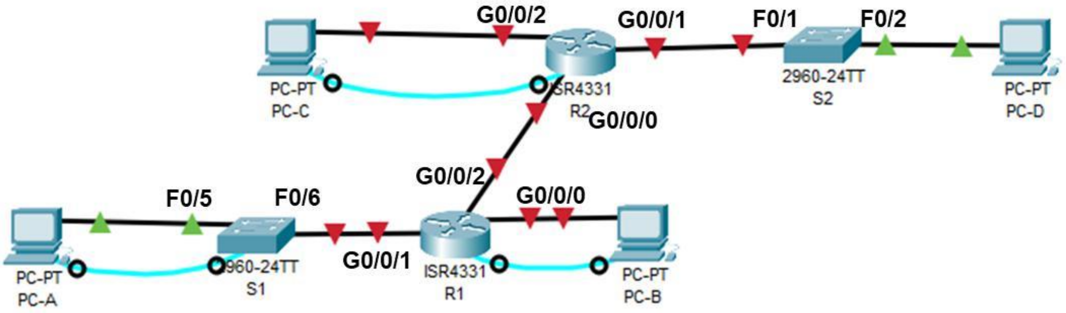
**CCNA** **ITN Lab 3**

**Names: Shanjida,**

**Team-No.: 04** **Rubaiya, Febin**

# IPv4 Subnetting and Routing Secure SSH Connection and Device Security TCP, UDP, DNS



## Lab Preparations

ITN Assessments: Modules 14 - 15: Network Application Communications Exam

Modules 16 - 17: Building and Securing a Small Network Exam (By the **ITN Module Group Exams 1-17** you exercise for the **ITN Final Exam.)**

NP Course: NP Chapter 4-7

Re-Call Cisco IOS Commands (prepare for the **ITN Skill Test**)

IPv4 Subnetting and Summary Routes

## Lab Instructions

Task 1 - IPv4 Network and Static Routes Task 2 - Accessing Network Devices with SSH Task 3 - Securing Network Devices Task4 - Observe the TCP 3-Way Handshake, UDP, and DNS

## Deliverables and List of Due Dates

Write your answers in **red color**. You may use the comment capabilities of the free Adobe reader.

# Preparation

## Part 1: Recall for the ITN Skill Test: Basic Configuration Commands

a. Read the Lab Instructions of this Lab

b. Check the IOS Command List, provided for the Labs.

c. Which IOS commands are necessary to configure the following tasks?

- Enter the privileged mode from startup mode. **Router>enable**
- Enter the configuration (EXEC) mode from terminal. **Router# config t or configure terminal**
- Set the hostname to R1. **Router(config)# hostname R1**
- Disable DNS lookup. **R1(config)# no ip domain-lookup**
- Assign **class** the EXEC encrypted password **R1(config)# enable secret class**
- Configure global password encryption. **R1(config)# service password-encryption**
- Return from configuration (EXEC) mode: **R1(config)# end**
- Assign **cisco** the console password and enforce login and set **logging synchronous** to prevent console messages from interrupting command entry.
  **R1(config)# line con 0**

  **R1(config-line) # password cisco**

  **R1(config-line) # login**

  **R1(config-line) # logging synchronous**

  **R1(config-line) # exit**
- Use vty (Telnet) lines 0-4, assign **cisco** as the vty (Telnet) password and enforce login.
  **R1(config)# line vty 0 4**

  **R1(configline) # password cisco**

  **R1(config-line) # login**

  **R1(configline) # exit**
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

  **R1(config)# banner motd # unauthorized access is prohibited #**
- Save the running configuration to the startup configuration file.

  **R1(config)# copy running-config startup-config**
- Display the **running configuration**. **R1(config)# show running-config or sh run**
- Display the status of all **interfaces** in brief. **R1(config)#show ip interface brief**
  **or sh ip int br**

## Part 2: Calculate IPv4 Subnets

### Step 1: Network Topology A

The 10.10.10.0/24 network address is used to provide the addresses in the network. Determine the number of subnets in Network Topology A.

a. How many subnets are there? 9

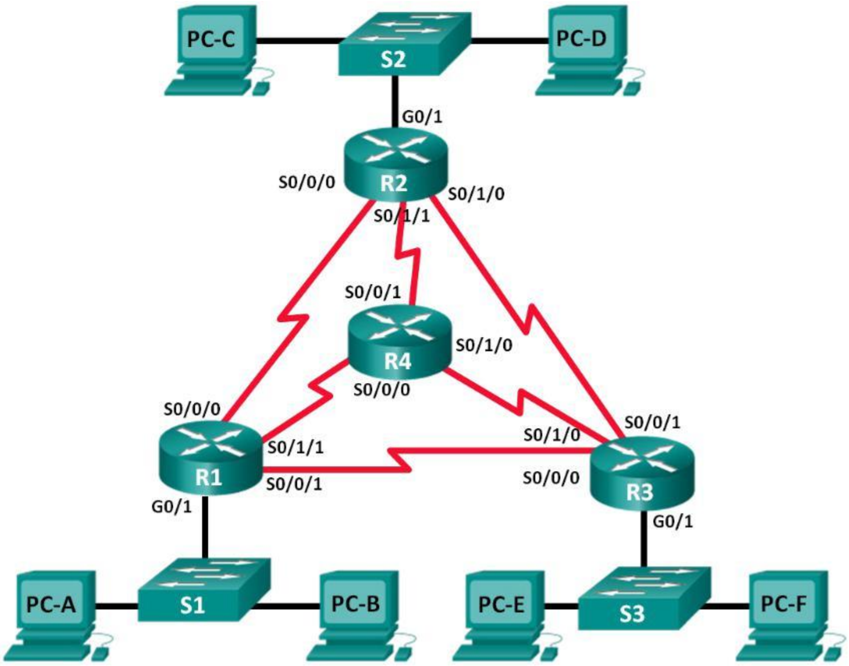
b. The Inter-Router links have no other hosts connected. Which subnet mask should be used?
**255.255.255.252**

c. The LANs connected to the switches have the different host numbers. Which subnet mask are valid for these LANs?

S1: 10 hosts mask: **255.255.255.240/28**

S2: 27 hosts mask: **255.255.255.224/27**

S3: 48 hosts mask: **255.255.255.192/26**

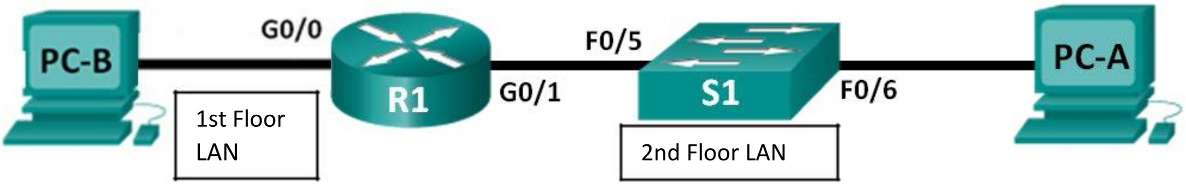


d. Record the subnet information.
- Derive the subnets from the largest subnet to the smallest subnet.
- Name the LAN subnets according to their switch number Sx Name the Inter-Router subnets Rx-Ry

| Subnet | Subnet Address | First Usable Host Address | Last Usable Host Address | Broadcast Address |
|---|---|---|---|---|
| LAN3/26 | 10.10.10.0/26 | 10.10.10.1 | 10.10.10.62 | 10.10.10.63 |
| LAN2/27 | 10.10.10.64/27 | 10.10.10.65 | 10.10.10.96 | 10.10.10.97 |
| LAN1/28 | 10.10.10.98/28 | 10.10.10.99 | 10.10.10.112 | 10.10.10.113 |
| R3-R2 | 10.10.10.114/30 | 10.10.10.115 | 10.10.10.116 | 10.10.10.117 |
| R3-R1 | 10.10.10.118/30 | 10.10.10.119 | 10.10.10.120 | 10.10.10.121 |
| R1-R2 | 10.10.10.122/30 | 10.10.10.123 | 10.10.10.124 | 10.10.10.125 |
| R3-R4 | 10.10.10.126/30 | 10.10.10.127 | 10.10.10.128 | 10.10.10.129 |
| R2-R4 | 10.10.10.130/30 | 10.10.10.131 | 10.10.10.132 | 10.10.10.133 |
| R1-R4 | 10.10.10.134/30 | 10.10.10.135 | 10.10.10.136 | 10.10.10.137 |

### Step 2: Network Subnetting

Given is the following simple network without any Internet access.



