a ping from PC-1 to its default gateway. Successful (y/n)?
- Try to ping Router EAST from PC-1. Why is it not working?

Because static route for PC-1 LAN or OSPF routing has not been enabled or configured on Router WEST.

Part 3: Dynamic NAT for PC-1 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)# config)#access-list 10 remark ACE permits only hosts on network 192.168.1.0/24
config)#access-list 10 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 10 interface g0/0/0 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**? **g0/0/0**

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

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

Step 4: Test the configuration.

- From PC-1, ping the Webserver2. If the ping was unsuccessful, troubleshoot.

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

| Pro | Inside global | Inside local | Outside local | Outside global |
|------|-------------------|----------------|--------------------|--------------------|
| icmp | 209.165.201.18:29 | 192.168.1.3:29 | 209.165.200.226:29 | 209.165.200.226:29 |
| icmp | 209.165.201.18:30 | 192.168.1.3:30 | 209.165.200.226:30 | 209.165.200.226:30 |
| icmp | 209.165.201.18:31 | 192.168.1.3:31 | 209.165.200.226:31 | 209.165.200.226:31 |
| icmp | 209.165.201.18:32 | 192.168.1.3:32 | 209.165.200.226:32 | 209.165.200.226:32 |

Why was a port number added to the translation entry, although ICMP does not use port numbers.?

The port number is used to identify each session

- From PC-3, ping the Webserver2. Why is the ping not successful?

Because NAT has not been configured on Router EAST that is connected to the LAN that PC-3 belongs to.

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

- Clear the NAT translations and statistics.

```
WEST# clear ip nat translation *
(not with PT) WEST# clear ip nat statistics
```

- From PC-1, create a Telnet connection to the ISP serial interface s0/1/0 and display the NAT table on the WEST router. Record the inside local socket mapped to inside global:

to

| Pro | Inside global | Inside local | Outside local | Outside global |
|-----|---------------------|------------------|-------------------|-------------------|
| tcp | 209.165.201.18:1025 | 192.168.1.3:1025 | 209.165.201.17:23 | 209.165.201.17:23 |
| tcp | 209.165.201.18:1026 | 192.168.1.3:1026 | 209.165.201.17:23 | 209.165.201.17:23 |
| tcp | 209.165.201.18:1027 | 192.168.1.3:1027 | 209.165.201.17:23 | 209.165.201.17:23 |

Which protocol and ports were used in this translation?

TCP and port 23

- c. From PC-1, open a browser and enter the IP address of Webserver2. Display the NAT table. Record protocol and Port used in this translation?

Inside local: 192.168.1.3:1028

Inside global: 209.165.201.18:1028

Outside local: 209.165.200.226

Outside global: 209.165.200.226

- d. Display the NAT statistics and NAT table.

WEST# **show ip nat statistics**

How many active translations do you have? 4

```
WEST#show ip nat statistics
Total translations: 4 (0 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: GigabitEthernet0/0/0
Hits: 208 Misses: 69
Expired translations: 28
Dynamic mappings:
```

Part 4: Dynamic NAT for PC-3 LAN

Step 1: Create NAT translation in router EAST

- a. Create Standard ACL for router EAST

```
EAST(config)# access-list 10 remark ACE permits hosts on network 192.168.3.0/24
access-list 10 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 10 interface g0/0/0 overload
```

- c. Specify and configure inside and outside interfaces.

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

Step 2: Test the configuration.

- a. From PC-3, 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**:

to

```
EAST#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 209.165.203.22:13 192.168.3.3:13 209.165.200.226:13 209.165.200.226:13
icmp 209.165.203.22:14 192.168.3.3:14 209.165.200.226:14 209.165.200.226:14
icmp 209.165.203.22:15 192.168.3.3:15 209.165.200.226:15 209.165.200.226:15
icmp 209.165.203.22:16 192.168.3.3:16 209.165.200.226:16 209.165.200.226:16
```

- b. From PC-3, ping router WEST serial interface. Successful (y/n)? Y

- c. Is a ping from PC-3 to PC-1 working now? Explain, why this still does not work.

