CE231 – Assignment 1: Routing and Switching Essentials

Dr. M. Reed v3.3

Submission details (one document, one Packet Tracer file):

You will submit a SINGLE word processed document in one of the following formats:

- Word format (.doc or .docx)
- Portable document format (PDF)

You may either edit this document with the required information (and append answers to the parts you are asked to write), or write your own document containing the required information.

Submission time and place is as described in the Undergraduate Assignment Deadline Schedule.

The parts that you need to fill in or content to append are:

- Complete the blank fields in Table 1
- Complete the blank fields in Table 2
- Append the configurations of your configured routers and switches (only the output of "show running-config" with additional comments).
- Append the explanation for Task 8.

Additionally, you must submit your working Packet Tracer file with the **same** configuration as that given in the document.

You MUST use Packet Tracer 6.2.0 (or later) for this assignment, it is available for download in Windows from the CE231 Moodle page (or Cisco Network Academy site). You must use the provided scenario.pkt file available from the CE231 Moodle page.

Marks will be awarded as follows:

- 20% for Task 1 (Table 1 and Table 2)
- 35% for Tasks 2,3,4 and 5 (basic configuration of a working network)
- 20% for Task 6, Access Control Lists
- 5% for Task 7, Documentation and submission of Packet Tracer file.
- 20% for Task 8, Explanation of routing and switching decisions. 5/20 of these marks will be for good presentation including use of English and appropriate use of references.

NOTE: this document is a generic description for the whole group. Every student also has a unique combination of IP address range, VLAN identifiers and sizes of LANs distributed through the CE231 course pages. Under no circumstances should you use values allocated to another student – doing so will give rise to an investigation of plagiarism. You will find your own individual settings on the CE231 course page using your registration number as a key to your individual page.