Available is the IP address range 192.168.100.0 / 24. Subnet the network to provide 60 host addresses per subnet while wasting the fewest address in table 1.

| Subnet | Subnet Address | First Usable Host Address | Last Usable Host Address | Broadcast Address |
|---|---|---|---|---|
| 1 | 192.168.100.0 | 192.168.100.1 | 192.168.100.62 | 192.168.100.63 |
| 2 | 192.168.100.64 | 192.168.100.65 | 192.168.100.126 | 192.168.100.127 |
| 3 | 192.168.100.128 | 192.168.100.129 | 192.168.100.190 | 192.168.100.191 |
| 4 | 192.168.100.192 | 192.168.100.193 | 192.168.100.254 | 192.168.100.255 |

We assign the third subnet to the First Floor LAN. Assign the last network host address (the highest) in this subnet to the G0/0 interface of router R1 in table2.

Assign the first network host address in this subnet to the NIC interface of PC-B in table2.

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| R1 | G0/0 | 192.168.100.190 | 255.255.255.192 | no |
| | G0/1 | 192.168.100.254 | 255.255.255.224 | no |
| S1 | VLAN1 | 192.168.100.253 | 255.255.255.224 | 192.168.100.254 |
| PC-A | NIC | 192.168.100.225 | 255.255.255.224 | 192.168.100.254 |
| PC-B | NIC | 192.168.100.129 | 255.255.255.192 | 192.168.100.190 |

Starting with the forth subnet of table 1, subnet this network again so that the new subnets will provide 28 host addresses per subnet while wasting the fewest addresses in table3.

| Subnet | Subnet Address | First Usable Host Address | Last Usable Host Address | Broadcast Address |
|---|---|---|---|---|
| 4th-1 | 192.168.100.192 | 192.168.100.193 | 192.168.100.222 | 192.168.100.223 |
| 4th-2 | 192.168.100.224 | 192.168.100.225 | 192.168.100.254 | 192.168.100.255 |

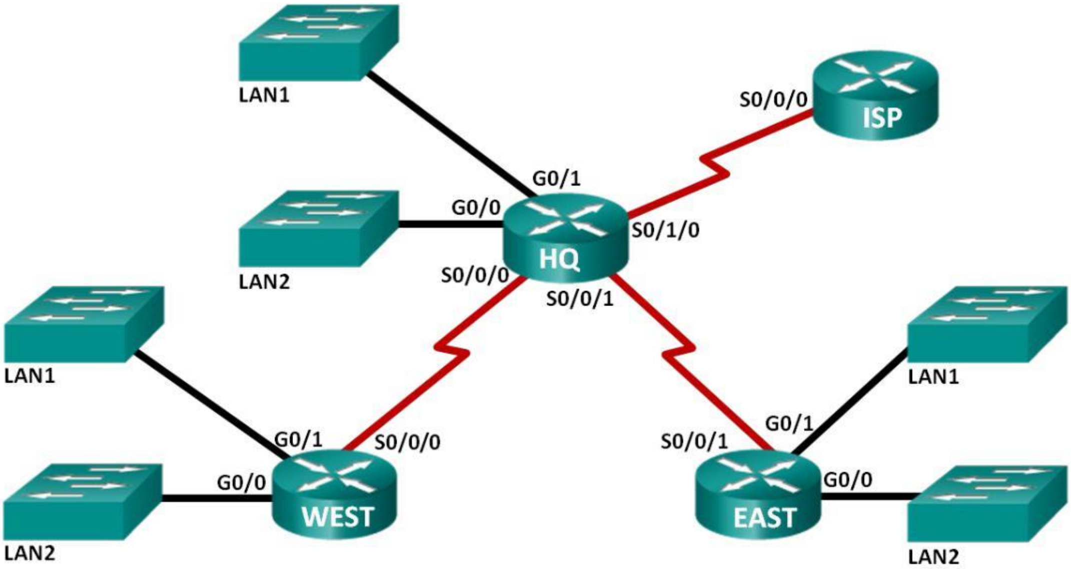
Assign the second of these new 28-host subnets to the Second Floor LAN. Assign the last network host address (the highest) in the Second Floor LAN subnet to the G0/1 interface of router R1 in table2.

Assign the second to the last address (the second highest) in this subnet to the VLAN 1 interface of the Second Floor Switch in table2.

Assign the first address in this subnet to the NIC interface of PC-A in table2.

## Part 3: Calculating IPv4 Summary Routes

### Topology



### Addressing Table

| Subnet | IPv4 Address | Subnet | IPv4 Address |
|---|---|---|---|
| HQ LAN1 | 192.168.64.0/23 | WEST LAN1 | 192.168.70.0/25 |
| HQ LAN2 | 192.168.66.0/23 | WEST LAN2 | 192.168.70.128/25 |
| | | Link from HQ to EAST | 192.168.71.4/30 |
| EAST LAN1 | 192.168.68.0/24 | Link from HQ to WEST | 192.168.71.0/30 |
| EAST LAN2 | 192.168.69.0/24 | Link from HQ to ISP | 209.165.201.0/30 |

#### Step 1: Determine the summary route for HQ LAN1 and HQ LAN2

You may work step by step to the following scheme: List the HQ LAN1 and HQ LAN2 IP subnet mask in decimal form. Then List the HQ LAN1 and HQ LAN2 IP address in binary form. Finally Count the number of far left matching bits to determine the subnet mask for the summary route:

a. How many far left matching bits are present in the two networks? **22 bits are matched**

b. List the matching binary bits for HQ subnets. **11000000.10101000.010000 /(192.168.010000) are matching**

c. Add zeros to comprise the remainder of the network address in binary form. **192.168.01000000.00000000**
**zeros to compromise the reminder are denoted with blue color.**
**Matching binary bits are underlined as red.**

d. List the summarized network address in decimal form. **192.168.64.0/22**

| Subnet | IPv4 Address | Subnet Mask | Subnet IP Address in Binary Form |
|---|---|---|---|
| HQ LAN1 | 192.168.64.0/23 | **255.255.254.0** | **11000000.10101000.01000000.00000000** |
| HQ LAN2 | 192.168.66.0/23 | **255.255.254.0** | **11000000.10101000.01000010.00000000** |
| HQ LANs Summary Address | **192.168.64.0/22** | **255.255.252.0** | **11000000.10101000.01000000.00000000** |

### Step 2: Determine the summary route for EAST LAN1 and EAST LAN2

a. How many far left matching bits are present in the two networks? **23 bits are matched**

b. Build the summarized network address
**192.168.01000100.00000000=192.168.68.0/23**
**Matching binary bits are underlined as red.**

| Subnet | IPv4 Address | Subnet Mask | Subnet Address in Binary Form |
|---|---|---|---|
| EAST LAN1 | 192.168.68.0/24 | **255.255.255.0** | **11000000.10101000.01000100.00000000** |
| EAST LAN2 | 192.168.69.0/24 | **255.255.255.0** | **11000000.10101000.01000101.00000000** |
| EAST LANs<br>Summary Address | **192.168.68.0/23** | **255.255.254.0** | **11000000.10101000.01000100.00000000** |

### Step 3: Determine the summary route for WEST LAN1 and WEST LAN2

a. How many far left matching bits are present in the two networks? **24**

b. Build the summarized network address
**192.168.01000110.00000000= 192.168.70.0/24**

| Subnet | IPv4 Address | Subnet Mask | Subnet IP Address in Binary Form |
|---|---|---|---|
| WEST LAN1 | 192.168.70.0/25 | **255.255.255.128** | **11000000.10101000.01000110.00000000** |
| WEST LAN2 | 192.168.70.128/25 | **255.255.255.128** | **11000000.10101000.01000110.10000000** |
| WEST LANs<br>Summary Address | 192.168.70.0/24 | **255.255.255.0** | **11000000.10101000.01000110.00000000** |

