What is ACLs

- ACL (Access control list) is a set of rules which allow or deny traffic moving the router.
- It function as a packet filter instructing the router to permit or deny a specific traffic .(also called as Packet Filtering Firewall)
- ACL's can filter traffic based on source/destination IP address, source/destination layer 4 ports etc..
- ACL's are configure globally on the router (global config mode)
- They are an ordered sequence of ACE's (Access control entries) e.g.

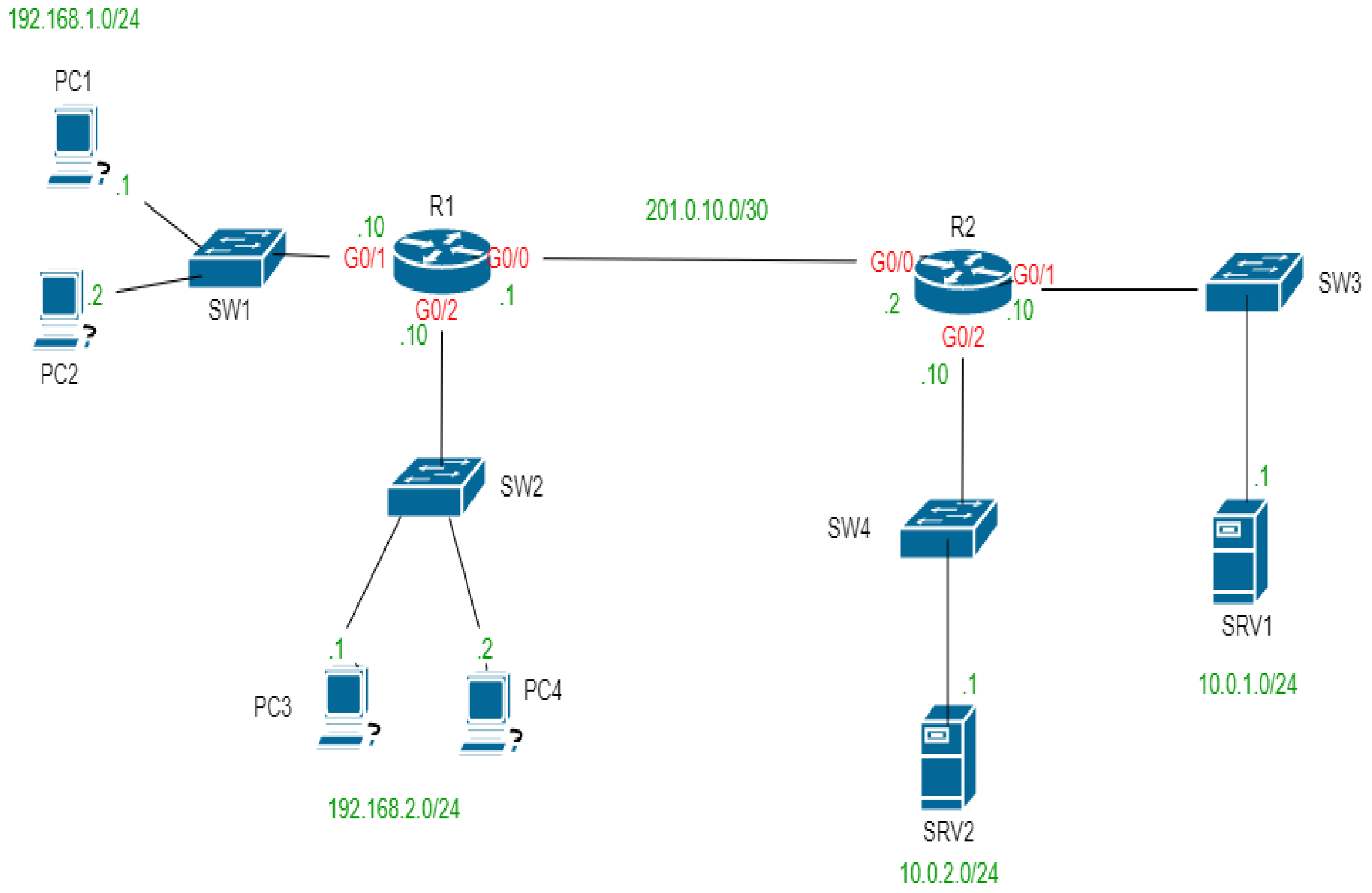
ACL 1

- 1 if source IP = 192.168.1.0/24 then permit
- 2 if source IP = 192.168.2.0/24 then deny
- 3 if source IP =any, then permit