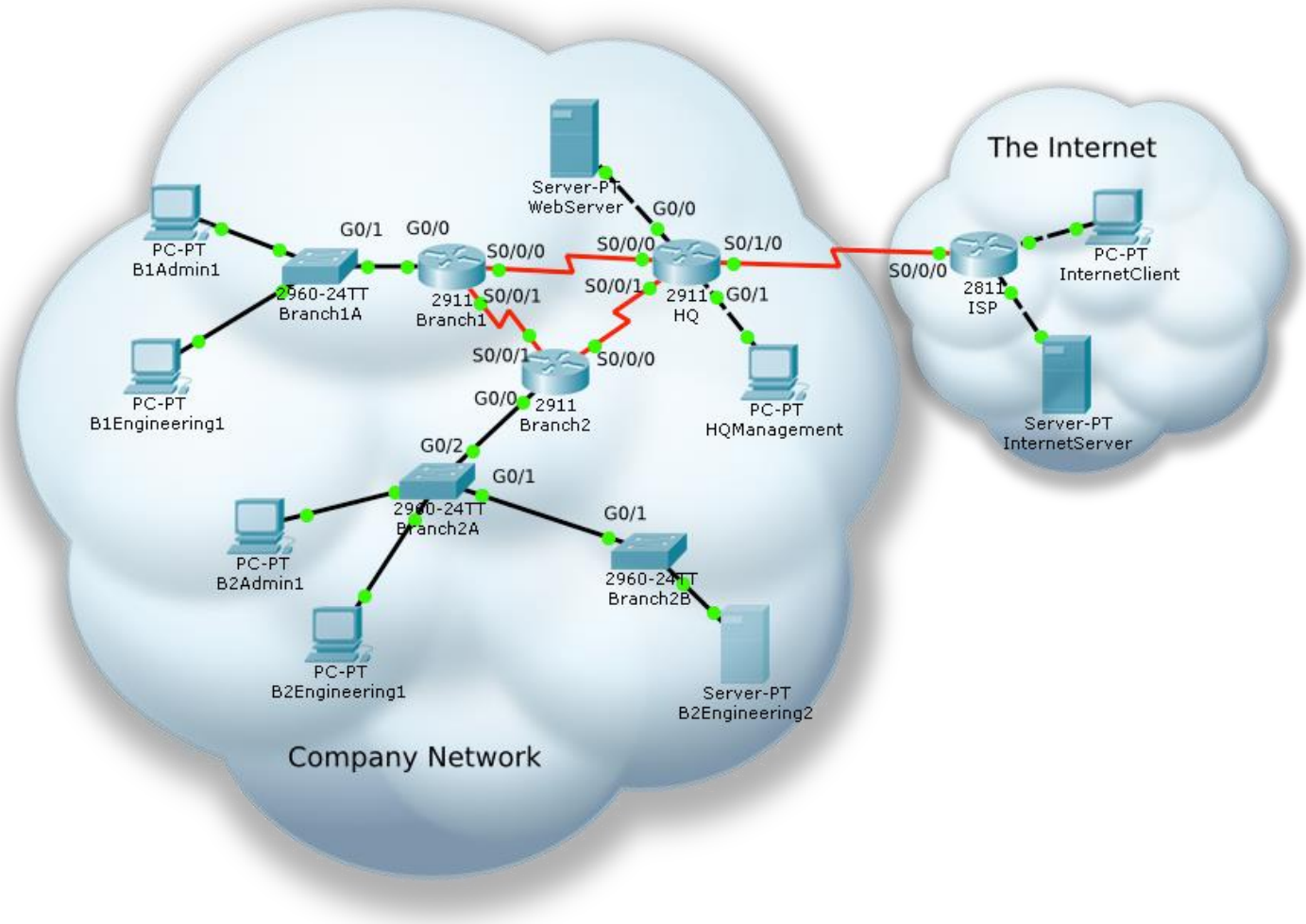

Figure 1 Assignment topology

Scenario

You are to design a new Company Network that is given to you in Figure 1 (also the Packet Tracer scenario). In this assignment, you have been given a summarized address range that you will use to create an efficient addressing scheme to accommodate all hosts on the network shown in Figure 1. You will use your own unique addresses, LAN sizes and VLAN allocations through a page accessed using your registration number from the CE231 courses page. A combination of a routing protocol and a static default route will be required so that hosts on networks not directly connected can communicate. You will also be required to set up access control lists. You must complete this assignment using Cisco Packet Tracer version 6.2.0 (or later).

Task 1: Create an Addressing Scheme.

Use the address range allocated to you to create an addressing scheme to accommodate all hosts on the network. You must begin the address assignments at the address given to you on your own unique page from the CE231 course page. You have been allocated the number of hosts on each network attached to each subnet; enter the number of hosts from your individual settings web page into Table 1 for the blank entries. **Note that a router interface counts as one host and is included in the number of hosts allocated to you. So "30 hosts" means: 1 router interface and 29 other hosts**. You also have individual settings for VLAN identifiers and some other addresses. Note that the settings on ISP have already been made and you **must not** change the settings in the ISP router.

Document all subnet addresses in Table 1.

Table 1

Device	Interface	Network Name	Number of Hosts	Subnet	Subnet Mask
HQ	G0/0	NetH1	2	202.202.25.0	255.255.255.0
	G0/1	NetH2	8	192.168.24.112	255.255.255.240
	S0/0/0	NetHB1	2	192.168.24.144	255.255.255.252
	S0/0/1	NetHB2	2	192.168.24.156	255.255.255.252
	S0/1/0	NetISP	2	123.123.123.0	255.255.255.0
Branch1	G0/0.A1	VLAN A1	9	192.168.24.96	255.255.255.240
	G0/0.E1	VLAN E1	17	192.168.24.64	255.255.255.224
	G0/0.M1	VLAN M1	5	192.168.24.128	255.255.255.248
	S0/0/0	NetHB1	2	192.168.24.144	255.255.255.252
	S0/0/1	NetB12	2	192.168.24.152	255.255.255.252
Branch2	G0/0.A2	VLAN A2	25	192.168.24.0	255.255.255.224
	G0/0.E2	VLAN E2	25	192.168.24.32	255.255.255.224
	G0/0.M2	VLAN M2	5	192.168.24.136	255.255.255.248
	S0/0/0	NetHB2	2	192.168.24.156	255.255.255.252
	S0/0/1	NetB12	2	192.168.24.152	255.255.255.252

Document router/switch interface and PC addresses in Table 2.