### Step 4: Determine the summary routes for HQ, EAST and WEST

a. List the matching binary bits for HQ, EAST, and WEST subnets.
**11000000.10101000.01000**

b. Add zeros to comprise the remainder of the network address in binary form. **000.00000000**

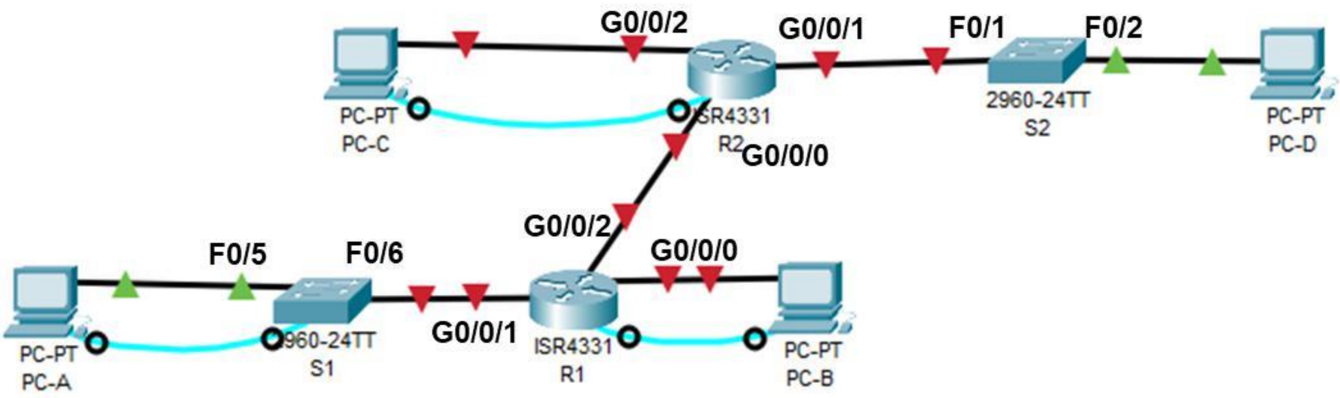
c. List the summarized network address in decimal form.
**Summarized network address = 192.168.01000100.00000000=192.168.64.0/22**

| Subnet | IPv4 Address | Subnet Mask | Subnet IP Address in Binary Form |
|---|---|---|---|
| HQ | **192.168.64.0/22** | **255.255.255.252** | **11000000.10101000.01000000.00000000** |
| EAST | **192.168.68.0/23** | **255.255.254.0** | **11000000.10101000.01000100.00000000** |
| WEST | **192.168.70.0/24** | **255.255.255.0** | **11000000.10101000.01000110.00000000** |
| Network Address<br>Summary Route | **192.168.64.0/22** | **255.255.255.252** | **11000000.10101000.01000000.00000000** |

**!!A summary route may be used by the ISP as static route to your stub network!!**

# Task 1 – IPv4 Network and Static Routes

### Packet Tracer Topology



### Addresing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| R1 | G0/0/0 | 10.0.2.1 | 255.255.255.0 | N/A |
| | G0/0/1 | 10.0.1.1 | 255.255.255.0 | N/A |
| | G0/0/2 | 172.16.0.1 | 255.255.255.252 | N/A |
| S1 | VLAN 1 | 10.0.1.2 | 255.255.255.0 | 10.0.1.1 |
| R2 | G0/0/0 | 172.16.0.2 | 255.255.255.252 | N/A |
| | G0/0/1 | 192.168.20.1 | 255.255.255.0 | N/A |
| | G0/0/2 | 192.168.10.1 | 255.255.255.0 | N/A |
| PC-A | NIC | 10.0.1.10 | 255.255.255.0 | 10.0.1.1 |
| PC-B | NIC | 10.0.2.20 | 255.255.255.0 | 10.0.2.1 |
| PC-C | NIC | 192.168.10.30 | 255.255.255.0 | 192.168.10.1 |
| PC-D | NIC | 192.168.20.40 | 255.255.255.0 | 192.168.20.1 |

## Part 1: Set Up Network Topology and Initialize Devices

### Step 1: Build topology in Packet Tracer.

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

a. Build the network with ISR4331 routers, 2960 switches, and PCs in Packet Tracer. Rename the devices.

b. Implement a 3rd Gigabit Ethernet interface GLC-T SFP in slot G0/0/2 in each ISR 4331 router.

## Part 2: Router R1 Settings

### Step 1: Perform basic Router configurations

Access router R1 through the Serial Console Port and Desktop Terminal of PC-B

- Assign a device name **R1** to the router **Router(config)#** **hostname R1**
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names **R1(config)#** **no ip domain-lookup**

### Step 2: Secure access lines and basic device security

- Assign **class** as the privileged EXEC secret **R1(config)#** **enable secret class**
- Create a **banner** that warns anyone accessing the device that unauthorized access is prohibited **R1(config)#** **banner motd # unauthorized access is prohibited #**
- Assign **cisco** as the console password and enable login

```
R1(config)# line con 0
R1(config-line) # password cisco
R1(config-line) # login
```

- Assign **cisco** the Telnet (VTY) password for 5 lines and enable login

```
R1(config)# line vty 0 4
R1(config-line) # password cisco
R1(config-line) # login
```

- **Encrypt** the clear text passwords in the configuration file

```
R1(config)# service password-encryption
```

### Step 3: Configure and activate router interfaces

d. Configure and activate interface g0/0/0 with IP address, mask and description

```
R1(config)# interface g0/0/0
R1(config-if)# description Connected to PC-B
R1(config-if)# ip address 10.0.2.1 255.255.255.0
R1(config-if)# no shutdown
```

e. Configure and activate interface g0/0/1 with IP address, mask and description

```
R1(config)# interface g0/0/1
R1(config-if)# description Connected to S1
R1(config-if)# ip address 10.0.1.1 255.255.255.0
R1(config-if)# no shutdown
```

f. Configure and activate interface g0/0/2 with IP address, mask and description

```
R1(config)# interface g0/0/2
R1(config-if)# description Connected to R2
R1(config-if)# ip address 172.16.0.1 255.255.255.252
R1(config-if)# no shutdown
```

### Step 4: Test LAN A and LAN B Connectivity

Assign static IP address, network mask and default gateway to PC-A and PC-B. **Done**

- From PC-A ping switch S1. Successful (y/n) **yes**
- Test PC-A to PC-B connectivity by ping. Successful (y/n) **yes**

**Note:** Remove errors and reconfigure network in case of no connectivity.

# Part 3: Router R2 Settings

## Step 1: Perform basic Router configurations

Access router R2 through the Serial Console Port and Desktop Terminal of PC-C

- Assign a device name **R2** to the router **Router(config)# hostname R2**
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names **R2(config)# no ip domain-lookup**

## Step 2: Secure access lines and basic device security

- Assign **class** as the privileged EXEC secret **R2(config)# enable secret class**
- Create a **banner** that warns anyone accessing the device that unauthorized access is prohibited
  **R2(config)# banner motd # unauthorized access is prohibited #**
- Assign **cisco** as the console password and enable login

```
R2(config)# line con 0
R2(config-line) # password cisco
R2(config-line) # login
```

- Assign **cisco** the Telnet (VTY) password for 5 lines and enable login

```
R2(config)# line vty 0 4
R2(config-line) # password cisco
R2(config-line) # login
```

- **Encrypt** the clear text passwords in the configuration file
  **R2(config)# service password-encryption**

## Step 3: Configure and activate router interfaces

- Configure and activate interface g0/0/0 with IP address, mask and description

```
R2(config)# interface g0/0/0
R2(config-if)# description Connected to R1
R2(config-if)# ip address 10.0.0.2 255.255.255.252
R2(config-if)# no shutdown
```

- Configure and activate interface g0/0/1 with IP address, mask and description

```
R2(config)# interface g0/0/1
R2(config-if)# description Connected to S2
R2(config-if)# ip address 10.0.20.1 255.255.255.0
R2(config-if)# no shutdown
```

