

CCNP BCMSN Part 1

Cisco Switch Challenge 1

Outline

This challenge involves the configuration an IP address on a VLAN

Objectives

The objectives of this challenge are to:

- Setup the VLAN address.
- Define a domain-name.
- Define the default gateway.

Example

```
> en
# config t
(config)# int vlan 1
(config-if)# ip address ?
  A.B.C.D  IP address
(config-if)# ip address 148.183.229.5 ?
  A.B.C.D  IP subnet mask
(config-if)# ip address 148.183.229.5 255.255.248.0
(config-if)# exit
(config)# ip domain-name ?
  WORD    Default domain name

(config)# ip domain-name perthshire.cc
(config)# ip default-gateway ?
  A.B.C.D  IP address of default gateway
(config)# ip default-gateway 148.183.229.6
```

Cisco Switch Challenge 2

Outline

This challenge involves the configuration of the console password and to enable the HTTP server.

Objectives

The objectives of this challenge are to:

- Setup the console password.
- Enable the HTTP server.
- Define the HTTP port.
- Define the name server.

Example

```
> en
# config t
(config)#lin con ?
  <0-0> First Line number
(config)# line con 0
(config-line)# password ?
  0 Specifies an UNENCRYPTED password will follow
  7 Specifies a HIDDEN password will follow
  LINE The UNENCRYPTED (cleartext) line password
(config-line)# password texas
(config-line)# exit
(config)# ip http ?
  access-class Restrict access by access-class
  authentication Set http authentication method
  path Set base path for HTML
  port HTTP port
  server Enable HTTP server
(config)# ip http server
(config)# ip http port ?
  <0-65535> HTTP port
(config)# ip http port 1024
(config)# cdp ?
  advertise-v2 CDP sends version-2 advertisements
  holdtime Specify the holdtime (in sec) to be sent in packets
  timer Specify the rate at which CDP packets are sent (in sec)
  run
(config)# cdp run
(config)# ip name-server 14.154.109.7
```

Cisco Switch Challenge 3

Outline

This challenge involves the configuration of the VTY server and SNMP settings

Objectives

The objectives of this challenge are to:

- Setup a password on the Telnet session.
- Define a username and password.
- Define SNMP parameters.

Example

```
# config t
(config)#line vty ?
    <0-15> First Line number

(config)#line vty 0 ?
    <1-15> Last Line number
    <cr>
(config)# line vty 0 15
(config-line)# login
(config-line)# password manchester
(config-line)# exit
(config)# username june ?
    access-class          Restrict access by access-class
    autocommand           Automatically issue a command after the user logs in
    callback-dialstring   Callback dialstring
    callback-line         Associate a specific line with this callback
    callback-rotary       Associate a rotary group with this callback
    dnis                  Do not require password when obtained via DNIS
    nocallback-verify     Do not require authentication after callback
    noescape              Prevent the user from using an escape character
    nohangup              Do not disconnect after an automatic command
    nopassword            No password is required for the user to log in
    password              Specify the password for the user
    privilege             Set user privilege level
    secret                Specify the secret for the user
    user-maxlinks         Limit the user's number of inbound links
    <cr>

(config)# username june password ?
    0     Specifies an UNENCRYPTED password will follow
    7     Specifies a HIDDEN password will follow
    LINE  The UNENCRYPTED (cleartext) user password
(config)# username june password default1
(config)# snmp-server ?
    chassis-id           String to uniquely identify this chassis
    community            Enable SNMP; set community string and access privs
    contact              Text for mib object sysContact
    enable               Enable SNMP Traps or Informs
    engineID             Configure a local or remote SNMPv3 engineID
    group                Define a User Security Model group
    host                 Specify hosts to receive SNMP notifications
    ifindex              Enable ifindex persistence
    inform               Configure SNMP Inform options
    location             Text for mib object sysLocation
    manager              Modify SNMP manager parameters
    packetsize           Largest SNMP packet size
    queue-length         Message queue length for each TRAP host
    system-shutdown      Enable use of the SNMP reload command
    tftp-server-list     Limit TFTP servers used via SNMP
    trap                 SNMP trap options
    trap-source          Assign an interface for the source address of all traps
    trap-timeout         Set timeout for TRAP message retransmissions
    user                 Define a user who can access the SNMP engine
    view                 Define an SNMPv2 MIB view
(config)# snmp-server community ?
    WORD  SNMP community string
(config)# snmp-server community popup
(config)# snmp-server contact ?
    LINE  identification of the contact person for this managed node
```

```

(config)# snmp-server contact june
(config)# snmp-server location ?
    LINE The physical location of this node
(config)# snmp-server location glasgow
(config)# snmp-server enable ?
    informs Enable SNMP Informs
    traps Enable SNMP Traps
(config)#snmp-s enable traps ?
    bridge Enable SNMP STP Bridge MIB traps
    c2900 Enable SNMP c2900 traps
    cluster Enable Cluster traps
    config Enable SNMP config traps
    entity Enable SNMP entity traps
    envmon Enable SNMP environmental monitor traps
    flash Enable SNMP FLASH notifications
    hsrp Enable SNMP HSRP traps
    mac-notification Enable SNMP MAC Notification traps
    port-security Enable SNMP port security traps
    rtr Enable SNMP Response Time Reporter traps
    snmp Enable SNMP traps
    syslog Enable SNMP syslog traps
    vlan-membership Enable SNMP VLAN membership traps
    vlancreate Enable SNMP VLAN created traps
    vlandelete Enable SNMP VLAN deleted traps
    vtp Enable SNMP VTP traps
    <cr>
(config)# snmp-server enable traps
(config)# snmp-server chassis-id ?
    LINE Unique ID string
(config)# snmp-server chassis-id brighton

```

Cisco Switch Challenge 4

Outline

This challenge involves the configuration of a hosts table

Objectives

The objectives of this challenge are to:

- Define the default gateway.
- Enable an IP hosts table.

Example

```

# config t
Enter configuration commands, one per line. End with CNTL/Z.
(config)# ip default-gateway 142.163.250.7

(config)# ip host ?
    WORD Name of host
(config)# ip host brechin ?