Assign the **las**t usable IP address of each LAN to a **router** interface. Replace "first from VLAN …" with your actual address.

Table 2

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0	202.202.25.254	255.255.255.0	N/A
	G0/1	192.168.24.126	255.255.255.240	N/A
	S0/0/0	192.168.24.145	255.255.255.252	N/A
	S0/0/1	192.168.24.157	255.255.255.252	N/A
	S0/1/0	123.123.123.27	255.255.255.0	
Branch1	G0/0.A1	192.168.24.110	255.255.255.240	N/A
	G0/0.E1	192.168.24.94	255.255.255.224	N/A
	G0/0.M1	192.168.24.142	255.255.255.248	N/A
	S0/0/0	192.168.24.146	255.255.255.252	N/A
	S0/0/1	192.168.24.154	255.255.255.252	N/A
Branch2	G0/0.A2	192.168.24.30	255.255.255.224	N/A
	G0/0.E2	192.168.24.62	255.255.255.224	N/A
	G0/0.M2	192.168.24.134	255.255.255.248	N/A
	S0/0/0	192.168.24.158	255.255.255.252	N/A
	S0/0/1	192.168.24.153	255.255.255.252	N/A
ISP	Fa0/0	155.245.0.254	255.255.255.0	N/A
	Fa0/1	155.245.1.254	255.255.255.0	N/A
	S0/0/0	123.123.123.254	255.255.255.0	None
B1Admin1	Ethernet	192.168.24.97	255.255.255.240	192.168.24.110
B1Engineering1	Ethernet	192.168.24.65	255.255.255.224	192.168.24.94
B2Admin1	Ethernet	192.168.24.1	255.255.255.224	192.168.24.30
B2Engineering1	Ethernet	192.168.24.33	255.255.255.224	192.168.24.62
B2Engineering2	Ethernet	192.168.24.34	255.255.255.224	192.168.24.62
WebServer	Ethernet	202.202.25.1	255.255.255.0	202.202.25.254
HQManagement	Ethernet	192.168.24.113	255.255.255.240	192.168.24.126
InternetClient	Ethernet	155.245.1.1	255.255.255.0	155.245.1.254
InternetServer	Ethernet	155.245.0.1	255.255.255.0	155.245.0.254
Branch1A	VLAN M1	192.168.24.129	255.255.255.248	192.168.24.142
Branch2A	VLAN M2	192.168.24.137	255.255.255.248	192.168.24.146
Branch2B	VLAN M2	192.168.24.138	255.255.255.248	192.168.24.146

Task 2: Configure basic device settings.

Configure the routers and switches according to the following guidelines:

- Routers/switches should be secured against unauthorised access and passwords should be stored in a secure manner. Use only the password “cisco” in your configurations.
- There is no DNS server in the network.
- Configure a message-of-the-day banner that warns against unauthorized use and states “This router is managed by 0123456”, where 0123456 is **replaced with your registration number**.
- Console input should not be broken with console output messages.

Task 3: Configure switches, router interfaces and hosts.

There are only a few hosts present in the Packet Tracer scenario you have been issued with (and shown in Figure 1), but you will be assigning ports ready for future hosts to be added. The number of expected hosts was issued in your individual settings.

Assign VLAN identifiers to the access ports in the switches. In switch Branch1A, the Admin hosts (VLAN A1) are to be assigned the lower number ports (Fa0/1 ….) and the Engineering hosts (VLAN E1) the higher number ports (… Fa0/24). Assign half of the VLAN A2 admin hosts to the lower numbered ports of switch Branch2A and the other half of the A2 hosts to the lower numbered ports of switch Branch2B. For the VLAN E2 hosts, assign half to the upper ports of Branch2A and half to the upper ports of Branch2B. VLANs M1 and M2 are the VLANs used to manage the switches.

Assign router and switch VLAN interface IP addresses as you have documented in your design in Table 2.

Switch ports should be secured such that only ports actually connected are active. All access switch ports should be secured such that they remember the first connected device; any other devices connected in the future will cause the switch port to be disabled.

Assign the appropriate ports to act as trunk ports.

Configure the hosts appropriately.

