11 Cisco Device Functions - Lab Exercise
12 The Life of a Packet - Answer Key
13 The Cisco Troubleshooting Methodology - Answer Key
14 Cisco Router and Switch Basics - Answer Key
15 Cisco Device Management - Answer Key.
16 Routing Fundamentals - Answer Key
17 Dynamic Routing Protocols - Answer Key
18 Connectivity Troubleshooting - Answer Key
19-1 RIP Configuration - Answer Key
20-1 EIGRP Configuration - Answer Key
21-1 OSPF Configuration - Answer Key.
23-1 VLAN and Inter-VLAN Routing Configuration - Answer Key
24-1 DHCP Configuration - Lab Exercise
25-1 HSRP Configuration - Answer Key
26-1 Spanning Tree Troubleshooting - Answer Key.
27-1 EtherChannel Configuration - Answer Key
28-1 Port Security Configuration Answer Key
29-1 ACL Configuration - Answer Key
30-1 NAT Configuration - Answer Key
31 IPv6 Addressing Configuration - Answer Key
32-1 IPv6 Routing Configuration - Answer Key
33-1 WAN Configuration - Answer Key.
34-1 BGP Configuration - Answer Key
35-1 Cisco Device Security Configuration - Answer Key
36 Network Device Management - Answer Key

Router Configurations
IOS Basics & Device Functions (04, 11, 12, 14, 15)

```
enable
configure terminal
hostname R1
no ip domain-lookup
enable secret cisco123
service password-encryption
username admin privilege 15 secret cisco123
ip domain-name ccna.lab
crypto key generate rsa modulus 1024
```

```
line console 0
password cisco123
login
logging synchronous
line vty 0 15
login local
transport input ssh
```

Interface & Packet Flow (12, 16)

```
interface g0/0
description LAN-Connection
ip address 192.168.10.1 255.255.255.0
no shutdown
duplex full
speed 1000
```

Static Routing (16)

```
ip route 0.0.0.0 0.0.0.0 209.165.200.226
ip route 172.16.20.0 255.255.255.0 192.168.10.2
show ip route
```

Dynamic Routing (17, 19-1, 20-1, 21-1)

RIP v2:

```
router rip
version 2
no auto-summary
network 192.168.10.0
network 172.16.20.0
passive-interface g0/0
```

EIGRP:

```
router eigrp 100
network 192.168.10.0 0.0.0.255
network 172.16.20.0 0.0.0.255
no auto-summary
```

OSPF:

```
router ospf 1
router-id 1.1.1.1
network 192.168.10.0 0.0.0.255 area 0
network 172.16.20.0 0.0.0.255 area 0
passive-interface default
no passive-interface g0/1
```

VLAN Router-on-a-Stick (23-1)

```
interface g0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
interface g0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
```

DHCP Server (24-1)

```
ip dhcp excluded-address 192.168.10.1 192.168.10.20
ip dhcp pool VLAN10_POOL
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8 8.8.4.4
```

HSRP (25-1)

```
interface g0/0
ip address 192.168.10.2 255.255.255.0
standby 10 ip 192.168.10.1
standby 10 priority 110
standby 10 preempt
standby 10 track g0/1 20
```

ACLs (29-1)

```
ip access-list extended TELNET_BLOCK
deny tcp 172.16.20.0 0.0.0.255 any eq 23
permit ip any any
interface g0/1
ip access-group TELNET_BLOCK in
```

NAT/PAT (30-1)

```
access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 interface g0/1 overload
interface g0/0
ip nat inside
interface g0/1
ip nat outside
```

IPv6 (31, 32-1)

```
ipv6 unicast-routing
interface g0/0
ipv6 address 2001:DB8:10:1::1/64
ipv6 enable
interface g0/1
```

```
ipv6 address 2001:DB8:20:1::1/64
ipv6 route ::/0 2001:DB8:20:1::2
```

WAN Serial (33-1)

```
interface s0/0/0
ip address 10.1.1.1 255.255.255.252
encapsulation ppp
clock rate 64000
no shutdown
```

BGP (34-1)

```
router bgp 65001
bgp log-neighbor-changes
neighbor 10.1.1.2 remote-as 65002
neighbor 10.1.1.2 update-source s0/0/0
address-family ipv4
network 192.168.10.0 mask 255.255.255.0
Exit-address-family
```

Switch Configurations

IOS Basics & Device Functions (04, 11, 14, 15)

```
enable
configure terminal
hostname SW1
enable secret cisco123
service password-encryption
interface vlan 1
ip address 192.168.10.2 255.255.255.0
no shutdown
ip default-gateway 192.168.10.1
```

VLANs & Trunks (23-1)

```
vlan 10
name USERS
vlan 20
name SERVERS
interface range f0/1 - 10
switchport mode access
switchport access vlan 10
switchport port-security maximum 2
switchport port-security mac-address sticky
interface range f0/11 - 20
switchport mode access
```

```
switchport access vlan 20
interface g0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,99
switchport trunk native vlan 99
```

Spanning Tree (26-1)