```

```

<0-65535>   Default telnet port number
A.B.C.D     Host IP address
additional  Append addresses
(config)# ip host brechin 209.250.181.10

(config)# ip host mississippi 208.194.196.5

(config)# ip host westvirginia 205.27.128.4
(config)# exit
# show hosts

```

Cisco Switch Challenge 5

Outline

This challenge involves the configuration of ethernet port settings and CDP.

Objectives

The objectives of this challenge are to:

- Setup a description on FA0/1.
- Setup a speed on FA0/1.
- Setup duplex on FA0/1.
- Define CDP details.

Example

```

# config t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# int fa0/1
(config-if)# no shutdown
(config-if)# description ?
    LINE  Up to 240 characters describing this interface
(config-if)# description aironet 1200
(config-if)# speed ?
    10    Force 10 Mbps operation
    100   Force 100 Mbps operation
    auto  Enable AUTO speed configuration
(config-if)# speed 100
(config-if)# duplex ?
    auto  Enable AUTO duplex configuration
    full  Force full duplex operation
    half  Force half-duplex operation
(config-if)# duplex full
(config-if)# int fa0/2
(config-if)# no shutdown
(config-if)# exit
(config)# cdp run
(config)# int fa0/1
(config-if)# cdp ?
    enable Enable CDP on interface
(config-if)# cdp enable

```

```

(config-if)# exit
(config)# cdp ?
  advertise-v2  CDP sends version-2 advertisements
  holdtime     Specify the holdtime (in sec) to be sent in packets
  timer        Specify the rate at which CDP packets are sent (in sec)
  run
(config)# cdp timer ?
  <5-254> Rate at which CDP packets are sent (in sec)
  (config)# cdp timer 89
(config)# cdp hold ?
  <10-255> Length of time (in sec) that receiver must keep this packet
(config)# cdp holdtime 41

```

Cisco Switch Challenge 6

Outline

This challenge involves the configuration of VLANs.

Objectives

The objectives of this challenge are to:

- Setup VLAN 1, and define an IP address.
- Setup VLAN 2, and define an IP address.

Example

```

> en
# vlan database
(vlan)# vlan 1 name newjersey

      VLAN 1 added:

      Name: newjersey
(vlan)# ?
VLAN database editing buffer manipulation commands:
  abort  Exit mode without applying the changes
  apply  Apply current changes and bump revision number
  exit   Apply changes, bump revision number, and exit mode
  no     Negate a command or set its defaults
  reset  Abandon current changes and reread current database
  show   Show database information
  vlan   Add, delete, or modify values associated with a single VLAN
  vtp    Perform VTP administrative functions.
(vlan)# vlan 2 ?
  are           Maximum number of All Route Explorer hops for this VLAN
  backupcrf    Backup CRF mode of the VLAN
  bridge       Bridging characteristics of the VLAN
  media        Media type of the VLAN
  mtu          VLAN Maximum Transmission Unit
  name         Ascii name of the VLAN
  parent       ID number of the Parent VLAN of FDDI or Token Ring type VLANs
  ring         Ring number of FDDI or Token Ring type VLANs
  said         IEEE 802.10 SAID
  state        Operational state of the VLAN

```

```

ste      Maximum number of Spanning Tree Explorer hops for this VLAN
stp      Spanning tree characteristics of the VLAN
tb-vlan1 ID number of the first translational VLAN for this VLAN (or zero
         if none)
tb-vlan2 ID number of the second translational VLAN for this VLAN (or zero
         if none)
<cr>
(vlan)#vlan 2 name ?
WORD The ascii name for the VLAN
(vlan)# vlan 2 name brighton

      VLAN 2 added:

      Name: brighton
(vlan)# exit
APPLY completed.
Exiting....
# config t
(config)# int vlan 1
(config-if)# ip address 131.45.110.4 255.192.0.0
(config-if)# shutdown
(config-if)# exit
(config)# int vlan 2
(config-if)# ip address 81.200.53.4 255.255.0.0
(config-if)# exit

```

Note the **vlan database** command will be phased-out. An improved method is:

```

Switch(config)# vlan 1
Switch(config-vlan)# ?
VLAN configuration commands:
are      Maximum number of All Route Explorer hops for this VLAN (or
         zero if none specified)
backupcrf Backup CRF mode of the VLAN
bridge   Bridging characteristics of the VLAN
exit     Apply changes, bump revision number, and exit mode
media    Media type of the VLAN
mtu      VLAN Maximum Transmission Unit
name     Ascii name of the VLAN
no       Negate a command or set its defaults
parent   ID number of the Parent VLAN of FDDI or Token Ring type VLANs
private-vlan Configure a private VLAN
remote-span Configure as Remote SPAN VLAN
ring     Ring number of FDDI or Token Ring type VLANs
said     IEEE 802.10 SAID
shutdown Shutdown VLAN switching
state    Operational state of the VLAN
ste      Maximum number of Spanning Tree Explorer hops for this VLAN (or
         zero if none specified)
stp      Spanning tree characteristics of the VLAN
tb-vlan1 ID number of the first translational VLAN for this VLAN (or
         zero if none)
tb-vlan2 ID number of the second translational VLAN for this VLAN (or
         zero if none)
Switch(config-vlan)# name ?
WORD The ascii name for the VLAN
Switch(config-vlan)# name newjersey

```

Cisco Switch Challenge 7

Outline

This challenge involves the configuration of switchport access parameters.

Objectives

The objectives of this challenge are to:

- Setup VLAN 2.
- Define switchport access for VLAN 2.