Task 4: Configure routing

Configure OSPF on all Company Network routers (*i.e.* not ISP) to advertise all directly connected networks. HQ should have a default route to “The Internet” (ISP and the connected devices) and this default route should be *propagated (distributed)* to all other routers. The default route in HQ should be the only static route in any of the routers (except those already pre-set in ISP). All hosts should be able to ping each other. Routers should not advertise, or listen to, routing updates on any unnecessary networks.

Task 5: Configure secure remote access

Configure each router and switch (except ISP) to allow remote, command line, management using the most secure protocol available.

Task 6: Configure Access Control Lists

Note this part of the assignment is intentionally difficult and getting it all correct should be considered an extension task. If you wish to attempt only some of this task (for reduced marks) simply implementing points 6 and 7 in Step 2 will demonstrate that you understand the basics of ACLs.

Step 1: Ensure that you have full connectivity between the end hosts before configuring ACLs.

Step 2: Configure access control lists to provide the following policy in the Company Network

1. Only allow hosts in NetH2 (including HQManagement) to remotely manage the routers and switches in the Company Network. You will need to think carefully about where on each router this ACL is applied as it is about input to the router management interface, not traffic through it.
2. Do not allow any TCP connections from the Internet into the Company Network except for the particular traffic to WebServer specified in part 3 of the policy.
3. Allow all clients in the Internet (including InternetClient and InternetServer) to connect to WebServer using HTTP. This must be the only host in the Company Network accessible to connections from the Internet.
4. Do not allow any hosts in NetH1 to access any TCP servers in the Company Network or send UDP traffic into the Company Network.
5. Allow hosts in the Company Network to access TCP servers in NetH1.
6. Allow hosts in the Company Network to connect to, and access, HTTP servers in the "Internet".
7. All other traffic to, or from, the Internet not specified above should be blocked.

Explanation of this policy: this policy would be suitable for a company where NetH1 is a "demilitarized zone" containing the company's Internet facing servers. Servers in NetH1 are open to compromise from the Internet so we do not want to allow connections from those servers to the rest of the network. HQManagement could be a management terminal, which is allowed to remotely manage the routers and switches.

Step 3: Test policy

Check that each of the policy points is implemented by performing appropriate tests. Note that Packet Tracer allows testing of HTTP. Also Telnet and SSH can be attempted from the Packet Tracer command prompt in a PC or server.

Task 7: Document configurations and include in your submitted document.

For each router and switch (except ISP), copy the output of "show running-config" into a text editor (or Word) and add comments to each part of the configuration e.g. the name of each LAN on each interface). You can add comments to a configuration using the "!" symbol at the start of entering a line and the `description` command for all interfaces.

```
R1#show running-config
Building configuration...

Current configuration : 3281 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
!Encrypts all passwords
service password-encryption
!
hostname R1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
no ip cef
no ipv6 cef
!SSH details
username cisco privilege 15 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```



```
!
license udi pid CISCO2911/K9 sn FTX1524S8IG
!IP domain name was found on Router already pre-setup
no ip domain-lookup
ip domain-name span.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
description its WebServer which connects to HQ router
ip address 202.202.25.254 255.255.255.0
ip access-group HQ_ALLOW_TCP in
duplex auto
speed auto
!
interface GigabitEthernet0/1
description its HQManagement connection
ip address 192.168.24.126 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
description Links to Branch1 router
ip address 192.168.24.145 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
description Links to Branch2 router
ip address 192.168.24.157 255.255.255.252
clock rate 128000
!Access group lets only HTTP out link to ISP router.
interface Serial0/1/0
ip address 123.123.123.27 255.255.255.0
ip access-group HQ_INTERNET out
!Clock rate because DCE connection.
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!OSPF for communicating between routers.
router ospf 1
log-adjacency-changes
network 192.168.24.157 0.0.0.0 area 0
network 192.168.24.145 0.0.0.0 area 0
network 192.168.24.0 0.0.0.255 area 0
default-information originate
```