- Configure and activate interface g0/0/2 with IP address, mask and description

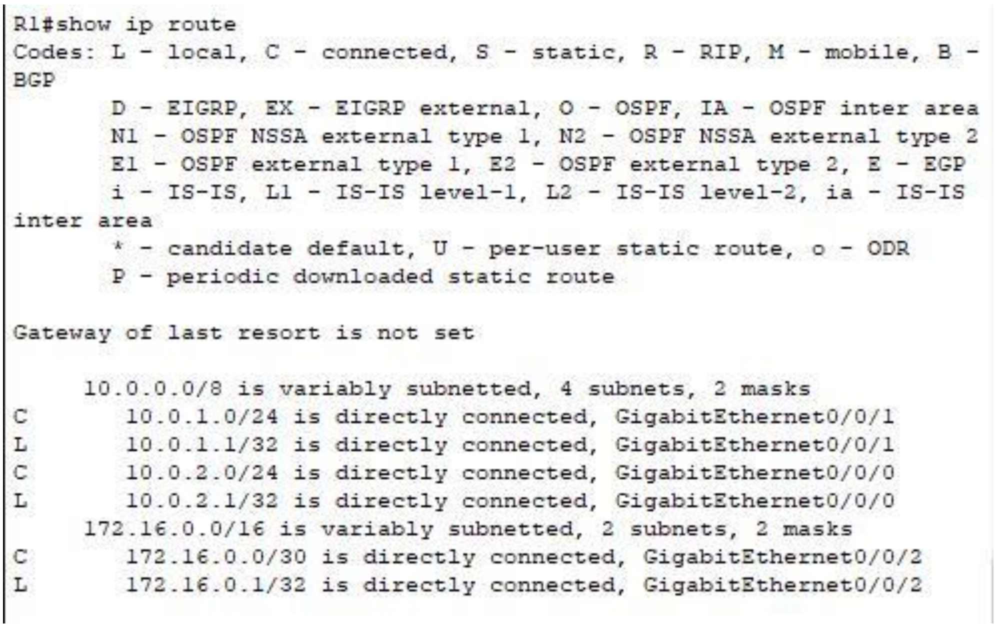
```
R2(config)# interface g0/0/2
R2(config-if)# description Connected to PC-C
R2(config-if)# ip address 10.0.10.1 255.255.255.0
R2(config-if)# no shutdown
```

## Step 4: Test LAN C and LAN D Connectivity

- Assign static IP address, network mask and default gateway to PC-C and PC-D.
- From PC-D ping router R2 interface g0/0/2. Successful (y/n) yes
- From router R2 ping router R1 interface g0/0/2. Successful (y/n) yes
  **Note**: Remove errors and reconfigure network in case of no connectivity.

### Step 5: Check Routes in Router R1

- Display routing table of router R1. Record the networks which are reachable by router R1.



```
R1#show ip route
Codes: L - local, C - connected, S - static, 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

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.0.1.0/24 is directly connected, GigabitEthernet0/0/1
L       10.0.1.1/32 is directly connected, GigabitEthernet0/0/1
C       10.0.2.0/24 is directly connected, GigabitEthernet0/0/0
L       10.0.2.1/32 is directly connected, GigabitEthernet0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.0.0/30 is directly connected, GigabitEthernet0/0/2
L       172.16.0.1/32 is directly connected, GigabitEthernet0/0/2
```

- Explain, why PC-D is not reachable from PC-A: **This means that PC-D is not operating on the same network.**

## Part 4: Configure Static Routes

### Step 1: Configure a recursive static route on R2.

With a **recursive static route**, the next-hop IP address is specified. Because only the next-hop IP is specified, the router must perform multiple lookups in the routing table before forwarding packets. The IP address is the next hop router address:

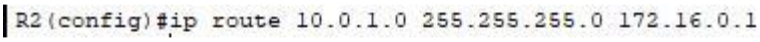
a. Which network(s) must be configured as static routes on R2? **10.0.1.0/24 and 10.0.2.0/24**

c. Which next hop address must be used on R2?

**R1 g0/0/2 IP address: 172.16.0.1 must be used as next hop address.**

c. Configure the required LAN as **recursive static route** on R2. Record the required command.

**PC-A LAN network address: 10.0.1.0**



```
R2(config)#ip route 10.0.1.0 255.255.255.0 172.16.0.1
```

### Step 2: Directly connected static route on R2.

With a directly connected static route, the *exit-interface* parameter is specified, which allows the router to resolve a forwarding decision in one lookup. A directly connected static route is typically used with a point-to-point serial interface.

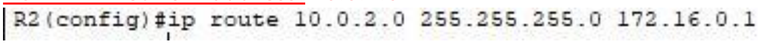
a. Which network(s) must be configured as static routes on R2?

**same**

b. Configure the PC-B LAN as **directly connected static route** on R2. Record the required command.

c.

**PC-B LAN network address: 10.0.2.0**

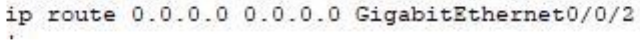


```
R2(config)#ip route 10.0.2.0 255.255.255.0 172.16.0.1
```

## Step 3: Static default route on R1

A default route identifies the gateway to which the router sends all IP packets for which it does not have a learned or static route. A default static route is a static route with 0.0.0.0 as the destination IP address and subnet mask. This is commonly referred to as a “quad zero” route. In a default route, either the next-hop IP address (recursive static route) or exit interface (directly connected static route) can be specified.

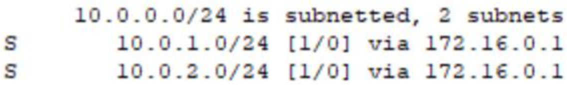
a. Configure a **static default route** at R1 using the **exit interface of g0/0/2**. Record the required command.
**I have configured the R1 router with a default route using the exit interface of g0/0/2.**



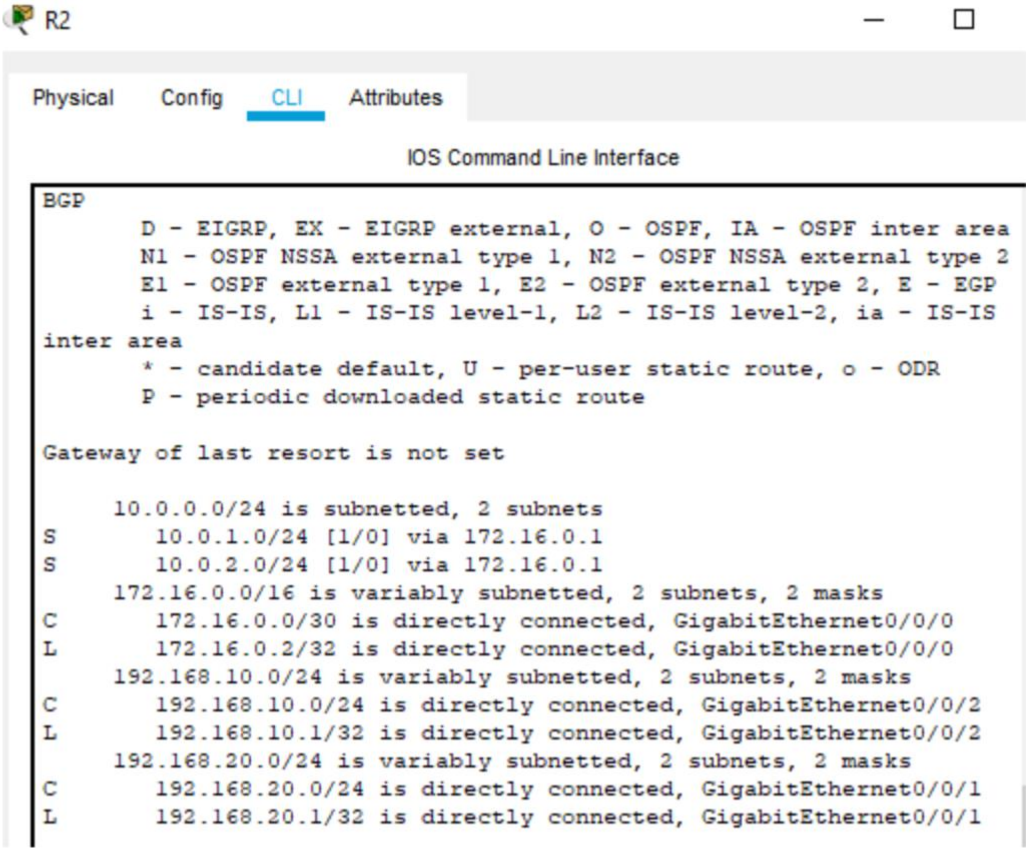
```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/2
```