Example

```
> en
# vlan database
(vlan)# vlan 2 name amsterdam

      VLAN 2 added:

      Name: amsterdam
(vlan)# exit
APPLY completed.
Exiting....
# config t
(config)# int vlan 2

(config-if)# ip address 161.161.238.9 255.255.255.248

(config-if)# exit
(config)# int fa0/2
(config-if)# switchport access ?
      vlan Set VLAN when interface is in access mode
(config-if)# switchport access vlan 2
(config-if)# int fa0/5
(config-if)# switchport access vlan 2
```

Note the **vlan database** command will be phased-out. An improved method is:

```
Switch(config)# vlan 2
Switch(config-vlan)# ?
VLAN configuration commands:
  are          Maximum number of All Route Explorer hops for this VLAN (or
              zero if none specified)
  backupcrf   Backup CRF mode of the VLAN
  bridge      Bridging characteristics of the VLAN
  exit        Apply changes, bump revision number, and exit mode
  media       Media type of the VLAN
  mtu         VLAN Maximum Transmission Unit
  name        Ascii name of the VLAN
  no          Negate a command or set its defaults
  parent      ID number of the Parent VLAN of FDDI or Token Ring type VLANs
  private-vlan Configure a private VLAN
  remote-span Configure as Remote SPAN VLAN
  ring        Ring number of FDDI or Token Ring type VLANs
```

said	IEEE 802.10 SAID
shutdown	Shutdown VLAN switching
state	Operational state of the VLAN
ste	Maximum number of Spanning Tree Explorer hops for this VLAN (or zero if none specified)
stp	Spanning tree characteristics of the VLAN
tb-vlan1	ID number of the first translational VLAN for this VLAN (or zero if none)
tb-vlan2	ID number of the second translational VLAN for this VLAN (or zero if none)
Switch(config-vlan)# name ?	
WORD	The ascii name for the VLAN
Switch(config-vlan)# name newjersey	

Cisco Switch Challenge 8

Outline

This challenge involves the configuration of timeouts for the console.

Objectives

The objectives of this challenge are to:

- Setup a password on the console.
- Define timeouts for the console.

Example

```
> en
# config t
(config)# line con 0
(config-line)# password lothian
(config-line)# timeout ?
    login Timeouts related to the login sequence
(config-line)# timeout login ?
    response Timeout for any user input during login sequences
(config-line)# timeout login response ?
    <0-300> Timeout in seconds
(config-line)# timeout login response 19
(config-line)# exec-timeout ?
    <0-35791> Timeout in minutes
(config-line)# exec-timeout 11
(config-line)# log ?
    synchronous Synchronized message output
(config-line)# log synchronous
(config-line)# line vty 0 8
(config-line)# login
(config-line)# password mississippi
(config-line)# timeout login response 12
(config-line)# exec-timeout 10
```

Cisco Switch Challenge 9

Outline

This challenge involves the configuration the clock, boot system and DHCP pool.

Objectives

The objectives of this challenge are to:

- Setup the clock.
- Define the boot system.
- Define the name of the DHCP pool.

Example

```
# clock ?
  set Set the time and date
# clock set 06:25
# config t
(config)# ip ?
Global IP configuration subcommands:
  access-list Named access-list
  accounting-list Select hosts for which IP accounting information is kept
  accounting-threshold Sets the maximum number of accounting entries
  accounting-transits Sets the maximum number of transit entries
  alias Alias an IP address to a TCP port
  default-gateway Specify default gateway (if not routing IP)
  dhcp-server Specify address of DHCP server to use
  domain-list Domain name to complete unqualified host names.
  domain-lookup Enable IP Domain Name System hostname translation
  domain-name Define the default domain name
  finger finger server
  ftp FTP configuration commands
  gdp Router discovery mechanism
  gratuitous-arps Generate gratuitous ARPs for PPP/SLIP peer addresses
  host Add an entry to the ip hostname table
  host-routing Enable host-based routing (proxy ARP and redirect)
  hp-host Enable the HP proxy probe service
  http HTTP server configuration
  icmp ICMP options
  igmp IGMP options
  local Specify local options
  name-server Specify address of name server to use
  radius RADIUS configuration commands
  rcmd Rcmd commands
  reflexive-list Reflexive access list
  security Specify system wide security information
  source-route Process packets with source routing header options
  sticky-arp Allow the creation of sticky ARP entries
  subnet-zero Allow 'subnet zero' subnets
  tacacs TACACS configuration commands
  tcp Global TCP parameters
```

```

telnet                Specify telnet options
tftp                  tftp configuration commands
(config)# ip subnet-zero
(config)# ip classless

(config)# boot system ?
WORD      TFTP filename or URL
flash    Boot from flash memory
mop      Boot from a Decnet MOP server
rcp      Boot from a server via rcp
tftp     Boot from a tftp server
(config)# boot system tftp c28.bin

(config)# ip dhcp ?
conflict      DHCP address conflict parameters
database      Configure DHCP database agents
excluded-address Prevent DHCP from assigning certain addresses
limited-broadcast-address Use all 1's broadcast address
ping          Specify ping parameters used by DHCP
pool          Configure DHCP address pools
relay         DHCP relay agent parameters
smart-relay   Enable Smart Relay feature

(config)# ip dhcp pool ?
WORD Pool name
(config)# ip dhcp pool paris
(dhcp-config)# ?
DHCP pool configuration commands:
bootfile      Boot file name
client-identifier Client identifier
client-name   Client name
default-router Default routers
dns-server    DNS servers
domain-name   Domain name
exit          Exit from DHCP pool configuration mode
hardware-address Client hardware address
host          Client IP address and mask
lease         Address lease time
netbios-name-server NetBIOS (WINS) name servers
netbios-node-type NetBIOS node type
network       Network number and mask
next-server   Next server in boot process
no            Negate a command or set its defaults
option        Raw DHCP options

```

Cisco Switch Challenge 10

Outline

This challenge involves the configuration of the Ethernet ports.

Objectives

The objectives of this challenge are to:

- Setup the first three Ethernet ports.

Example

```
# config t
(config)# int e0/1
(config-if)# description aironet 1200
(config-if)# shutdown
(config-if)# int e0/2
(config-if)# description production depart
(config-if)# shutdown
(config-if)# int e0/3
(config-if)# shutdown
```

Cisco Switch Challenge 11

Outline

This challenge involves the configuration of passwords, and usernames.

Objectives

The objectives of this challenge are to:

- Define the name server.
- Define the passwords.
- Setup usernames and passwords.