```
!
ip classless
!Static default route to ISP router.
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
!
ip flow-export version 9
!Access list for allowing all TCP protocols to WebServer.
ip access-list extended HQ_ALLLOW_TCP
permit tcp 192.168.24.0 0.0.0.255 202.202.25.0 0.0.0.255 eq domain
permit tcp 192.168.24.0 0.0.0.255 202.202.25.0 0.0.0.255 eq ftp
permit tcp 192.168.24.0 0.0.0.255 202.202.25.0 0.0.0.255 eq pop3
permit tcp 192.168.24.0 0.0.0.255 202.202.25.0 0.0.0.255 eq smtp
permit tcp 192.168.24.0 0.0.0.255 202.202.25.0 0.0.0.255 eq telnet
permit tcp 192.168.24.0 0.0.0.255 202.202.25.0 0.0.0.255 eq www
!Access list for allowing out interface for HTTP.
ip access-list extended HQ_INTERNET
permit tcp any any eq www
!Access list for not allowing TCP protocols for WebServer to other
networks.
ip access-list extended H1_TCP
deny tcp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq domain
deny tcp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq ftp
deny tcp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq pop3
deny tcp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq smtp
deny tcp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq telnet
deny tcp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq www
!Access list for no allowing UDP protocols for Webserver to other
networks.
ip access-list extended H1_UDP
deny udp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq bootpc
deny udp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq bootps
deny udp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq domain
deny udp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq isakmp
deny udp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq non500-
isakmp
deny udp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq snmp
deny udp 202.202.25.0 0.0.0.255 192.168.24.0 0.0.0.255 eq tftp
!
no cdp run
!Banner of the day.
banner motd ^CUnauthorized access is prohibited this Router is
managed by 1402039^C
!
line con 0
password 7 0822455D0A16
logging synchronous
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
logging synchronous
login local
transport input ssh
!
```



```
End
R2#show running-config
Building configuration...

Current configuration : 1930 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
no ip cef
no ipv6 cef
!
username cisco privilege 15 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO2911/K9 sn FTX15247GAH
!
no ip domain-lookup
ip domain-name span.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.54
 description Sub-interface belongs to VLAN54 ports
 encapsulation dot1Q 54
 ip address 192.168.24.110 255.255.255.240
!
interface GigabitEthernet0/0.124
 description Sub-interface belongs to VLAN124 ports
 encapsulation dot1Q 124
 ip address 192.168.24.94 255.255.255.224
!
interface GigabitEthernet0/0.174
 description Sub-interface is for Remotly access to S1
 encapsulation dot1Q 174
 ip address 192.168.24.142 255.255.255.248
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
```



```
 speed auto
 shutdown
!
interface Serial0/0/0
 description Linked to HQ router
 ip address 192.168.24.146 255.255.255.252
!
interface Serial0/0/1
 description Linked to Branch2 router
 ip address 192.168.24.154 255.255.255.252
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 2
 log-adjacency-changes
 network 192.168.24.0 0.0.0.255 area 0
 network 192.168.24.146 0.0.0.0 area 0
 network 192.168.24.154 0.0.0.0 area 0
!
ip classless
!
ip flow-export version 9
!
no cdp run
!
banner motd ^CUnauthorized access is prohibited this Router is
managed by 1402039^C
!
line con 0
 password 7 0822455D0A16
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 access-class Management in
 password 7 0822455D0A16
 logging synchronous
 login local
 transport input ssh
!
End
R3#show running-config
Building configuration...

Current configuration : 1893 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
```



```
hostname R3
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
no ip cef
no ipv6 cef
!
username cisco privilege 15 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO2911/K9 sn FTX1524ABCP
!
no ip domain-lookup
ip domain-name span.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.69
 description Sub-interface links to VLAN69 ports
 encapsulation dot1Q 69
 ip address 192.168.24.30 255.255.255.224
!
interface GigabitEthernet0/0.104
 description Sub-interface links to VLAN104 ports
 encapsulation dot1Q 104
 ip address 192.168.24.62 255.255.255.224
!
interface GigabitEthernet0/0.204
 description Sub-interface used to remotly manage Branch2A and
Branch2B
 encapsulation dot1Q 204
 ip address 192.168.24.134 255.255.255.248
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description Links to HQ router
 ip address 192.168.24.158 255.255.255.252
!
interface Serial0/0/1
 description Links to Branch1 router
 ip address 192.168.24.153 255.255.255.252
```