Basic overview of how ACL works

- Configuring an ACL in global config mode will not make the ACL take effect
- After being created the ACC must be applied to an interface
- ACLs are applied either inbound or outbound
- ACLs are made up of one or more ACEs
- When the router check a packet against the ACL, it process the ACEs in order from top to bottom
- If the packet matches one ACE in the ACL the router takes the action and stop processing the ACL. All entries below the matching entry will be ignored.
- ACL support a default implicit deny rule at the end of all ACLs. It tells the router to deny all traffic that doesn’t match any of the configured entries in the ACL
- A maximum of 1 ACL can be applied to a single interface per direction
  - Inbound = Max 1 ACL
  - Outbound = Max 1 ACL

Basic overview of How ACL’s works



- Requirement
  - Host in 192.168.1.0/24 can access the 10.0.1.0/24 network
  - Host in 192.168.2.0/24 cannot access the 10.0.1.0/24 network

Types of Access control list

- There are two types of ACL . These 2 types have 2 sub-type

1. **Standard ACL**:

- Match traffic base on source IP address only.
- Implemented closest to the destination .
- Can permit or block a network, host, subnet
  - Standard Number ACLs: which are identify with a number (number ranges from 1-99 and 1300-1999)
  - Standard Named ACLs : which are identify with a name

2. **Extended ACL** :

- Match traffic base source/destination IP, source/destination port number, protocol, etc
- Implemented closest to the source
- Can allow or deny a network, Host, subnet and service
  - Extended Number ACL : which are identify with a number (number ranges from 100 -199 and 2000 - 2699)
  - Extended Name ACL : which are identify with a name

Standard Number ACL (configurations)

- The basic command to configure a standard number ACL is

```
R1(config)# access-list no {deny/permit} <source ip add>  <wildcard-mask>
```

Examples:

```
R1(config)#access-list 10 deny 192.168.1.1 0.0.0.0
```

(Its denies 192.168.1.1/32. a single host)

OR

```
R1(config)#access-list 10 deny 192.168.1.1
R1(config)#access-list 10 deny host 192.168.1.1
```

```
R1(config)#access-list 10 permit any
```

OR

```
R1(config)#acces-list 10 permit 0.0.0.0 255.255.255.255
```

- **To apply to an interface**

```
R1(config) # ip access-group no {in/out}
```

- **To verify the ACL configuration use the following command**
  - Show access-list
  - Show ip access-list
  - Show run | section access-list   (this display just ACL section on the running –configure)

Standard Named ACL (configurations)

- They are configured by entering “standard named ACL config mode” and the configure each entry within that config mode.

Syntax:

```
R1(config)#ip access-list standard <acl-name>
R1(config-std-nacl)#[entry-no]{deny|permit} <source ip add> <WCM>
```