Example

```
> en
# config t
(config)# ip name-server 205.105.14.3
(config)# password dates
(config)# enable password default
(config)# enable secret dates
(config)# username katie password hotel
(config)# username william password eggplant
(config)# username anne ?
  access-class          Restrict access by access-class
  autocommand           Automatically issue a command after the user logs in
  callback-dialstring   Callback dialstring
  callback-line         Associate a specific line with this callback
  callback-rotary       Associate a rotary group with this callback
  dnis                  Do not require password when obtained via DNIS
  nocallback-verify     Do not require authentication after callback
  noescape              Prevent the user from using an escape character
  nohangup              Do not disconnect after an automatic command
  nopassword            No password is required for the user to log in
  password              Specify the password for the user
  privilege             Set user privilege this.level
  secret                Specify the secret for the user
  user-maxlinks         Limit the user's number of inbound links
```

```
(config)# username anne nopassword
```

Cisco Switch Challenge 12

Outline

This challenge involves the configuration of switchports

Objectives

The objectives of this challenge are to:

- Define the switchport mode.
- Enable trunking.
- Define spanning-tree costs.

Example

```
# config t
(config)# int fa0/1
(config-if)# switchport ?
  access          Set access mode characteristics of the interface
  block           Disable forwarding of unknown uni/multi cast addresses
  broadcast       Set broadcast suppression level on this interface
  encapsulation  Set trunking encapsulation when interface is in trunking mode
  host            Set port host
  mode            Set trunking mode of the interface
  multicast       Set multicast suppression level on this interface
  native         Set trunking native characteristics when interface is in
                 trunking mode
  nonegotiate    Device will not engage in negotiation protocol on this
                 interface
  port-security  Security related command
  priority        Set appliance 802.1p priority
  protected      Configure an interface to be a protected port
  pruning        Set pruning VLAN characteristics when interface is in trunking
                 mode
  trunk          Set trunking characteristics of the interface
  unicast        Set unicast suppression level on this interface
  voice          Voice appliance attributes
  <cr>
(config-if)# switchport mode ?
  access          Set trunking mode to ACCESS unconditionally
  dot1q-tunnel   Set trunking mode to DOT1Q TUNNEL unconditionally
  dynamic        Set trunking mode to dynamically negotiate access or trunk mode
  trunk          Set trunking mode to TRUNK unconditionally
(config-if)# switchport mode trunk
(config-if)# switchport trunk ?
  allowed        Set allowed VLAN characteristics when interface is in trunking
                 mode
  encapsulation  Set trunking encapsulation when interface is in trunking mode
  native         Set trunking native characteristics when interface is in
                 trunking mode
  pruning        Set pruning VLAN characteristics when interface is in trunking
```

```

mode
(config-if)# switchport trunk encapsulation ?
dot1q      Interface uses only 802.1q trunking encapsulation when trunking
isl        Interface uses only ISL trunking encapsulation when trunking
negotiate  Device will negotiate trunking encapsulation with peer on
           interface
(config-if)#switch trunk encapsulation ?
dot1q      Interface uses only 802.1q trunking encapsulation when trunking
isl        Interface uses only ISL trunking encapsulation when trunking
negotiate  Device will negotiate trunking encapsulation with peer on
           interface
(config-if)# switchport trunk encapsulation dot1q

(config-if)# spanning-tree ?
bpdufilter Don't send or receive BPDUs on this interface
bpduguard  Don't accept BPDUs on this interface
cost       Change an interface's spanning tree port path cost
guard      Change an interface's spanning tree guard mode
link-type  Specify a link type for spanning tree protocol use
port-priority Change an interface's spanning tree port priority
portfast   Enable an interface to move directly to forwarding on link up
stack-port Enable stack port
vlan       VLAN Switch Spanning Tree
(config-if)# spanning-tree cost ?
<1-200000000> port path cost
(config-if)# spanning-tree cost 3
(config-if)# int fa0/2
(config-if)# switchport mode trunk
(config-if)# switchport trunk encapsulation dot1q
(config-if)# spanning-tree cost 31
(config-if)# int fa0/3
(config-if)# switchport mode trunk
(config-if)# switchport trunk encapsulation dot1q
(config-if)# spanning-tree cost 33

```

Cisco Switch Challenge 13

Outline

This challenge involves the configuration the host table, hostname and default gateway.

Objectives

The objectives of this challenge are to:

- Define the default gateway.
- Define the hostname.
- Create a hosts table.

Example

```

> en
# config t
(config)# ip default-gateway 36.125.171.9

```

```
(config)# hostname montana
montana (config)# ip host tennessee 211.99.108.9
montana (config)# ip host kirkcaldy 154.242.2.8
montana (config)# ip host edinburgh 64.2.249.2
```

Cisco Switch Challenge 14

Outline

This challenge involves the configuration of logging.

Objectives

The objectives of this challenge are to:

- Enable logging.
- Define Syslog server.
- Define buffer size.
- Define logging level.

Example

```
> enable
# config t
(config)# lo ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  cns-events          Set CNS Event logging level
  console             Set console logging level
  exception           Limit size of exception flush output
  facility            Facility parameter for syslog messages
  file               Set logging file parameters
  history            Configure syslog history table
  monitor            Set terminal line (monitor) logging level
  on                 Enable logging to all supported destinations
  rate-limit         Set messages per second limit
  source-interface   Specify interface for source address in logging
                    transactions
  trap              Set syslog server logging level
(config)# logging on
(config)# logging 212.72.52.7
(config)# logging buffer ?
<0-7>                Logging severity level
<4096-2147483647>   Logging buffer size
alerts              Immediate action needed                (severity=1)
critical           Critical conditions                    (severity=2)
debugging         Debugging messages                      (severity=7)
emergencies       System is unusable                       (severity=0)
errors            Error conditions                        (severity=3)
informational     Informational messages                  (severity=6)
notifications     Normal but significant conditions      (severity=5)
warnings         Warning conditions                      (severity=4)
<cr>
```

```

(config)# logging buffer 440240
(config)# logging host 138.24.170.8
Switch(config)# logging trap ?
<0-7>          Logging severity level
alerts         Immediate action needed          (severity=1)
critical       Critical conditions                (severity=2)
debugging      Debugging messages                      (severity=7)
emergencies    System is unusable                       (severity=0)
errors         Error conditions                        (severity=3)
informational  Informational messages                  (severity=6)
notifications  Normal but significant conditions       (severity=5)
warnings      Warning conditions                     (severity=4)
<cr>
(config)# logging trap emergency
(config)# logging monitor emergency
(config)# logging console emergency
(config)# logging buffer emergency

```

Cisco Switch Challenge 15

Outline

This challenge involves the configuration of the HTTP server and in creating banners.