Because NAT and access control entries have not been configured on Router West that is connected PC-1 LAN to allow traffic from outside to inside of PC-1 LAN

Reflection

1. Name advantages, which are given by NAT/NAPT.

1. NAT/NAPT can be used to conserve private IP addresses given to organizations for the devices on their networks.
2. It provides security within the LAN area by preventing private IP addresses from being seen in other networks.
3. It provides consistency for internal network addressing schemes whereby changes can be made in the public IP addressing schemes without changing the addressing of the private IP addresses.
4. It provides flexibility to public networks.

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

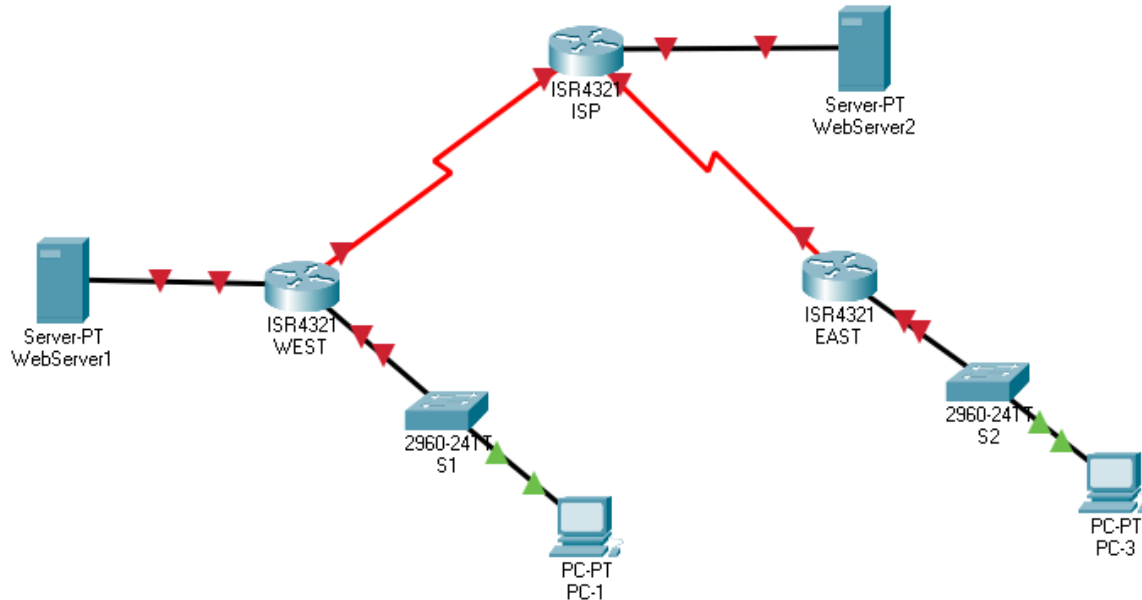
1. To identify sessions in the source and destination hosts
2. Ensures that return packets are delivered to the respective sessions on the host that the requests were sent.
3. It helps provide security by keeping track of sessions so as to prevent man-in-the-middle attack.

3. What are limitations of NAT?

1. NAT increases forward delays because of the translation of the private IP addresses to public IP addresses.
2. It is difficult to trace packets because packets addresses must have undergone several changes before they arrived at their destination.
3. NAT makes tunneling protocol like IPsec to be difficult because changes in the addressing affects the integrity checks of the protocol.
4. Some applications cannot work with NAT because they require end-to-end addressing which is lost in NAT.

Task 2 – Securing Networks with ACLs

Topology



Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|------------|-----------|-----------------|-----------------|-----------------|
| WEST | G0/0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| | G0/0/1 | 10.0.1.1 | 255.255.255.0 | N/A |
| | S0/1/0 | 209.165.201.18 | 255.255.255.252 | N/A |
| ISP | G0/0/0 | 209.165.200.225 | 255.255.255.224 | N/A |
| | S0/1/0 | 209.165.201.17 | 255.255.255.252 | N/A |
| | S0/1/1 | 209.165.203.21 | 255.255.255.252 | N/A |
| EAST | G0/0/0 | 192.168.3.1 | 255.255.255.0 | N/A |
| | S0/1/0 | 209.165.203.22 | 255.255.255.252 | N/A |
| PC-1 | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-3 | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 |
| WebServer1 | NIC | 10.0.1.10 | 255.255.255.0 | 10.0.1.1 |
| WebServer2 | NIC | 209.165.200.226 | 255.255.255.224 | 209.165.200.225 |

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.** We will follow this best practice for these policies.