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20 root primary
spanning-tree portfast default
spanning-tree portfast bpduguard default
interface range f0/1 - 24
spanning-tree portfast
```

EtherChannel (27-1)

```
interface range g0/1 - 2
channel-group 1 mode active
switchport mode trunk
switchport trunk allowed vlan 10,20
exit
interface port-channel 1
switchport mode trunk
switchport trunk allowed vlan 10,20
```

Port Security (28-1)

```
interface f0/5
switchport mode access
switchport access vlan 10
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
```

Device Management (35-1, 36)

```
ip domain-name ccna.lab
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 15
transport input ssh
login local
ntp server 192.168.10.1
logging host 192.168.10.10
logging trap informational
snmp-server community CCNA_RO RO
banner motd #Authorized Access Only#
```

Troubleshooting Commands (13, 18)

Router:

show ip interface brief
show ip route
show ip protocols
show cdp neighbors detail
show controllers s0/0/0
debug ip packet
undebug all

Switch:

show vlan brief
show interfaces trunk
show spanning-tree
show mac address-table
show port-security interface f0/1
show etherchannel summary

Save All:

copy running-config startup-config
write memory

Cisco Commands

Changing switch hostname	
Switch(config)#hostname **SW1**	
Configuring passwords	
SW1(config)#enable secret **cisco**	MD5 hash.
SW1(config)#enable password **notcisco**	Clear text.
Securing console port	
SW1(config)#line con 0 SW1(config-line)#password **cisco** SW1(config-line)#login	
Securing terminal lines	
SW1(config)#line vty 0 4 SW1(config-line)#password **cisco** SW1(config-line)#login	
Encrypting passwords	
SW1(config)#service password-encryption	
Configuring banners	
SW1(config)#banner motd $ -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- **UNAUTHORIZED ACCESS IS PROHIBITED** -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- $	
Giving the switch an IP address	
SW1(config)#interface vlan 1 SW1(config-if)#ip address **172.16.1.11 255.255.255.0** (or **dhcp)** SW1(config-if)#shutdown	
Setting the default gateway	
SW1(config)#ip default-gateway **172.16.1.1**	
Saving configuration	
SW1#copy running-config startup-config Destination filename [startup-config]? Building configuration… [OK]	Press enter to confirm file name.
SW1#wr Building configuration… [OK]	Short for write memory.
Working environment (name lookup, history, exec-timeout and logging behavior)	
SW1(config)#no ip domain-lookup SW1(config)#line vty 0 4 SW1(config-line)#history size **15** SW1(config-line)# exec-timeout **10 30** SW1(config-line)#logging synchronous	Also valid for line con 0.
Configuring switch to use SSH	
• **Configure DNS domain name:** SW1(config)#ip domain-name **example.com** • **Configure a username and password:** SW1(config)#username **admin** password **cisco** • **Generate encryption keys:** SW1(config)#crypto key generate rsa How many bits in the modulus [512]: **1024** • **Define SSH version to use:** SW1(config)#ip ssh version 2 • **Enable vty lines to use SSH:** SW1(config)#line vty 0 4 SW1(config-line)#login local SW1(config-line)#transport input telnet ssh	The size of the key modulus in the range of 360 to 2048. You can set vty lines to use only telnet or only ssh or both as in the example.

Aliases	
SW1(config)#alias exec **c** configure terminal SW1(config)#alias exec **s** show ip interface brief SW1(config)#alias exec **sr** show running-config	Used to create shortcuts for long commands.
Description, speed and duplex	
SW1(config)#interface fastEthernet 0/1 SW1(config-if)#description **LINK TO INTERNET ROUTER** SW1(config-if)#speed 100 **(options: 10, 100, auto)** SW1(config)#interface range fastEthernet 0/5 – 10 SW1(config-if-range)#duplex full **(options: half, full, auto)**	The **range** keyword used to set a group of interfaces at once.

Verify Basic Configuration	
SW1#show version	Shows information about the switch and its interfaces, RAM, NVRAM, flash, IOS, etc.
SW1#show running-config	Shows the current configuration file stored in DRAM.
SW1#show startup-config	Shows the configuration file stored in NVRAM which is used at first boot process.
SW1#show history	Lists the commands currently held in the history buffer.
SW1#show ip interface brief	Shows an overview of all interfaces, their physical status, protocol status and ip address if assigned.
SW1#show interface vlan 1	Shows detailed information about the specified interface, its status, protocol, duplex, speed, encapsulation, last 5 min traffic.
SW1#show interfaces description	Shows the description of all interfaces
SW1#show interfaces status	Shows the status of all interfaces like connected or not, speed, duplex, trunk or access vlan.
SW1#show crypto key mypubkey rsa	Shows the public encryption key used for SSH.
SW1#show dhcp lease	Shows information about the leased IP address (when an interface is configured to get IP address via a dhcp server)

Configuring port security	