## Step 4: Verify connectivity of the LANs.

a. Display IP routing table of router R2. Is there a path to PC-A LAN (y/n)? **yes**



```
     10.0.0.0/24 is subnetted, 2 subnets
S       10.0.1.0/24 [1/0] via 172.16.0.1
S       10.0.2.0/24 [1/0] via 172.16.0.1
```



```
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

     10.0.0.0/24 is subnetted, 2 subnets
S       10.0.1.0/24 [1/0] via 172.16.0.1
S       10.0.2.0/24 [1/0] via 172.16.0.1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.0.0/30 is directly connected, GigabitEthernet0/0/0
L       172.16.0.2/32 is directly connected, GigabitEthernet0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/2
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/2
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0/1
```

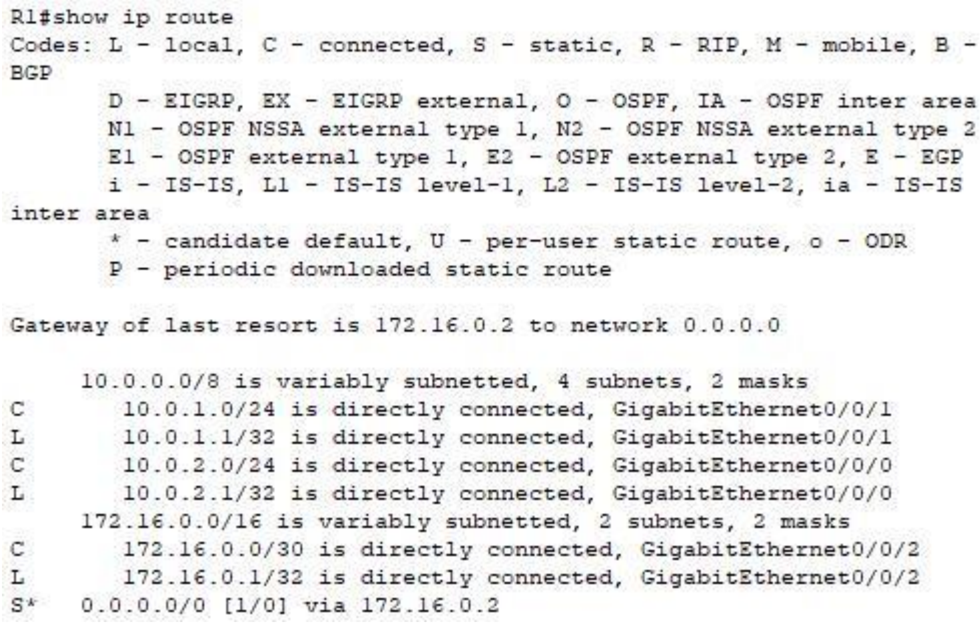
b. From PC-A, is it possible to ping R2 interface g0/0/0 (y/n)? **y**

c. From PC-A, is it possible to ping PC-C (y/n)? **y**

d. From PC-D, is it possible to ping PC-A (y/n)? **y**

**Note:** Remove errors and reconfigure network in case of no connectivity.

e. Display the routing table of router R1.



```
R1#show ip route
Codes: L - local, C - connected, S - static, 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 172.16.0.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.0.1.0/24 is directly connected, GigabitEthernet0/0/1
L       10.0.1.1/32 is directly connected, GigabitEthernet0/0/1
C       10.0.2.0/24 is directly connected, GigabitEthernet0/0/0
L       10.0.2.1/32 is directly connected, GigabitEthernet0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.0.0/30 is directly connected, GigabitEthernet0/0/2
L       172.16.0.1/32 is directly connected, GigabitEthernet0/0/2
S*   0.0.0.0/0 [1/0] via 172.16.0.2
```

I. Which networks are routed in router R1?

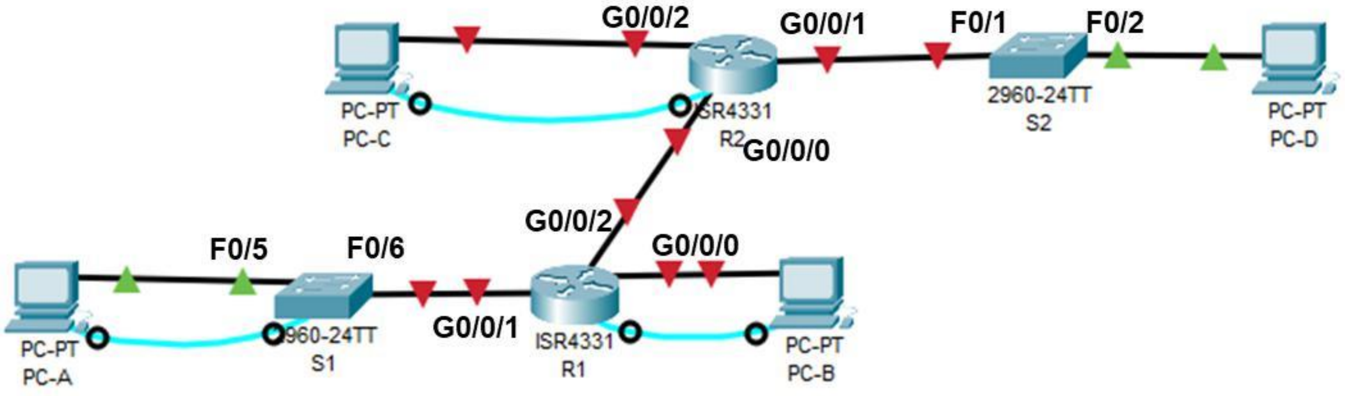
**10.0.1.0/24, 10.0.2.0/24, 172.16.0.0/16 and 0.0.0.0/0**

II. How is this new static default route marked in the routing table?

**with * mark in the router table as S$^*$**

# Task 2 – Accessing Network Devices with SSH

### Packet Tracer Topology



Continue with topology and addressing of Task 1.

### Objectives

Protocols such as Telnet do not authenticate or encrypt the information. This allows a network sniffer to intercept passwords and configuration information. Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection. SSH encrypts all information and provides authentication of the remote computer.

## Part 1: Configure Router R2 for SSH Access

### Step 1: Configure device authentication with crypto key.

The device name and domain are used as part in the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command. We use **RSA** encryption with a key length of **1024 Bytes**.

a. Configure the domain for the device.

```
R2(config)# ip domain-name ccna-lab.com
```

b. Configure crypto key

```
R2(config)# crypto key generate rsa
```

The name for the keys will be: **R2.ccna-lab.com**

Choose the size of the key of 1024 bits.

```
How many bits in the modulus [512]: 1024
```

### Step 2: Configure a local username stored in the local database.

The local database is used to store usernames and passwords with additional privilege levels.
**Note**: A **privilege level of 15** gives the user **administrator** rights.

```
R2(config)# username admin privilege 15 secret adminpass
```

### Step 3: Enable SSH on the VTY lines.

a. Enable only SSH on the **inbound** VTY lines using the **transport input** command.

```
R2(config)# line vty 0 4 R2(config-

line)# transport input ssh
```

b. Change the login method to use the **local database** for user verification and save the running configuration to the startup configuration file.

```
R2(config-line)# login
local
R2(config-line)# end
R2# copy running-config startup-config
```