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? **Router WEST**
2. From PC-1 allow a **Telnet** connection to serial interface S0/1/0 of router EAST.
This rule must be implemented on which router? **Router WEST**
3. Allow **web traffic** (http only) originating from the 192.168.3.0/24 network to access 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? **Router EAST**

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

- a. Which router must be configured? **Router WEST**
- b. Which filtering interface must be selected for our tasks? **GigabitEthernet 0/0/0**
- c. What number range for extended ACLs maybe used? **100-199**
- d. 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 www
```

Which command must be used for security policy 2?

```
(config)# access-list 100 permit tcp 192.168.1.3 0.0.0.0 209.165.203.22 0.0.0.3 eq 23
```

ACL 100 shall be applied in which direction on the interface of your choice?

```
config)# interface g0/0/0  
config-if)# ip access-group 100 in
```

- e. Configure ACL 100 and Apply ACL 100 to the correct interface.

Step 3: Verify ACL 100.

- a. Open up a web browser on PC-1, and access WebServer1 <http://10.0.1.10>. It should be successful; troubleshoot, if not.

First line of HTTP response in browser?

- b. Open up a web browser on PC-1, and access WebServer2 <http://209.165.200.226>. It should be successful; troubleshoot, if not.

First line of HTTP response in browser?

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

First line of response?

```
C:\>telnet 209.165.203.22  
Trying 209.165.203.22...Open
```

User Access Verification

```
Password:  
EAST>en  
Password:  
EAST#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
EAST(config)#exit  
EAST#config t
```

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

How many ACLs are active? **3**

Is there any explicit **deny any any**? Discuss why or why not? **There is no explicit "deny any any" because only access list entries configured will be enabled and automatically**

- e. From the PC-1 command prompt, issue a ping to IP address of WebServer2. Explain your results. **deny other access.**
Because icmp has not been allowed on Router WEST which is connected to PC-1 LAN to any destination IP address

Part 2: Extended Named ACLs

Step 1: Configure a named extended ACL

- a. Configure the task 3.) policy on 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 0.0.0.255 209.165.200.226 0.0.0.31 eq www
```

Is it necessary to explicitly block web traffic to other networks?

No, I do not think it is necessary because the first ACL has permitted hosts on the network to only 209.165.200.226

- b. Configure the security policy of task 3 on router EAST. The name of the ACL is WEB-POLICY.
- c. Apply ACL WEB-POLICY to the **correct interface** on router EAST.

Step 2: Verify Named ACL WEB-POLICY.

- a. From router EAST command prompt, issue the **show ip interface gx/x/x** command for the active Ethernet interface.

What information of ACLs is listed in this context? **Inbound access list is WEB-POLICY**

- b. Open a web browser on PC-3 and access the WebServer2 (<http://209.165.200.226>). It should be successful; troubleshoot, if not.
- c. From a PC-3 command prompt, ping PC-1. This should fail. Explain why. There are 2 reasons for it.
1. ICMP traffic has not been allowed on Router EAST from any host or PC-1 from PC-1 LAN
2. ICMP has not also been permitted into Router WEST from any networks or the network that PC-3 belongs to.

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-1 LAN or PC-3 LAN. Management has decided that ICMP echo request and echo reply traffic between PC-1 LAN and WebServer1 LAN should be allowed. You must modify the ACL on router WEST.

Step 1: Modify ACL 100 on router WEST.

- a. From WEST privileged EXEC mode, issue the **show access-lists** command.

Check the line numbers in this access list! How many lines are there?

```
WEST#show access-lists
Standard IP access list 10
 10 permit 192.168.1.0 0.0.0.255 (2 match(es))
Extended IP access list 100
 10 permit tcp host 192.168.1.3 209.165.203.20 0.0.0.3 eq telnet
 20 permit tcp 192.168.1.0 0.0.0.255 any eq www (12 match(es))
```

- b. 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:

ping request and reply to and from WebServer1 can be sent and received successful

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

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

Step 2: Verify modified ACLs.