Objectives

The objectives of this challenge are to:

- Enable HTTP.
- Define the HTTP server port.
- Define authentication.
- Define the helper path.
- Define an access-class number.
- Create banners.

Example

```

> en
# config t
(config)# ip http server
(config)# ip http port ?
<0-65535> HTTP port
(config)# ip http port 1024
(config)# ip http ?
access-class  Restrict access by access-class
authentication Set http authentication method
help-path     HTTP help root URL
path          Set base path for HTML
port          HTTP port
server        Enable HTTP server
(config)# ip http authentication ?
enable       Use enable passwords
local        Use local username and passwords
tacacs       Use tacacs to authorize user

```

```

(config)# ip http authentication local
(config)# ip http help-path ?
      WORD  root URL for help pages
(config)# ip http help-path file:///c:\wireless\help
(config)# ip http access-class 10
(config)# banner motd gorgie home
(config)# banner login welcome
(config)# banner exec admin device

```

Cisco Switch Challenge 16

Outline

This challenge involves the configuration of the clock and boot settings.

Objectives

The objectives of this challenge are to:

- Define the clock setting.
- Define the boot method.

Example

```

# clock ?
  set  Set the time and date
# clock set 06:25
(config)# ip subnet-zero
(config)# ip classless
(config)# boot ?
  boothlpr          Boot Helper System Image
  buffersize        Specify the buffer size for filesystem-simulated NVRAM
  config-file       Configuration File
  enable-break      Enable Break while booting
  helper            Helper Image(s)
  helper-config-file Helper Configuration File
  manual            Manual Boot
  private-config-file Private Configuration File
  system            System Image
(config)# boot system ?
  WORD  TFTP filename or URL
  flash Boot from flash memory
  mop   Boot from a Decnet MOP server
  rcp   Boot from a server via rcp
  tftp  Boot from a tftp server
(config)# boot system tftp c28.bin

```

Cisco Switch Challenge 17

Outline

This challenge involves the configuration of the DHCP server.

Objectives

The objectives of this challenge are to:

- Setup a DHCP pool.
- Define the network addresses.
- Define the DNS-server.
- Define the NetBIOS server.
- Setup the lease time.
- Define the default-router.
- Define excluded addresses.
- Define ping time-out.

Example

```
> en
# config t
(config)#ip dhcp pool ?
    WORD Pool name
(config)# ip dhcp pool wyoming
(config-dhcp)# network 249.189.108.0 ?
    /nn or A.B.C.D Network mask or prefix length
    <cr>
(config-dhcp)# network 249.189.108.0 255.255.255.254
(config-dhcp)# dns-server ?
    Hostname or A.B.C.D Server's name or IP address
(config-dhcp)# dns-server 249.189.108.58
(config-dhcp)# netbios-name-server 249.189.108.61
(config-dhcp)# lease 3
(config-dhcp)# default-router 249.189.108.87
(config-dhcp)# exit
(config)# ip dhcp ?
    conflict                DHCP address conflict parameters
    database                Configure DHCP database agents
    excluded-address        Prevent DHCP from assigning certain addresses
    limited-broadcast-address Use all 1's broadcast address
    ping                    Specify ping parameters used by DHCP
    pool                    Configure DHCP address pools
    relay                   DHCP relay agent parameters
    smart-relay             Enable Smart Relay feature
(config)# ip dhcp e ?
    A.B.C.D Low IP address
(config)# ip dhcp excluded-address 249.189.108.26
(config)# ip dhcp ping ?
    WORD Pool name
    packets Specify number of ping packets
    timeout Specify ping timeout
(config)# ip dhcp ping timeout ?
    <100-10000> Ping timeout in milliseconds
(config)# ip dhcp ping timeout 350
```

Cisco Switch Challenge 18

Outline

This challenge involves the configuration of services on the device.

Objectives

The objectives of this challenge are to:

- Setup services.
- Define timestamp formats.
- Disable small TCP servers.
- Disable small UDP servers.

Example

```
> en
# config t
(config)# service ?
  compress-config      Compress the configuration file
  config               TFTP load config files
  dhcp                Enable DHCP server and relay agent
  disable-ip-fast-frag Disable IP particle-based fast fragmentation
  exec-callback        Enable exec callback
  exec-wait            Delay EXEC startup on noisy lines
  finger               Allow responses to finger requests
  hide-telnet-addresses Hide destination addresses in telnet command
  linenumber           enable line number banner for each exec
  nagle                Enable Nagle's congestion control algorithm
  old-slip-prompts     Allow old scripts to operate with slip/ppp
  pad                  Enable PAD commands
  password-encryption Encrypt system passwords
  prompt              Enable mode specific prompt
  pt-vty-logging       Log significant VTY-Async events
  sequence-numbers     Stamp logger messages with a sequence number
  slave-log            Enable log capability of slave IPs
  tcp-keepalives-in    Generate keepalives on idle incoming network
                      connections
  tcp-keepalives-out   Generate keepalives on idle outgoing network
                      connections
  tcp-small-servers    Enable small TCP servers (e.g., ECHO)
  telnet-zeroidle      Set TCP window 0 when connection is idle
  timestamps           Timestamp debug/log messages
  udp-small-servers    Enable small UDP servers (e.g., ECHO)
(config)# service timestamps ?
  debug   Timestamp debug messages
  log     Timestamp log messages
  <cr>
(config)# service timestamps log ?
  datetime  Timestamp with date and time
  uptime    Timestamp with system uptime
  <cr>
(config)# service timestamps log datetime
(config)# service ?
  compress-config      Compress the configuration file
  config               TFTP load config files
```

```

dhcp Enable DHCP server and relay agent
disable-ip-fast-frag Disable IP particle-based fast fragmentation
exec-callback Enable exec callback
exec-wait Delay EXEC startup on noisy lines
finger Allow responses to finger requests
hide-telnet-addresses Hide destination addresses in telnet command
linenumber enable line number banner for each exec
nagle Enable Nagle's congestion control algorithm
old-slip-prompts Allow old scripts to operate with slip/ppp
pad Enable PAD commands
password-encryption Encrypt system passwords
prompt Enable mode specific prompt
pt-vty-logging Log significant VTY-Async events
sequence-numbers Stamp logger messages with a sequence number
slave-log Enable log capability of slave IPs
tcp-keepalives-in Generate keepalives on idle incoming network
connections
tcp-keepalives-out Generate keepalives on idle outgoing network
connections
tcp-small-servers Enable small TCP servers (e.g., ECHO)
telnet-zeroidle Set TCP window 0 when connection is idle
timestamps Timestamp debug/log messages
udp-small-servers Enable small UDP servers (e.g., ECHO)
(config)# service sequence-numbers
(config)# service dhcp
(config)# service finger

(config)# no service tcp-small-servers
(config)# no service udp-small-servers
(config)# service password-encryption