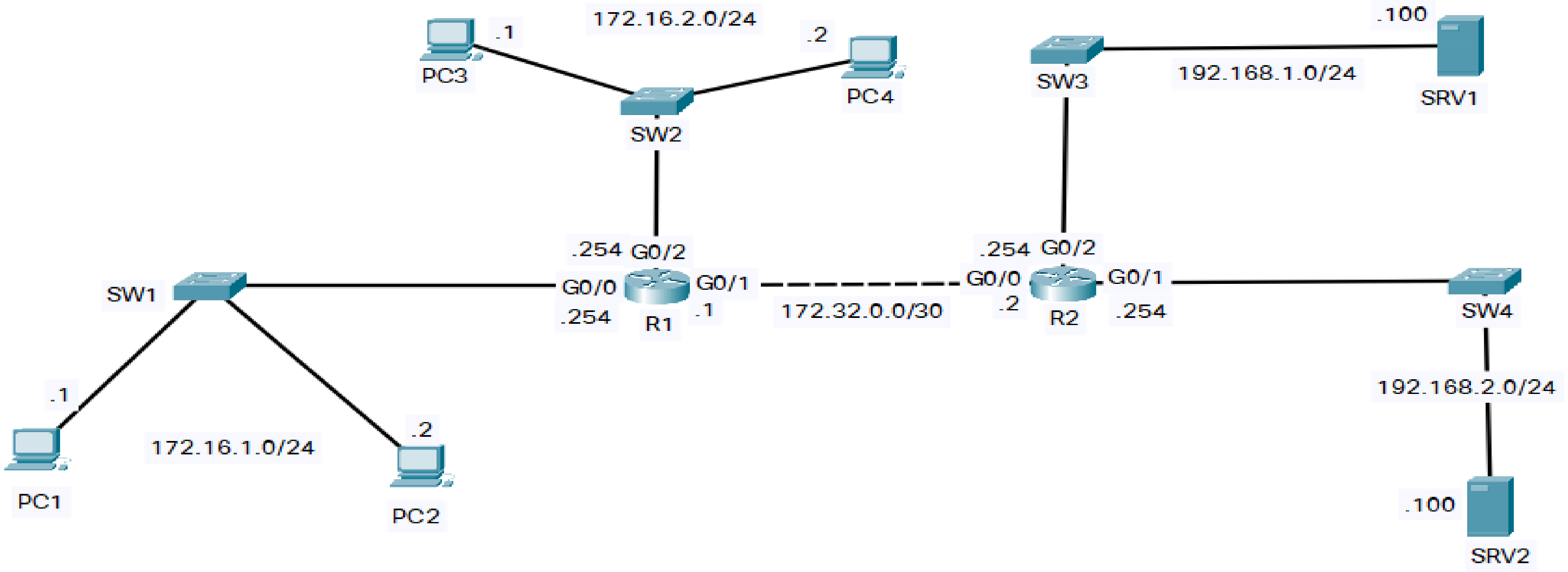
Example:

```
R1(config)#ip access-list standard block_HR
R1(config-std-nacl)#5 deny 192.168.1.0 0.0.0.255
R1(config-std-nacl)#10 permit any
R1(config-std-nacl)#int g0/0
R1(config-if)# ip access-group block_HR in
```

To write ACL statement

- Know which router to implement ACL
- Identify source and Destination
- Specify the direction (In/Out)

Hands-on projects configuring standard ACL



1. configure EIGP on R1 and R2 to allow full connectivity between the PCs and Servers
2. configure standard numbered ACLs on R1 and Standard Named ACLs on R2 to fulfill the following network policies:
   - only PC1 and PC3 can access 192.168.1.0/24
   - Hosts in 172.16.2.0/24 can't access 192.168.2.0/24
   - 172.16.1.0/24 can't access 172.16.2.0/24
   - 172.16.2.0/24 can't access 172.16.1.0/24

Another way to configure numbered ACLs

- We saw that numbered ACLs are configured in global config mode:

```
R1(config)# access-list 1 deny 172.16.1.1
R1(config)# access-list 1 permit any
```

- We also saw that named ACLs are configured in subcommands in a separate config mode:

```
R1(config)# ip access-list standard Block-HR
R1(config-std-nacl)# deny 172.16.1.1
R1(config-std-nacl)# permit any
```

- In modern IOS you can also configure numbered Acls in the exact same ways as named Acls

```
R1(config)# ip access-list standard 1
R1(config-std-nacl)# deny 172.16.1.1
R1(config-std-nacl)# permit any
```