- a. From PC-1, ping WebServer1. Were the pings successful (y/n)? **Y**

It should be successful; troubleshoot, if not.

- b. From WebServer1, ping the IP address of PC-1. Were the pings successful (y/n)? **Y**

It should be successful; troubleshoot, if not.

- c. Why did the ACLs work immediately for the ICMP messages, when you changed it?

because the ACL 100 has been applied on the interface g0/0/0 as an inbound interface to outside.

Reflection

1. Why is it required to plan and test ACLs carefully and precise?

Because if a mistake is made during the planning, it may be very difficult to troubleshoot.

2. Which advantages are given by Standard ACLs?

1. It is very easy to implement.

2. Since it checks only the ip address, routing processing is faster than when an extended ACL is configured.

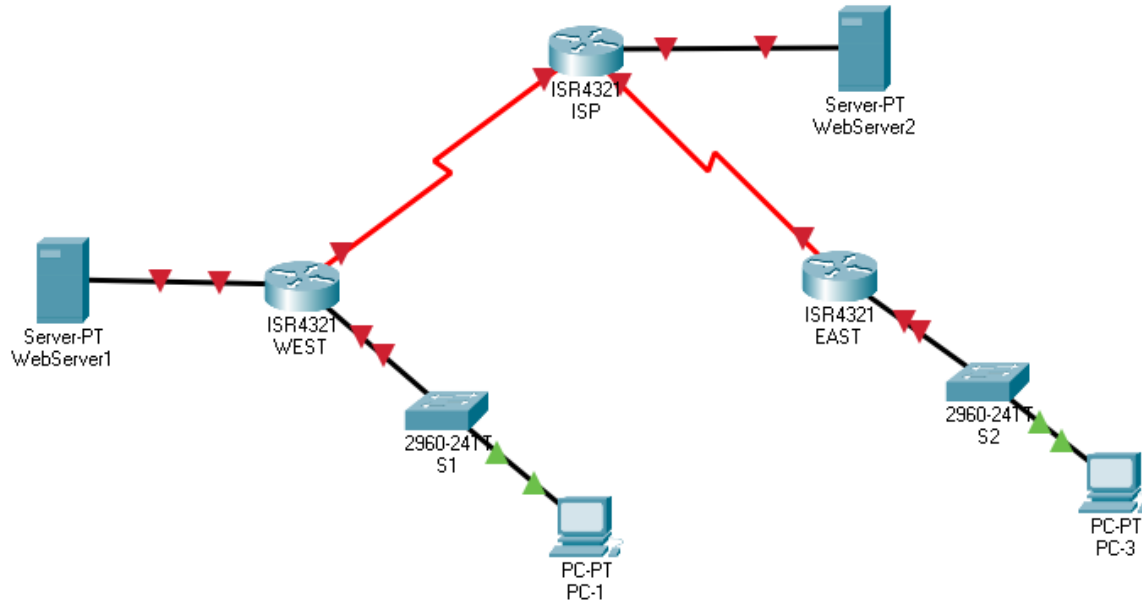
3. Which advantages are given by Extended ACLs?

1. Apart from blocking the Ip addresses, port numbers can also be blocked.

2. Since it is implemented close to the source, there is no need to a SLA with other networks on what to permit or reject into their networks

Task 3 – WAN – PPP Connections

Topology



Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|------------|-----------|-----------------|-----------------|-----------------|
| WEST | G0/0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| | G0/0/1 | 10.0.1.1 | 255.255.255.0 | N/A |
| | S0/1/0 | 209.165.201.18 | 255.255.255.252 | N/A |
| ISP | G0/0/0 | 209.165.200.225 | 255.255.255.224 | N/A |
| | S0/1/0 | 209.165.201.17 | 255.255.255.252 | N/A |
| | S0/1/1 | 209.165.203.21 | 255.255.255.252 | N/A |
| EAST | G0/0/0 | 192.168.3.1 | 255.255.255.0 | N/A |
| | S0/1/0 | 209.165.203.22 | 255.255.255.252 | N/A |
| PC-1 | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-3 | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 |
| WebServer1 | NIC | 10.0.1.10 | 255.255.255.0 | 10.0.1.1 |
| WebServer2 | NIC | 209.165.200.226 | 255.255.255.224 | 209.165.200.225 |

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

Part 1: PPP Encapsulation

Step 1: Change the serial encapsulation to PPP.