**Important Note**: From now, access via VTY without having a local user is prohibited!!

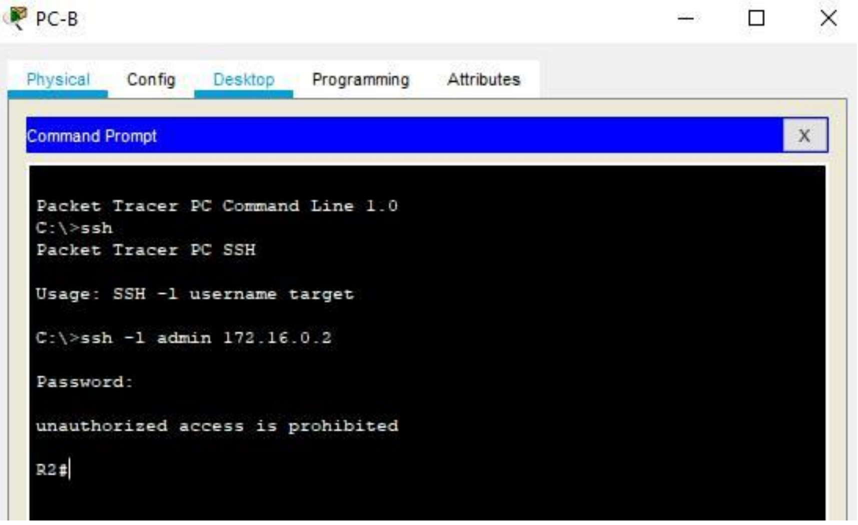
## Part 2: Use SSH Client to start an SSH session to the Router

### Step 1: SSH Client

SSH is most often used to log in to a remote device and execute commands; however, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

a. What is the default TCP port used for SSH sessions? 22

b. From PC-B, start the Telnet/SSH Client from Desktop and establish an SSH connection to router R2.

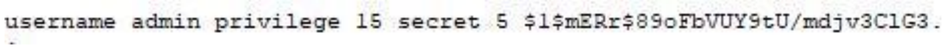


```
Packet Tracer PC Command Line 1.0
C:\>ssh
Packet Tracer PC SSH

Usage: SSH -l username target

C:\>ssh -l admin 172.16.0.2

Password:

unauthorized access is prohibited

R2#
```

### Step 2: Administration Tasks

a. Login as administrator on R2.
At login the data from local database will be used.

Record the administrator password from running-configuration.



```
username admin privilege 15 secret 5 $1$mERr$89oFbVUY9tU/mdjv3C1G3.
.
```

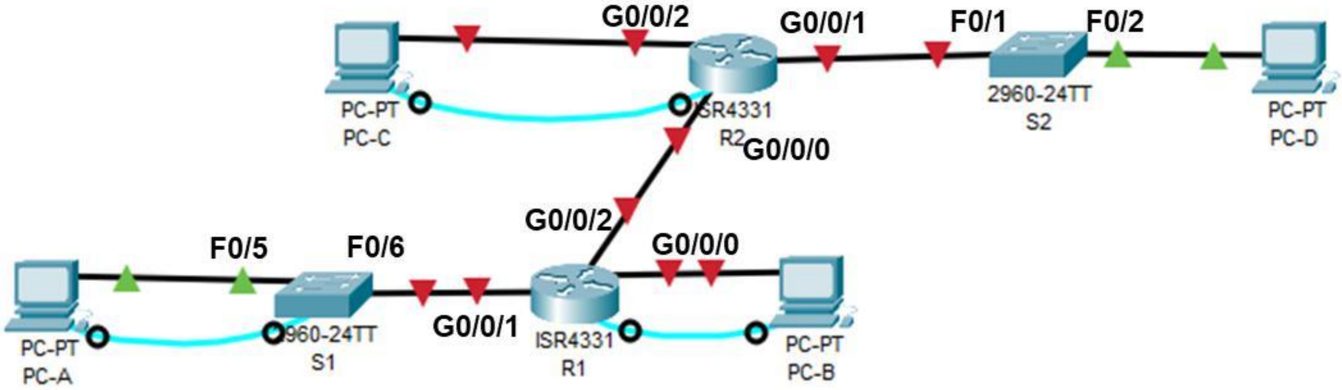
Which command created this representation of the admin password?

```
R2(config)# username admin privilege 15 secret adminpass
```

b. Enter **exit** to exit the SSH session and close the SSH Client. Done

# Task 3 - Securing Network Devices

### Packet Tracer Topology



Continue with topology and addressing of Task 1.

## Part 1: Basic Switch Security Measures

### Step 1: Configure Switch S1 via Console Cable

- Access switch S1 through the Serial Console Port and Desktop Terminal of PC-A
- Provide hostname **S1. Switch(config)# hostname S1**
- Prevent DNS domain lookup. **S1(config)# no ip domain-lookup**

### Step 2: Secure access lines and basic device security

- Assign **class** as the privileged EXEC secret
- Create a **banner** for motto-of-the-day

```
S1(config)#banner motd #Unauthorized access is denied #
```

- Implement terminal login (Console) and password is **cisco**

```
S1(config)# line con 0
S1(config-line) # password cisco
S1(config-line) # login
```

- Implement 5 Telnet lines (vty) and password is **cisco**.

```
S1(config)# line vty 0 4
S1(config-line) # password cisco
S1(config-line) # login
```

- **Encrypt** all passwords

```
S1(config)# service password-encryption
```

### Step 3: Switch Virtual Interface

Configure and switch-on VLAN 1 interface

```
S1(config)# interface Vlan1
S1(config-if)# ip address 10.0.1.2 255.255.255.0
S1(config-if)# ip default-gateway 10.0.1.1
```

Configure the switch default gateway.

```
S1(config)# ip default-gateway 10.0.1.1
```

### Step 4: Shut off unused switch ports.

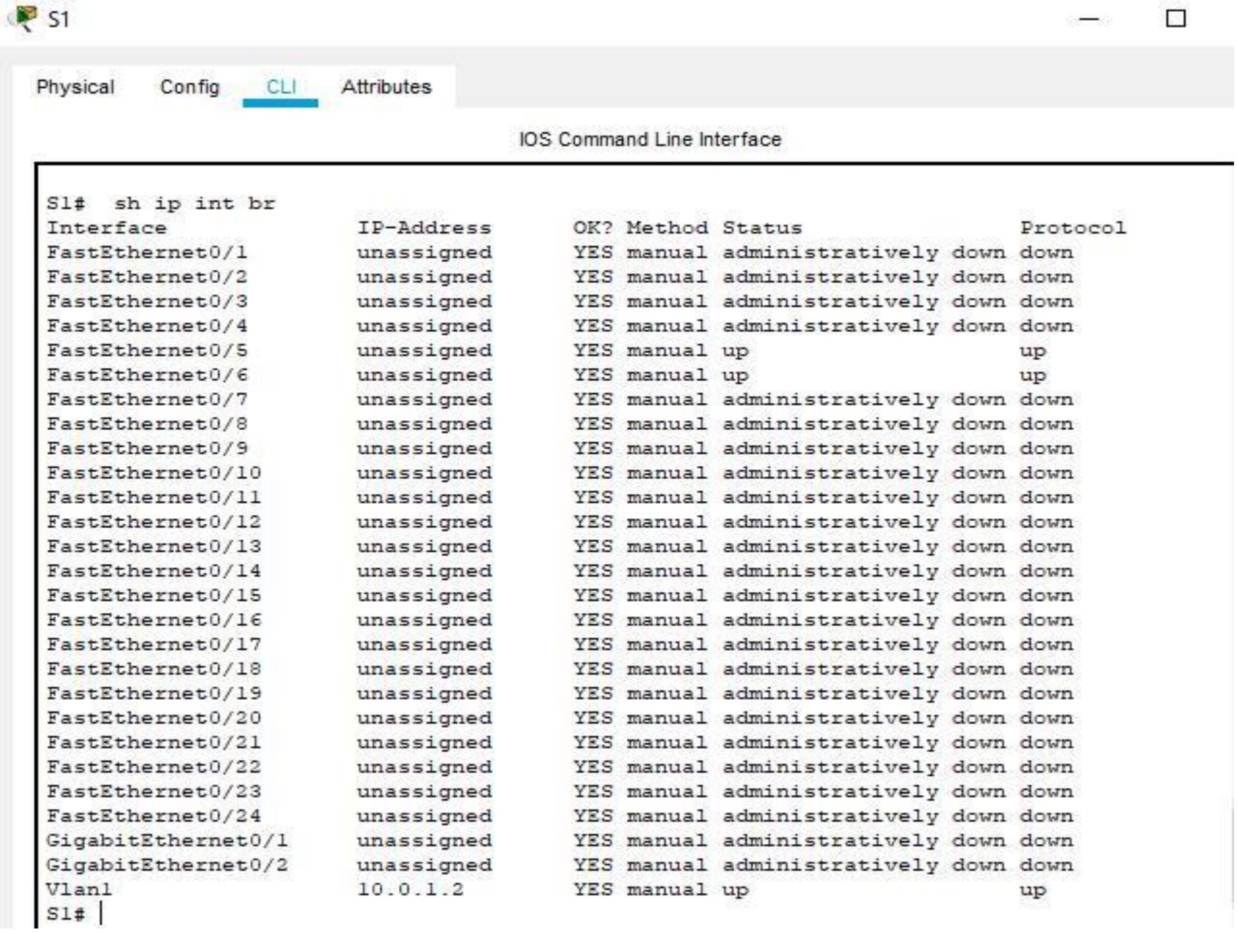
Switch ports must be secured as well. Switch ports are enabled by default. Shut down all ports that are not in use on the switch. Use the **interface range** command to shut down multiple interfaces at a time. Use it for those ports, which are not in use!

```
S1(config)# interface range f0/1-4,f0/7-24,g0/1-
2 S1(config-if-range)# shutdown
```