```
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 3
 log-adjacency-changes
 network 192.168.24.158 0.0.0.0 area 0
 network 192.168.24.0 0.0.0.255 area 0
 network 192.168.24.153 0.0.0.0 area 0
!
ip classless
!
ip flow-export version 9
!
no cdp run
!
banner motd ^CUnauthorized access is prohibited this Router is
managed by 1402039^C
!
line con 0
 password 7 0822455D0A16
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 logging synchronous
 login local
 transport input ssh
!
End
S1#show running-config
Building configuration...

Current configuration : 5701 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
no ip domain-lookup
ip domain-name span.com
!
username cisco secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
spanning-tree mode pvst
!Port-security enables features of security. Sticky learns first
address connected. Maximum is 1 for interface. Violation is shutdown.
```



```
interface FastEthernet0/1
 description Interfaces linked to VLAN 54
 switchport access vlan 54
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00E0.B01C.BB4C
!
interface FastEthernet0/2
 description Interfaces linked to VLAN 54
 switchport access vlan 54
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/3
 description Interfaces linked to VLAN 54
 switchport access vlan 54
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/4
 description Interfaces linked to VLAN 54
 switchport access vlan 54
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 description Interfaces linked to VLAN 54
 switchport access vlan 54
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 description Interfaces linked to VLAN 54
 switchport access vlan 54
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 description Interfaces linked to VLAN 54
 switchport access vlan 54
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
 description Interfaces linked to VLAN 54
 switchport access vlan 54
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
```



```
!
interface FastEthernet0/9
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/10
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/13
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/14
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/15
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/16
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
```



```
!
interface FastEthernet0/17
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.C72D.9635
!
interface FastEthernet0/19
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/20
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/21
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/22
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/23
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/24
 description Interfaces linked to VLAN 124
 switchport access vlan 124
 switchport mode access
 switchport port-security
```



```
 switchport port-security mac-address sticky
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan174
 ip address 192.168.24.129 255.255.255.248
!
ip default-gateway 192.168.24.142
!
banner motd ^CUnauthorized access is prohibited this Switch is
managed by 1402039^C
!
line con 0
 password 7 0822455D0A16
 logging synchronous
 login
!
line vty 0 4
 password 7 0822455D0A16
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 logging synchronous
 login local
 transport input ssh
!
End
S2#show running-config
Building configuration...

Current configuration : 5687 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
no ip domain-lookup
ip domain-name span.com
!
username cisco secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
spanning-tree mode pvst
```



```
!
interface FastEthernet0/1
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5E96.4CE6
!
interface FastEthernet0/3
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/4
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
```



```
 switchport port-security mac-address sticky
!
interface FastEthernet0/9
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/10
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 description Interface linked to VLAN 69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/13
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/14
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/15
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/16
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
```



```
 switchport port-security mac-address sticky
!
interface FastEthernet0/17
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/20
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/21
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/22
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/23
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/24
 description Interface linked to VLAN 104
 switchport access vlan 104
 switchport mode access
 switchport port-security
```



```
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0004.9A4A.D4CA
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan204
 description Manage S2 remotly
 ip address 192.168.24.137 255.255.255.248
!
banner motd ^CUnauthorized access is prohibited this Switch is
managed by 1402039^C
!
line con 0
 password 7 0822455D0A16
 logging synchronous
 login
!
line vty 0 4
 password 7 0822455D0A16
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 logging synchronous
 login local
 transport input ssh
!
End
S3#show running-config
Building configuration...