```

Cisco Switch Challenge 19

Outline

This challenge involves the configuration of a range of ports.

Objectives

The objectives of this challenge are to:

- Setup a range of ports.

Example

```

> en
# vlan database

(vlan)# vlan 1 name indiana

VLAN 1 added:

Name: indiana
(vlan)# vlan 2 name california

VLAN 2 added:

```

```

    Name: california
(vlan)# vlan 10 name finland

    VLAN 10 added:

    Name: finland
(vlan)# exit
APPLY completed.
Exiting...
# config t
(config)# int ?
  Async          Async interface
  BVI            Bridge-Group Virtual Interface
  Dialer         Dialer interface
  FastEthernet   FastEthernet IEEE 802.3
  GigabitEthernet GigabitEthernet IEEE 802.3z
  Group-Async    Async Group interface
  Lex            Lex interface
  Loopback       Loopback interface
  Multilink      Multilink-group interface
  Null           Null interface
  Port-channel   Ethernet Channel of interfaces
  Transparent    Transparent interface
  Tunnel         Tunnel interface
  Virtual-Template Virtual Template interface
  Virtual-TokenRing Virtual TokenRing
  Vlan           Catalyst Vlans
  fcpa          Fiber Channel
  range         interface range command
(config)# int range fa0/3 - 4
(config-if-range)# switchport access ?
  vlan Set VLAN when interface is in access mode
(config-if-range)# switchport access vlan ?
  <1-1005> VLAN ID of the VLAN when this port is in access mode
  dynamic When in access mode, this interfaces VLAN is controlled by VMPS
(config-if-range)# switchport access vlan 2
(config-if-range)# exit

(config)# int range fa0/5 - 7
(config-if-range)# switchport access vlan 10
(config-if-range)# exit

(config)# int range fa0/3 - 4
(config-if-range)# shutdown

```

Cisco Switch Challenge 20

Outline

This challenge involves the setting of logging and HTTP settings.

Objectives

The objectives of this challenge are to:

- Define a username and password.
- Setup logging.
- Define the clock.
- Define HTTP settings.
- Restrict HTTP access to a **single host**.

Example

```

> enable
# config t
(config)# username ?
    WORD  User name

(config)# username bill ?
    access-class      Restrict access by access-class
    autocommand       Automatically issue a command after the user logs in
    callback-dialstring  Callback dialstring
    callback-line      Associate a specific line with this callback
    callback-rotary    Associate a rotary group with this callback
    dnis               Do not require password when obtained via DNIS
    nocallback-verify  Do not require authentication after callback
    noescape           Prevent the user from using an escape character
    nohangup           Do not disconnect after an automatic command
    nopassword         No password is required for the user to log in
    password           Specify the password for the user
    privilege          Set user privilege level
    secret             Specify the secret for the user
    user-maxlinks      Limit the user's number of inbound links
    <cr>

(config)# username bill password ?
    0      Specifies an UNENCRYPTED password will follow
    7      Specifies a HIDDEN password will follow
    LINE   The UNENCRYPTED (cleartext) user password
(config)# username bill password smith
(config)# logging ?
    Hostname or A.B.C.D  IP address of the logging host
    buffered              Set buffered logging parameters
    cns-events            Set CNS Event logging level
    console               Set console logging level
    exception             Limit size of exception flush output
    facility               Facility parameter for syslog messages
    file                  Set logging file parameters
    history               Configure syslog history table
    monitor               Set terminal line (monitor) logging level
    on                    Enable logging to all supported destinations
    rate-limit            Set messages per second limit
    source-interface      Specify interface for source address in logging
                        transactions
    trap                  Set syslog server logging level

(config)# logging on
(config)# logging 212.72.52.7
(config)# logging buffer ?
    <0-7>                 Logging severity level
    <4096-2147483647>    Logging buffer size
    alerts                Immediate action needed          (severity=1)
    critical               Critical conditions                (severity=2)
    debugging              Debugging messages                (severity=7)
    emergencies            System is unusable                    (severity=0)
    errors                 Error conditions                    (severity=3)

```

```

informational      Informational messages      (severity=6)
notifications     Normal but significant conditions (severity=5)
warnings          Warning conditions         (severity=4)
<cr>
(config)# logging buffer 440240
(config)# logging trap ?
<0-7>             Logging severity level
alerts            Immediate action needed     (severity=1)
critical          Critical conditions         (severity=2)
debugging         Debugging messages         (severity=7)
emergencies       System is unusable         (severity=0)
errors            Error conditions           (severity=3)
informational     Informational messages     (severity=6)
notifications     Normal but significant conditions (severity=5)
warnings          Warning conditions         (severity=4)
<cr>
(config)# logging trap emergency
(config)# logging monitor emergency
(config)# logging console emergency
(config)# logging buffer emergency

(config)# access-list 2 permit host 192.168.1.1
(config)# access-list 2 deny any

(config)# ip http ?
access-class      Restrict access by access-class
authentication    Set http authentication method
path              Set base path for HTML
port              HTTP port
server            Enable HTTP server
(config)# ip http server
(config)# ip http port 1024
(config)# ip http authentication ?
enable           Use enable passwords
local            Use local username and passwords
tacacs           Use tacacs to authorize user
(config)# ip http authentication local
(config)# exit
# sh running

```

Cisco Switch Test 1 (Challenge 21)

Unit 1: Switch Basics

The most up-to-date version of this test is at:

<http://networksims.com/sw01.html>

Cisco Switch Challenge 22

Area: Switches – VLANs

Outline

This challenge involves defining VLANs.