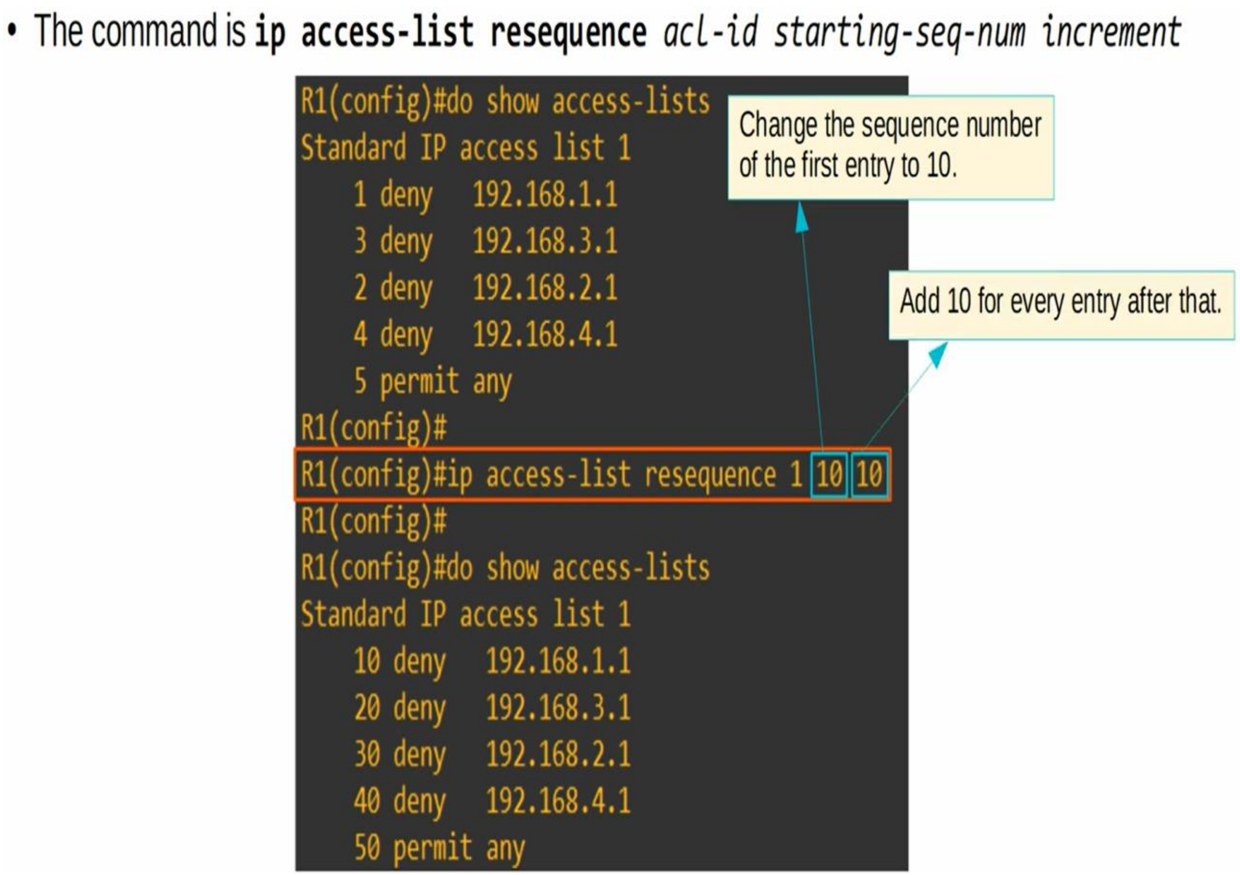
- This is just a different way of configuring numbered Acls.

Advantages of Named ACL config mode

- You can easily delete individual entries in the ACL with “ no entry-number):

R1(config-std-nacl)# no 30

- When configuring /editing numbered ACLs from the global config mode you can’t delete individual entries you can only delete the entire ACL
- You can insert new entries in between other entries by specifying the sequence number
- There is a resequencing function that helps edit ACLs.



- The command is **ip access-list resequence** *acl-id starting-seq-num increment*

```
R1(config)#do show access-lists
Standard IP access list 1
    1 deny   192.168.1.1
    3 deny   192.168.3.1
    2 deny   192.168.2.1
    4 deny   192.168.4.1
    5 permit any
R1(config)#
R1(config)#ip access-list resequence 1 10 10
R1(config)#
R1(config)#do show access-lists
Standard IP access list 1
    10 deny   192.168.1.1
    20 deny   192.168.3.1
    30 deny   192.168.2.1
    40 deny   192.168.4.1
    50 permit any
```

Change the sequence number of the first entry to 10.

Add 10 for every entry after that.

Extended ACLs

- Extended Acls functions mostly the same as standard Acls
- They can be numbered or named .just like standard Acls
- Numbered ACLs use the following ranges , 100-199 and 2000-2699.
- They are processed from top to bottom , just like standard ACLs
- Though, they can traffic based on more parameters, so they are more precise (and more complex) than standard ACLs. For example, layer 4 protocols|ports, source address , destination address and routing protocol