• **Make the switch interface as access port:** SW1(config-if)#switchport mode access • **Enable port security on the interface:** SW1(config-if)#switchport port-security • **Specify the maximum number of allowed MAC addresses:** SW1(config-if)#switchport port-security maximum 1 • **Define the action to take when violation occurs:** SW1(config-if)#switchport port-security violation shutdown **(options: shutdown, protect, restrict)** • **Specify the allowed MAC addresses:** SW1(config-if)#switchport port-security mac-address **68b5.9965.1195** **(options: H.H.H, sticky)**	The **sticky** keyword is used to let the interface dynamically learns and configures the MAC addresses of the currently connected hosts.

Verify and troubleshoot port security	
SW1#show mac-address-table	Shows the entries of the mac address table
SW1#show port-security	overview of port security of all interfaces
SW1#show port-security interface fa0/5	Shows detailed information about port security on the specified interface

Configuring VLANs	
• **Create a new VLAN and give it a name:** SW1(config)#vlan 10 SW1(config-vlan)#name SALES • **Assign an access interface to access a specific VLAN:** SW1(config)#interface fastEthernet 0/5 SW1(config-if)#switchport mode access SW1(config-if)#switchport access vlan 10	

Configuring an auxiliary VLAN for cisco IP phones	
SW1(config)#interface fastEthernet 0/5 SW1(config-if)#switchport access vlan 10 SW1(config-if)#switchport voice vlan 12	accessing vlan 10 (data) and 12 (VoIP)
Configuring Trunks	
SW1(config)#interface fastEthernet 0/1 SW1(config-if)#switchport mode trunk **(options: access, trunk, dynamic auto, dynamic desirable)** SW1(config-if)#switchport trunk allowed vlan add **10** **(options: add, remove, all, except)**	
Securing VLANS and Trunking	
• **Administratively disable unused interfaces:** SW1(config-if)#shutdown • **Prevent trunking by disabling auto negotiation on the interface:** SW1(config-if)#nonegotiate (or hardcode the port as an access port) SW1(config-if)#switchport mode access • **Assign the port to an unused VLAN:** SW1(config-if)#switchport access vlan 222	
Configuring VTP	
• **Configure VTP mode:** SW1(config)#vtp mode server **(options: server, client, transparent)** • **Configure VTP domain name:** SW1(config)#vtp domain **EXAMPLE (case-sensitive)** • **Configure VTP password: (optional)** SW1(config)#vtp password **cisco (case-sensitive)** • **Configure VTP pruning: (optional)** SW1(config)#vtp pruning **(only works on VTP servers)** • **Enable VTP version 2: (optional)** SW1(config)#vtp version 2 • **Bring up trunks between the switches**	The **transparent** VTP mode is used when an engineer wants to deactivate VTP on a particular switch

Verify and troubleshoot VLANS and VTP	
SW1#show interfaces *if* **switchport**	Lists information about administrative setting and operation status of interface
SW1#show interfaces trunk	Lists all the trunk ports on a switch including the trunk allowed VLANS
SW1#show vlan {brief| id| name| summary}	Lists information about the VLANs
SW1#show vtp status	Lists VTP configuration (mode, domain name, version, etc) and **revision** number
SW1#show vtp password	Shows the VTP password

STP optimization	
• **Hard coding the root bridge** (changing bridge priority): SW1(config)#spanning-tree vlan 1 root primary SW1(config)#spanning-tree vlan 1 root secondary SW1(config)#spanning-tree **[vlan 1]** priority 8192 • **Changing the STP mode:** SW1(config)#spanning-tree mode rapid-pvst **(options: mst, pvst, rapid-pvst)** • **Enabling portfast and BPDU guard on an interface:** SW1(config-if)#spanning-tree portfast SW1(config-if)#spanning-tree bpduguard enable • **Changing port cost:** SW1(config-if)#spanning-tree **[vlan 1]** cost 25 • **Bundling interfaces into an etherchannel:** SW1(config-if)#channel-group 1 mode on **(options: auto, desirable, on)**	Priority must be a multiply of 4096 Portfast and BPDU guard are enabled only on interfaces connected to end user hosts

Cisco Commands

STP verification and troubleshooting	
SW1#show spanning-tree	Shows detailed info about STP state
SW1#show spanning-tree interface fa0/2	Shows STP info only on a specific port
SW1#show spanning-tree vlan 1	Shows STP info only for a specific VLAN
SW1#show spanning-tree [vlan1] root	Shows info about the root switch
SW1#show spanning-tree [vlan1] bridge	Shows info about the local switch
SW1#show etherchannel 1	Show the state of the etherchannels
SW1#debug spanning-tree events	Provides informational messages about the changes in the STP topology
Enabling or disabling CDP	
• **Enabling CDP globally on a switch:** SW1(config)#cdp run • **Disabling CDP on a given interface:** SW1(config-if)#no cdp enable	
Using CDP for network verification and troubleshooting	
SW1#show cdp	Shows global information about CDP itself
SW1#show cdp interface fa0/2	Shows information about CDP on a specific interface
SW1#show cdp neighbors	Shows information about the directly connected cisco devices including interfaces names capabilities
SW1#show cdp neighbors detail	Shows detailed information about the neighboring cisco devices including device address and version of IOS they run
SW1#show cdp entry *	Same as show cdp neighbor detail
SW1#show cdp entry SW2	Shows detailed information about the specified entry only