Objectives

The objectives of this challenge are to:

- Define and create VLANs.
- Assign ports of VLANs.

The commands used are:

```
> enable
# config t
(config)# int vlan1
(config-if)# ip address 1.2.3.4 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan2
(config-if)# ip address 1.2.3.5 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan3
(config-if)# ip address 1.2.3.6 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan10
(config-if)# ip address 1.2.3.7 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan11
(config-if)# ip address 1.2.3.8 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan12
(config-if)# ip address 1.2.3.9 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int fa0/1
(config-if)# switchport access vlan 1
(config-if)# exit
(config)# int fa0/2
(config-if)# switchport access vlan 2
(config-if)# exit
```

Alt:

```
# vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.
(vlan)# vlan 1 name fred
```

Example

```
> enable
# config t
(config)# int vlan1
```

```

(config-if)# ip address 1.2.3.4 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan2
(config-if)# ip address 1.2.3.5 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan3
(config-if)# ip address 1.2.3.6 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan10
(config-if)# ip address 1.2.3.7 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan11
(config-if)# ip address 1.2.3.8 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# int vlan12
(config-if)# ip address 1.2.3.9 255.255.255.0
(config-if)# no shutdown
(config-if)# exit

(config)# int fa0/1
(config-if)# switchport ?
  access      Set access mode characteristics of the interface
  block       Disable forwarding of unknown uni/multi cast addresses
  broadcast    Set broadcast suppression level on this interface
  encapsulation Set trunking encapsulation when interface is in trunking mode
  host        Set port host
  mode        Set trunking mode of the interface
  multicast    Set multicast suppression level on this interface
  native      Set trunking native characteristics when interface is in
              trunking mode
  nonegotiate Device will not engage in negotiation protocol on this
              interface
  port-security Security related command
  priority     Set appliance 802.1p priority
  protected   Configure an interface to be a protected port
  pruning     Set pruning VLAN characteristics when interface is in trunking
              mode
  trunk       Set trunking characteristics of the interface
  unicast     Set unicast suppression level on this interface
  voice       Voice appliance attributes
  <cr>
(config-if)# switchport access ?
  vlan Set VLAN when interface is in access mode

(config-if)# switchport access vlan ?
  <1-4094> VLAN ID of the VLAN when this port is in access mode
  dynamic When in access mode, this interfaces VLAN is controlled by VMPS

(config-if)# switchport access vlan 1
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport access vlan 2
(config-if)# exit

(config)# exit

# show vlan

```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24
2	VLAN0002	active	Fa0/1
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports

Alt:

vlan database

% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

(vlan)# vlan 1 name fred

Cisco Switch Challenge 23

Area: Switches – VLANs

Outline

This challenge involves defining VLANs.

Objectives

The objectives of this challenge are to:

- Define and create VLANs.
- Assign ports of VLANs.

- Define the name of a VLAN.

The commands used are:

```
> enable
# config t
(config)# int vlan1
(config-if)# ip address 1.2.3.4 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# vlan 1
(config-vlan)# mtu 1000
(config-vlan)# name fred
(config-vlan)# exit
(config)# exit
```

Alt (to create VLAN and define details):

```
# vlan database
(vlan)# vlan 1 mtu 1000
(vlan)# vlan 1 name fred
```

Example

```
> enable
# config t
(config)# int vlan1
(config-if)# ip address 1.2.3.4 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# vlan 1
(config-vlan)# ?
```

VLAN configuration commands:

are	Maximum number of All Route Explorer hops for this VLAN (or zero if none specified)
backupcrf	Backup CRF mode of the VLAN
bridge	Bridging characteristics of the VLAN
exit	Apply changes, bump revision number, and exit mode
media	Media type of the VLAN
mtu	VLAN Maximum Transmission Unit
name	Ascii name of the VLAN
no	Negate a command or set its defaults
parent	ID number of the Parent VLAN of FDDI or Token Ring type VLANs
private-vlan	Configure a private VLAN
remote-span	Configure as Remote SPAN VLAN
ring	Ring number of FDDI or Token Ring type VLANs
said	IEEE 802.10 SAID
shutdown	Shutdown VLAN switching
state	Operational state of the VLAN
ste	Maximum number of Spanning Tree Explorer hops for this VLAN (or zero if none specified)
stp	Spanning tree characteristics of the VLAN
tb-vlan1	ID number of the first translational VLAN for this VLAN (or zero if none)
tb-vlan2	ID number of the second translational VLAN for this VLAN (or zero if none)

```
(config-vlan)# mtu ?
<576-18190> Value of VLAN Maximum Transmission Unit
```

```

(config-vlan)# mtu 1000

(config-vlan)# name ?
WORD The ascii name for the VLAN
(config-vlan)# name fred
(config-vlan)# exit
(config)# exit