Syntax for Numbers extended Acls

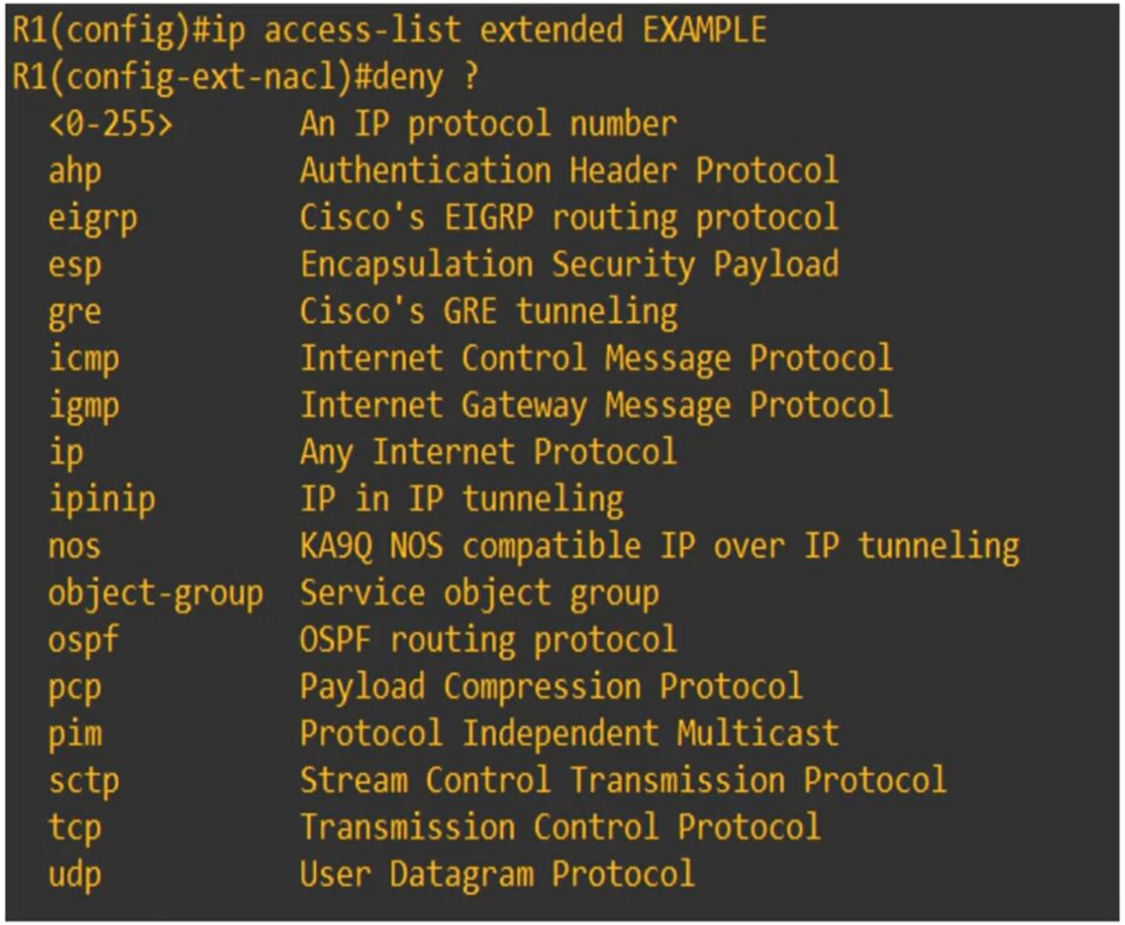
R1(config)#access-list *number*[**permit**|**deny**] *protocol src-ip dest-ip*

Syntax for Named extended Acls

R1(config)#**ip access-list extended** {*name | number*}

R1(config-ext-nacl)[**permit** | **deny**] *protocol src-ip dest-ip*

Matching the protocol



```
R1(config)#ip access-list extended EXAMPLE
R1(config-ext-nacl)#deny ?
  <0-255>       An IP protocol number
  ahp           Authentication Header Protocol
  eigrp         Cisco's EIGRP routing protocol
  esp           Encapsulation Security Payload
  gre           Cisco's GRE tunneling
  icmp          Internet Control Message Protocol
  igmp          Internet Gateway Message Protocol
  ip            Any Internet Protocol
  ipinip        IP in IP tunneling
  nos           KA9Q NOS compatible IP over IP tunneling
  object-group  Service object group
  ospf          OSPF routing protocol
  pcp           Payload Compression Protocol
  pim           Protocol Independent Multicast
  sctp          Stream Control Transmission Protocol
  tcp           Transmission Control Protocol
  udp           User Datagram Protocol
```