You can verify the switch port status using the **show ip interface brief** command.

```
S1# show ip interface brief
```

Record the status of interface g0/1:



```
S1#  sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual administratively down down
FastEthernet0/2        unassigned      YES manual administratively down down
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual up                    up
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  10.0.1.2        YES manual up                    up
S1# |
```

## Part 2: SSH at Switches

### Step 1: SSH connectivity on Switch S1

On switches the same security mechanisms as on routers may be applied.

a. Configure the domain for the device.

```
S1(config)# ip domain-name ccna-lab.com
```

b. Configure crypto key

```
S1(config)# crypto key generate rsa ...
How many bits in the modulus [512]: 1024
```

c. Enable SSH on the **inbound** VTY lines and login method to use the **local database** for user verification.

```
S1(config)# username admin privilege 15 secret
adminpass S1(config)# line vty 0 4
S1(config-line)# transport input
ssh S1(config-line)# login local
S1(config-line)# end
```

### Step 2: Test SSH connectivity to Switch S1.

a. Open a Telnet connection from PC-A to switch S1. Does S1 accept the Telnet connection? **NO**

b. Open an SSH connection from PC-A to switch S1. Does S1 accept the SSH connection? **YES**

- Issue the **show run** command.
  What indicates the configuration of SSH in the running-configuration?
  **transport input ssh in line vty 0 4 (from show run)**

## Part 3: Strengthen Login and Password Security

### Step 1: Strengthen passwords on Router R2.

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include mixing letters, numbers, and special characters in the password and setting a minimum length.

a. Change the privileged EXEC encrypted password to meet guidelines.

```
R2(config)# enable secret Enablep@55
```

b. Require that a minimum of 10 characters be used for all passwords.

```
R2(config)# security passwords min-length 10
```

### Step 2: Secure the console and VTY lines by timeout and lock

You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time.

a. The following commands cause the line to log out after five minutes of inactivity.

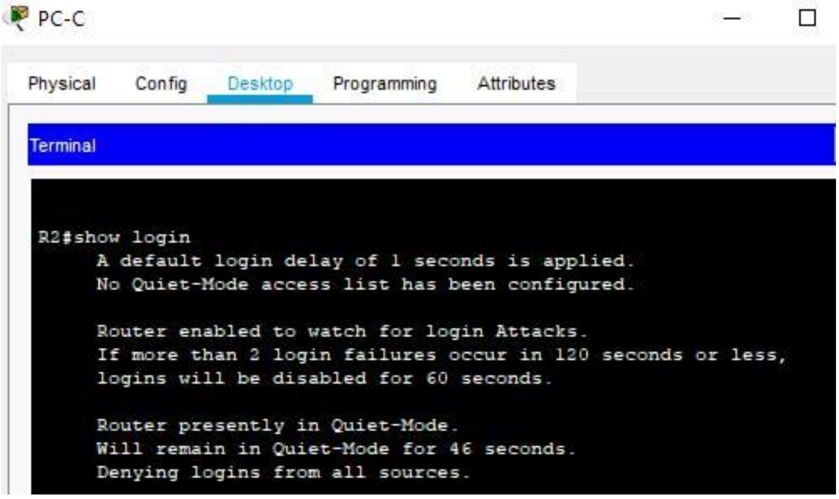
```
R2(config)# line console 0
R2(config-line)# exec-timeout 5 0
R2(config-line)# line vty 0 4
R2(config-line)# exec-timeout 5 0
```

b. The following command impedes brute force login attempts. The router blocks login attempts for 60 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
R2(config)# login block-for 60 attempts 2 within 120
```

c. From PC-D create an SSH connection to router R2 and intentionally mistype the user and password information to see if login access is blocked after two attempts.

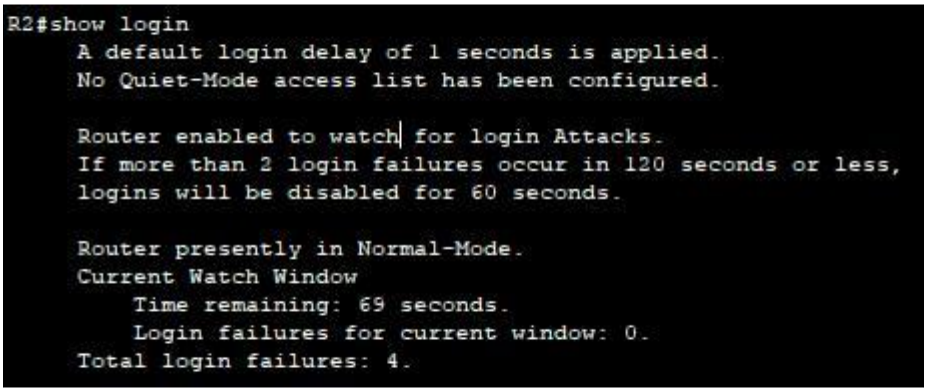
From your PC-C console session on the router, issue the **show login** command.



```
R2#show login
     A default login delay of 1 seconds is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 60 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 46 seconds.
     Denying logins from all sources.
```

d. After the 60 seconds has expired, SSH to R2 again and login using the **admin** username and **adminpass** for the password.

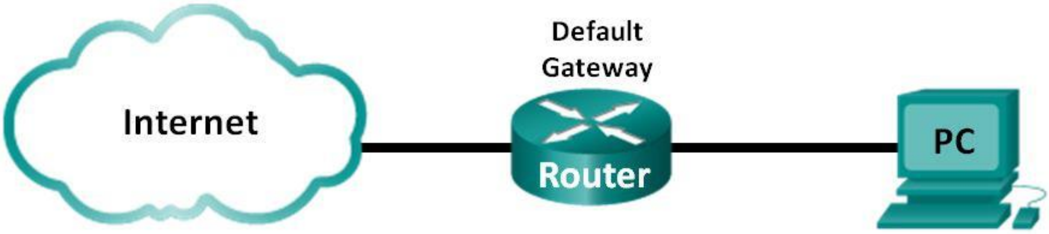
From your PC-C console session, after you successfully logged in, what was displayed in the log?