Current configuration : 5524 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S3
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
no ip domain-lookup
ip domain-name span.com
!
spanning-tree mode pvst
!
```



```
interface FastEthernet0/1
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/3
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/4
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/7
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/8
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
```



```
interface FastEthernet0/9
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/10
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/11
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/12
 description Interface linked to VLAN69
 switchport access vlan 69
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/13
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/14
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/15
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/16
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
```



```
interface FastEthernet0/17
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/18
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/19
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/20
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/21
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/22
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/23
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/24
 description Interface linked to VLAN104
 switchport access vlan 104
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00D0.D3E2.C060
```



```
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan204
 description Manages S3 remotly
 ip address 192.168.24.138 255.255.255.248
!
banner motd ^CUnauthorized access is prohibited this Switch is
managed by 1402039^C
!
line con 0
 password 7 0822455D0A16
 logging synchronous
 login
!
line vty 0 4
 password 7 0822455D0A16
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 logging synchronous
 login local
 transport input ssh
!
end
```

Task 8: Explain switching and routing decisions

First of all, B2Engineering2 send out a frame to f0/24 which receives the frame, it is then checked against port security as it is enabled. Mac entry is then checked against Mac address table, it passes the security and frame is passed. First it send out unicast frame, then switch looks at Mac address table for destination Mac address. Outgoing port for that switch is a trunk port and vlan number matches therefore it is allowed in a trunk. Switch send out frame to the port and only then g0/1 port send out a frame. Branch2A switch port g0/1 receives the frame, frame is then checked for source mac address, it passes, and then switch looks in its mac table for mac destination address. Following two steps are the same as previous switch.

Branch2 router then receives the frame, sub interface accepts the frame for his vlan, matches the mac address on both sides, de-encapsulates the frame, looks at the routing table, finds the IP address, then decrements the TTL[1] on the packet. It encapsulates the packet into HDLC [2] frame and sends it out to s0/0/0 interface. Interface s0/0/1 on HQ router receives the frame, de-encapsulates from HDLC [2] and sends it to upper layer. Router looks up IP address in routing table, it finds the destination IP address, decrements TL on the packet, then checks it on outgoing port which has access-list, packet

matches the criteria, packet is being permitted to encapsulate the packet into HDLC [2] frame and send out to s0/1/0 interface on HQ router. After that ISP router follows the same four steps as HQ router then he received the frame, and after it check the next-hop ip address, it is unicast, then ARP[3] process looks up ARP[3] table, if it matches the ARP[3] table. ARP [3] process sets frames destination mac address found in the table and encapsulates PDU [4] into Ethernet frame. Interface f0/0 sends out the frame, following port of course receives the frames matches with Mac address table information, then device de-encapsulates PDU [4] from ethernet frame, the next layer matches the ip addresses or broadcast addresses. Device de-encapsulates the packet, receives TCP SYN [5] segment which segment information. Connection reqest is accepted and device sets state to SYN_RECEIVED [5]. After that device sends TCP SYN+ACK [5] segment with segment information, it sees that destination ip address is not in the same subnet or not the same broadcast so default gateway is set and sets the next-hop as default gateway.

After that packet travels the same path it did on all the devices on his route till it reaches the B2Engineering2 device, packet is then receives on that device with TCP SYN+ACK[5] segment with al segment information, as it should TCP [5] segment sequence number is as expected and TCP[5] connection is successful. Then device sets connection state to FIN_WAIT_1, and sends the packet back to Internet server with same default-gateway. At the same time devices prepares next packet with TCP FIN+ACK [5] segment and sends on that default-gateway as well. Following after that two packets travel again on the same route to internet server, after it receives it device sets connections state to ESTABLISHED and waits for next packet to arrive.

Finally second packet arrives with TCP FIN+ACK [5] segment which changes established state to CLOSE_WAIT and LAST_ACK. And then again sends a packet to B2Engineering2 device with TCP FIN+ACK [5] segment. Packet travels again the same route to B2Engineering2 device, but now TCP segments sets connection state to CLOSING, and as confirmation sends TCP ACK [5] packet back to Internet Server, after it receives it Internet Server sets connection state to CLOSED and this means that packets successfully travelled and got the connection.

References:
[1] Time To Live (TTL) Processing. https://tools.ietf.org/html/rfc3443
[2] High-Level Data Link Control (HDLC) Frame. https://tools.ietf.org/html/rfc4349
[3] An Ethernet Address Resolution Protocol. https://tools.ietf.org/html/rfc826
[4] Protocol Operations for the Simple Network Management Protocol.
https://tools.ietf.org/html/rfc3416
[5] Transmission Control Protocol. https://tools.ietf.org/html/rfc793

End of Assignment