- Examples of ip protocol number

1 : ICMP

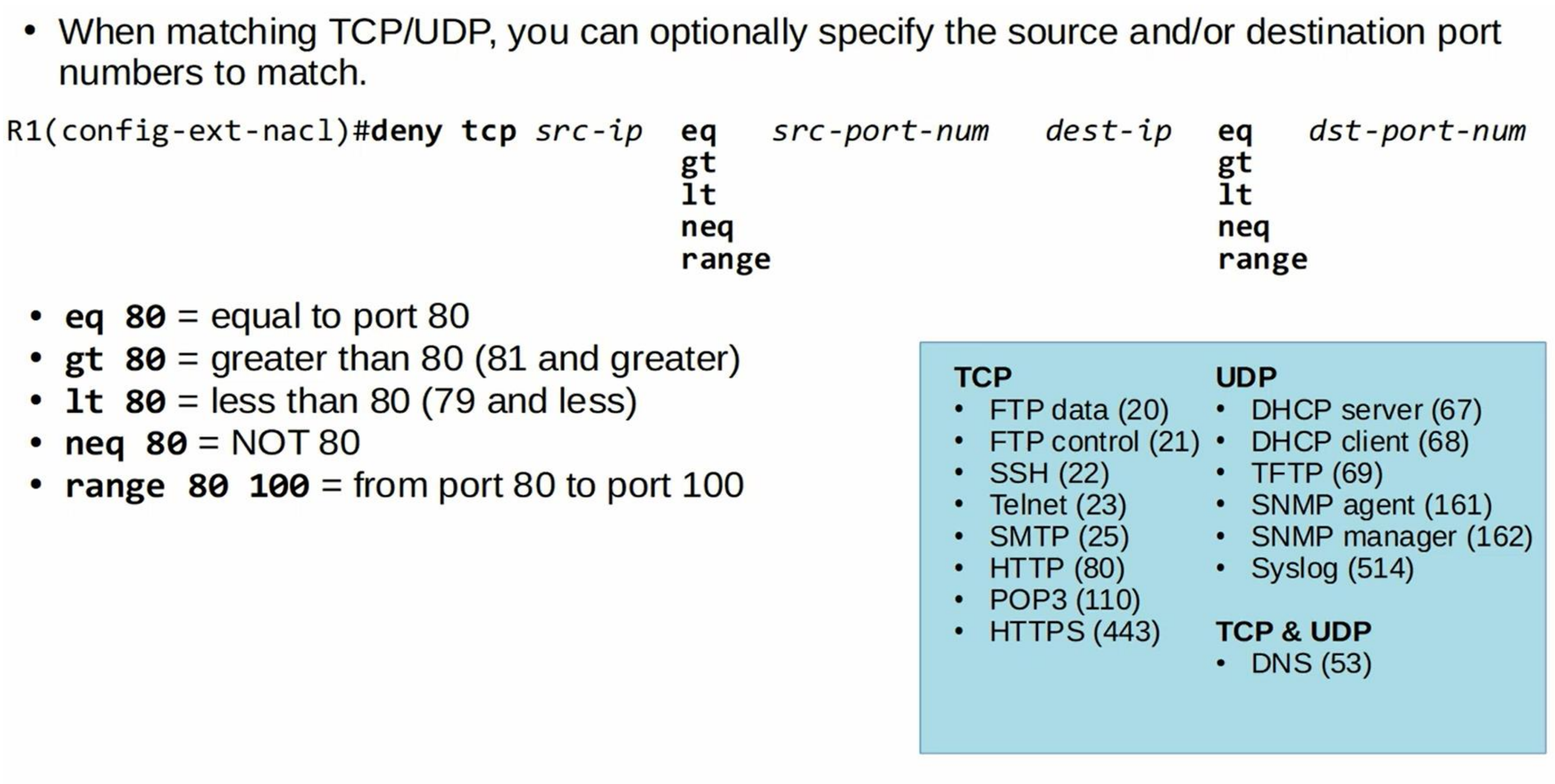
6 : TCP

17 : UDP

88 : EIGRP

89 OSPF

Matching the TCP/UDP port Number



- When matching TCP/UDP, you can optionally specify the source and/or destination port numbers to match.

```
R1(config-ext-nacl)#deny tcp src-ip   eq    src-port-num   dest-ip   eq    dst-port-num
                                      gt                             gt
                                      lt                             lt
                                      neq                            neq
                                      range                          range
```