```
R2#show login
     A default login delay of 1 seconds is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 60 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 69 seconds.
         Login failures for current window: 0.
     Total login failures: 4.
```

# Task 4 - Observe the TCP 3-Way Handshake, UDP, and DNS

## Topology



Use your private PC with Internet Connectivity.

## Part 1: TCP 3-Way Handshake Analysis

### Step 1: Retrieve the PC interface addresses.

Connect your PC to the switch on your workbench. For this lab, you need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

| | |
|---|---|
| IP address | 192.168.0.4 |
| MAC address | 30-5A-3A-8B-D8-AD |
| Default gateway IP address | 192.168.0.1 |
| DNS server IP address | 192.168.0.1 |

### Step 2: Start Wireshark and select the appropriate interface.

### Step 3: Perform a website data capture.

a. - Start a data capture. Open a browser and go to www.dn.th-koeln.de.
- **Close (!)** the browser window to end the HTTP session, and return to Wireshark.
- Stop the data capture.

b. By nslookup record the IP address of www.dn.th-koeln.de: **139.6.19.7**

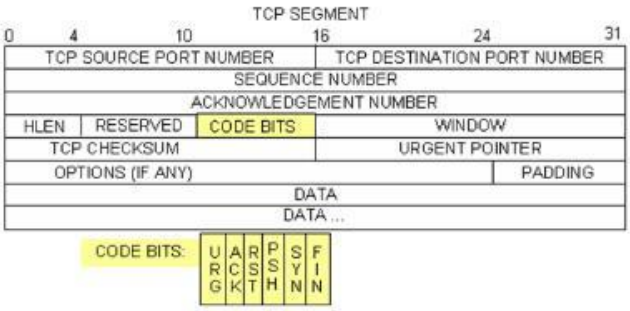
c. Check the Wireshark capture window.
Check the **Source**, **Destination**, and **Protocol** columns.
Find the appropriate packet for the start of the first TCP session to the Webserver in this capture.

**d. Filter your capture to this 1st TCP Session to the www.dn.th-koeln.de Webserver.**

Which Socket (IP address and Port) has been used by the webserver in the first TCP session you captured? **139.6.19.7:80**
Which Socket has been used by your Web client in the first TCP session? **192.168.0.4: 61143**

### Step 4: Analyze TCP Segments

The image shows a TCP datagram diagram.



a. Which three TCP messages start the setup of a TCP session?
**SYN (synchronize flag), SYN-ACK (synchronize-acknowledgement flag),ACK (acknowledge flag)**

**Note**: These messages are without any application data.

The web client initiates the TCP session. Select the 1st TCP message of a TCP session. Which flag is set in this first TCP segment? **SYN flag**

Record is the initial sequence number of the web client: **Sequence Number: Seq No=0**

b. Which TCP flags are set in the first response from the server? **SYN-ACK flag**

Record the sequence number and the acknowledgement number in this TCP message.

Seq No: **0** Ack No: **1**

c. Which TCP flag is set in the TCP segment, to finish the TCP 3-way-handshake? **ACK Flag**

Record the sequence number and the acknowledgement number in this TCP message.

Seq No: **1** Ack No: **0**

**Important Note:** in all TCP segments excluding the first segment, the ACK flag is set.

d. From the TCP 3-way-handshake packets record the initial TCP parameters **maximum windows size (WIN)** and **maximum segment size (MSS)** of the web client and the web server.

**Note**: By the window scale (WS) factor, the window size (WIN) is multiplied, check details of the Wirshark presentation of WS. (Answer yourself the Q: Is the DN-Webserver multiplier 7 or 128?)
**TCP Option - Window scale: 7 (multiply by 128)**

| Parameter | Web client | Web server |
|---|---|---|
| MSS | 1440 | 1380 |
| WIN | 64800 | 64800 |
| WS | 256 | 128 |
| WIN*WS | 64800*256 | 64800*128 |

### Step 5: Display IP flows by Wireshark.

a. In complex scenarios it is helpful to use additional analysis by Wireshark. For our HTTP session to www.heise.de show the TCP flow graph by selecting **Statistics – Flow Graph – TCP flow,** and display only TCP segments of the selected flow.

By which TCP messages is TCP closed? **FIN,ACK & ACK Flags**

**Note**: In TCP closing process, the ack. number is incremented without any data transmission.

b. The web client acknowledges the received TCP segment data (number of application bytes) by TCP packets with the ACK flag and the actual acknowledgement number.

Initial HTTP **client** ack. number after TCP session setup (SYN, SYN/ACK, **ACK**): ack$_{\text{initial}}$ = **1**

Final HTTP **client** ack. number, following the last closing FIN message(s): ack$_{\text{final}}$ = **640**

Calculate the number of Bytes M (TCP data = encapsulated HTTP data here), which has been received by the web **client** on application level.

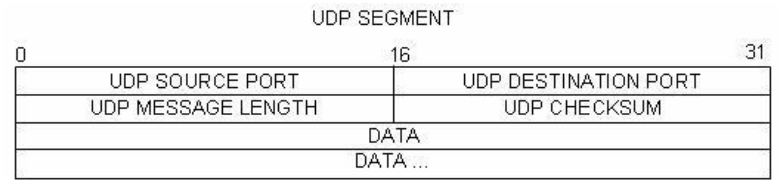
M = ack$_{\text{final}}$ – 1 – ack$_{\text{initial}}$

M =**640-1-0=639 BYTES**

## Part 4: Examine Captured DNS and UDP Packets

### Step 1: Continue and Examine UDP segment using DNS query.

From the same Wireshark capture, examine UDP by using a DNS query, as DNS is encapsulated in UDP. A UDP header only has four fields: source port, destination port, length, and checksum. Each field in UDP header is only 16 bits as depicted below.



UDP SEGMENT

0 16 31

| | |
|---|---|
| UDP SOURCE PORT | UDP DESTINATION PORT |
| UDP MESSAGE LENGTH | UDP CHECKSUM |
| DATA | |
| DATA ... | |

**Note**: If you do not see any results after the DNS filter was applied, close the web browser and in the command prompt window, type **ipconfig /flushdns**.
Restart the Wireshark capture and repeat the instructions in Part 2b –2e. If this does not resolve the issue, in the command prompt window, you can type **nslookup www.google.com as an alternative to the web browser.**

a. Which client socket is used for the DNS query (IP address, transport protocol, port number)?
**socket: 192.168.0.4:56912**
**transport protocol: UDP**

b. Which server socket is used for the DNS query (IP address, transport protocol, port number)?
**socket: 81.173.194.77:53**
**transport protocol: UDP**

c. Is your DNS server connected in the same subnet as your PC client? **y**

d. To the MAC address of which device is the DNS query sent? **c0:c5:22:eb:0f:6f**

e. In case you want to prevent your network of packet fragmentation, and the MTU size is 1500 Bytes, calculate the maximum UDP segment can be transferred.
**IP Header=20 bytes**
f. **MTU size=1500 bytes**
**therefore, Maximum UDP size= 1500-20=1480 bytes**

### Step 2: Examine DNS responses.

a. In your own DNS capture, evaluate the DNS query response and fill out the following table for the DNS query response message.

| DNS Flags / Answers | Value | Suggested Meaning |
|---|---|---|
| **Authoritative Server** Flag | **0** | **It is a Non-authoritative name server.**<br>**It does not have original source files.** |
| **Recursion desired** Flag | **1** | **Recursive request is desired** |
| **Recursion available** Flag | **1** | **Server can do recursive queries** |
| Answer **Name** | **www.google.com** | |
| Answer **Type** | **CNAME, A** | |
| Answer **Class** | **IN(0x0001)** | |
| Answer **Time to live** | **167 (2 minutes, 47 seconds)** | |
| Answer **Address** | **www.google.com (142.250.185.196)** | |

# Deliverables

## Lab Teams

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

## Module Group Exams

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

## Deliverables

Each teams uploads the following files:

- Create a PDF file **ITN-Lab3-Result.pdf** with the completed and answered **Lab Preparations and Lab Instructions**. All tasks must be worked on and all questions must be answered.
  Write your answers in **red color**. You may use the comment capabilities of the free Adobe reader.
- Save your final Packet Tracer file **ITN-Lab3-PT.pkt**
- Record the running configuration of router R1 and router R2 (show run) in one text file **ITN-Lab3-Configs.txt**

## Due Dates

| Group 1 | Teams 1-9 | Due Date |
|---|---|---|
| | Module Group Exams 14-15, 16-17 | 22.11. – EOB |
| | Upload Deliverables | 22.11. – EOB |
| | CCNA ZOOM Presentation | 24.11. - 16:45 ff. |
| | Final Exam / Skill Test | 26.11. – 15:00 ff. |

| Group 2 | Teams 1-9 | Due Date |
|---|---|---|
| | Module Group Exams 14-15, 16-17 | 29.11. - EOB |
| | Upload Deliverables | 29.11. - EOB |
| | CCNA ZOOM Presentation | 02.12. - 16:45 ff. |
| | Final Exam / Skill Test | 06.12. – 16:45 ff. |

- Per team you load one solution in Ilias in time.
- Per team you book one timeslot for acceptance.