- At router WEST change the encapsulation of the serial interface from HDLC to PPP without authentication.

Record the line status and line protocol for the serial interface (**show ip interface brief**)?

Serial0/1/0 209.165.201.18 YES manual up down

Why did the status of the interface change?

Because of encapsulation mismatch since the encapsulation of interface s0/1/0 of Router ISP has not been changed to PPP

- Change the encapsulation from HDLC to PPP without authentication at serial interface S0/1/0 of router ISP.
- Check the serial interface S0/1/0 on router ISP with **show interfaces s0/1/0**.

Which PPP protocols are running? Encapsulation PPP

- Check connectivity from router WEST to Router ISP serial interface. Connectivity (y/n)? Y

Step 2: Inspect PPP connection establishment

- Prepare PPP between router ISP and router EAST.
 - Configure the interface S0/1/1 of ISP for PPP encapsulation.
- Prepare PPP encapsulation at router EAST.
 - Configure the interface S0/1/0 of EAST for PPP encapsulation.
 - Test connectivity by pinging ISP router. Connectivity (y/n)? Y
- At router EAST issue the **debug ppp** commands to observe the process, which is associated with authentication.

EAST# **debug ppp negotiation**

- Examine the debug PPP messages during the PPP negotiation. Break the serial connection by returning the serial encapsulation to HDLC for interface S0/1/0 at the EAST router (**encapsulation hdlc**)

EAST(config-if)#encapsulation hdlc
EAST(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down

Serial0/1/0 PPP: Phase is TERMINATING
Serial0/1/0 LCP: State is Closed
Serial0/1/0 PPP: Phase is DOWN

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

EAST(config-if)#encapsulation ppp
EAST(config-if)#
Serial0/1/0 PPP: Using default call direction
Serial0/1/0 PPP: Treating connection as a dedicated line
Serial0/1/0 PPP: Phase is ESTABLISHING, Active Open
Serial0/1/0 LCP: State is Open
Serial0/1/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/1/0 Phase is ESTABLISHING, Finish LCP
Serial0/1/0 Phase is UP

- Issue the **undebug all** command on 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? Establishing, Forwarding and Up phases

Record the final PPP state. %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Reflection

- What are indicators that you may have a serial encapsulation mismatch on a serial link?
 - Line protocol state changed to DOWN.
 - ping reply cannot be delivered to the interface.
- What are indicators that you may have an authentication mismatch on a serial link?
 - Line protocol state changed to DOWN
 - Phase changed to DOWN

Deliverables

Lab Teams

This lab may be solved in teams of max. 3 students. All teams have to provide their deliverables in time.

Teams are grouped into 2 groups, which have different due dates and presentation dates.

Module Group Exams

Each team member must solve the requested **Module Group Exams** before delivery date.

Deliverables

Each teams delivers the following documents and files:

- One **PDF-File (.pdf)** with the completed **Homework and Instructions**.
All tasks and questions must be answered.
- One **PacketTracer-File (.pkt)** in PacketTracer Version 8 with your **final configuration**.
- One **Text-File in ASCII-Format (.txt, simple Text Editor)** with the **running configurations of Router WEST and Router EAST**.

Due Dates

| Group 1 | Teams 1-10 | Due Date |
|---------|------------------------|------------------|
| | Module Group Exams 3-7 | 30.5.- EOB |
| | Deliverable Upload | 30.5. - EOB |
| | CCNA ZOOM Presentation | 2.6. - 16:45 ff. |

| Group 2 | Teams 11-20 | Due Date |
|---------|------------------------|------------------|
| | Module Group Exams 1-2 | 6.6. - EOB |
| | Deliverable Upload | 6.6. - EOB |
| | CCNA ZOOM Presentation | 9.6. - 16:45 ff. |