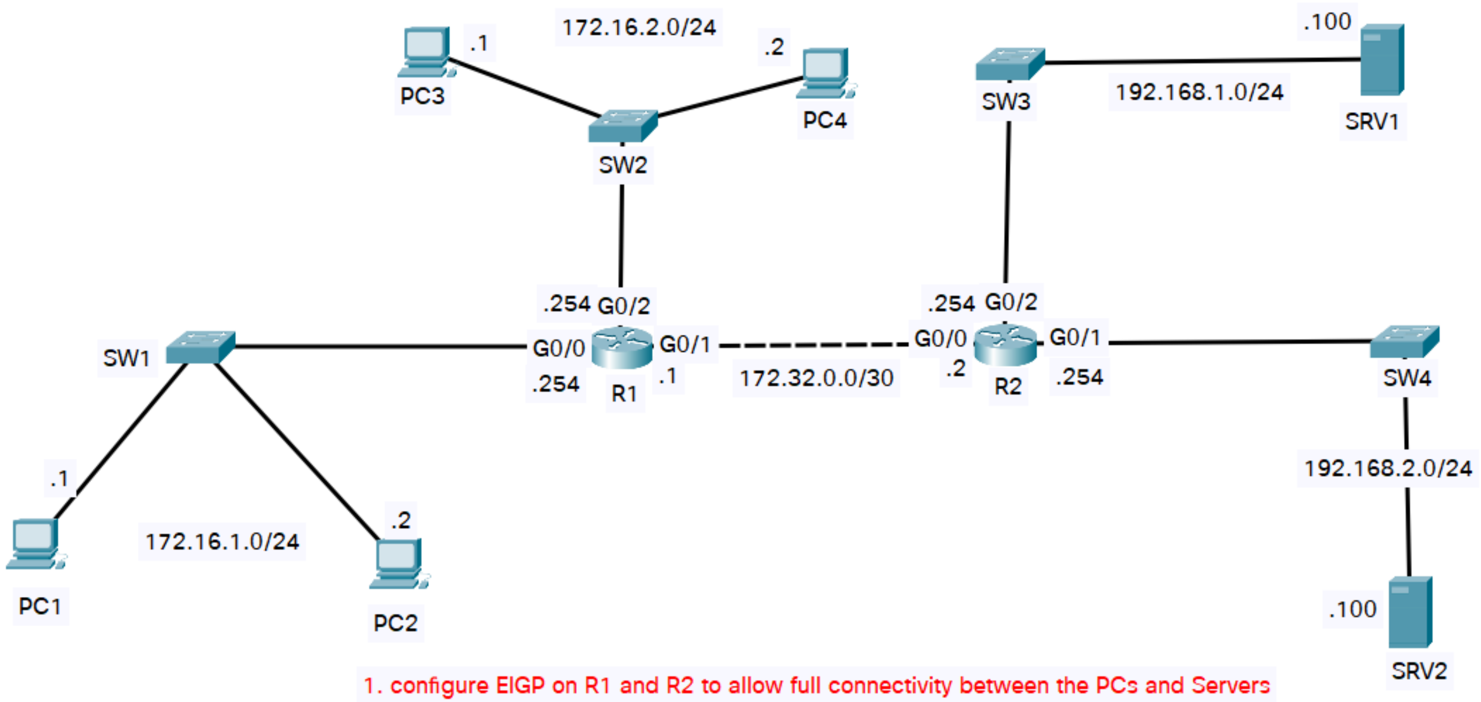
- **eq 80** = equal to port 80
- **gt 80** = greater than 80 (81 and greater)
- **lt 80** = less than 80 (79 and less)
- **neq 80** = NOT 80
- **range 80 100** = from port 80 to port 100

TCP
- FTP data (20)
- FTP control (21)
- SSH (22)
- Telnet (23)
- SMTP (25)
- HTTP (80)
- POP3 (110)
- HTTPS (443)

UDP
- DHCP server (67)
- DHCP client (68)
- TFTP (69)
- SNMP agent (161)
- SNMP manager (162)
- Syslog (514)

TCP & UDP
- DNS (53)

Hands-on project
Extended ACL



1. configure EIGP on R1 and R2 to allow full connectivity between the PCs and Servers
2. configure Extended ACLs to fulfill the following network policies:
   -Hosts in 172.16.2.0/24 can't communicate with PC1
   - Hosts in 172.16.1.0/24 can't access the DNS serever service on SRV1 1
   - Hosts in 172.16.2.0/24 can't access HTTP and HTTPS service on SRV2.

Hands-on project
Routing protocol and ACL

For EIGRP