```

The alternative method, which is deprecated is:

```

# vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.
(vlan)# vlan ?
<1-1005> ISL VLAN index

(vlan)# vlan 1 ?
are Maximum number of All Route Explorer hops for this VLAN
backupcrf Backup CRF mode of the VLAN
bridge Bridging characteristics of the VLAN
media Media type of the VLAN
mtu VLAN Maximum Transmission Unit
name Ascii name of the VLAN
parent ID number of the Parent VLAN of FDDI or Token Ring type VLANs
ring Ring number of FDDI or Token Ring type VLANs
said IEEE 802.10 SAID
state Operational state of the VLAN
ste Maximum number of Spanning Tree Explorer hops for this VLAN
stp Spanning tree characteristics of the VLAN
tb-vlan1 ID number of the first translational VLAN for this VLAN (or zero
if none)
tb-vlan2 ID number of the second translational VLAN for this VLAN (or zero
if none)

(vlan)# vlan 1 mtu ?
<576-18190> Value of VLAN Maximum Tranmission Unit

(vlan)# vlan 1 mt 1000

(vlan)# vlan 1 name ?
WORD The ascii name for the VLAN

(vlan)# vl 1 name fred

```

Cisco Switch Challenge 24

Area: Switches – Extended VLANs

Outline

This challenge involves defining an extended VLANs (from 1006 to 4096). Extended VLANs are not saved to the VLAN database, Instead they are saved to the configuration file, and can thus be seen in the startup and running configuration (this makes them easier to copy onto other devices).

Objectives

The objectives of this challenge are to:

- Create an extended VLAN (from 1006 to 4096).
- Define extended VLAN details.

The commands used are:

```
> enable
# config t
(config)# vtp mode transparent
(config)# vlan 1006
(config-vlan)# name test
(config-vlan)# mtu 1500
(config-vlan)# end
```

Example

```
> enable
# config t
(config)# vtp ?
  domain      Set the name of the VTP administrative domain.
  file        Configure IFS filesystem file where VTP configuration is stored.
  interface   Configure interface as the preferred source for the VTP IP updater
              address.
  mode        Configure VTP device mode
  password    Set the password for the VTP administrative domain
  pruning     Set the administrative domain to permit pruning
  version     Set the administrative domain to VTP version
(config)# vtp mode ?
  client      Set the device to client mode.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.
(config)# vtp mode transparent
(config)# vlan 1006
(config-vlan)# name test
(config-vlan)# mtu 1500
(config-vlan)# end
# sh running
```

```
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
vtp mode transparent
!
!
```

```
vlan 1006
  name test
  mtu 1500
!
```

Note: If the transparent mode was not set, the following would appear:

```
(config)# vlan 1006
(config-vlan)# exit
% Failed to create VLANs 1006
VLAN(s) not available in Port Manager.
Failed to commit extended VLAN(s) changes.
```

And the VLAN would **not** be created.

Note: Standard VLANs are stored in the VLAN database and do not appear in the running config.

Cisco Switch Challenge 25

Outline

This challenge involves the configuration of VMPS.

Objectives

The objectives of this challenge are to:

- Setup VMPS.

Example

```
# config t
(config)# vmps ?
  reconfirm Set VMPS reconfirm interval
  retry     Set VMPS retry count
  server    Configure server IP address
(config)# vmps server ?
  Hostname or A.B.C.D IP address
(config)# vmps server 199.156.165.8 ?
  primary Specify primary server
  <cr>
(config)# vmps server 199.156.165.8 primary
(config)# vmps server 208.89.97.3
(config)# vmps server 206.81.143.1
(config)# vm reconfirm ?
  <0-120> Number of minutes between reconfirmations
(config)# vm retry ?
  <1-10> Retry count per server
(config)# vmps reconfirm 50
(config)# vmps retry 5
```

```

(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# switchport access ?
      vlan  Set VLAN when interface is in access mode
(config-if)# switchport access vlan ?
      <1-1005>  VLAN ID of the VLAN when this port is in access mode
      dynamic  When in access mode, this interfaces VLAN is controlled by VMPS
(config-if)# switchport access vlan dynamic
(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# switchport access vlan dynamic
(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# switchport access vlan dynamic
(config-if)# exit
(config)# exit
# show vmps

```

Cisco Switch Challenge 26

Area: Switches – VMPS

Outline

It is possible to configure VLANs using a VMPS server. The switch can be a VMPS client, which points to a VMPS server.

Objectives

The objectives of this challenge are to:

- Define VMPS servers.
- Define VMPS details.
- Define dynamic membership for a port to a VLAN, through the VMPS server.

The commands used are:

```

> enable
# config t
(config)# vmps server 1.2.3.4 primary
(config)# vmps server 1.2.3.5
(config)# vmps rec 10
(config)# vmps ret 8
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# switchport access vlan dynamic

```

Example

```

> enable
# config t
(config)# vmps ?

```

```

reconfirm Set VMPS reconfirm interval
retry Set VMPS retry count
server Configure server IP address

(config)# vmps server ?
    Hostname or A.B.C.D IP address

(config)# vmps server 1.2.3.4 ?
    primary Specify primary server
    <cr>

(config)# vmps server 1.2.3.4 primary
(config)# vmps server 1.2.3.5

(config)# vmps reconfirm ?
    <0-120> Number of minutes between reconfirmations

(config)# vmps reconfirm 10

(config)# vm retry ?
    <1-10> Retry count per server

(config)# vm retry 8

(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# switchport ?
    access Set access mode characteristics of the interface
    block Disable forwarding of unknown uni/multi cast addresses
    broadcast Set broadcast suppression level on this interface
    encapsulation Set trunking encapsulation when interface is in trunking mode
    host Set port host
    mode Set trunking mode of the interface
    multicast Set multicast suppression level on this interface
    native Set trunking native characteristics when interface is in
        trunking mode
    nonegotiate Device will not engage in negotiation protocol on this
        interface
    port-security Security related command
    priority Set appliance 802.1p priority
    protected Configure an interface to be a protected port
    pruning Set pruning VLAN characteristics when interface is in trunking
        mode
    trunk Set trunking characteristics of the interface
    unicast Set unicast suppression level on this interface
    voice Voice appliance attributes
    <cr>

(config-if)# switchport a ?
    vlan Set VLAN when interface is in access mode

(config-if)# switchport a v ?
    <1-4094> VLAN ID of the VLAN when this port is in access mode
    dynamic When in access mode, this interfaces VLAN is controlled by VMPS

(config-if)# switchport access vlan dynamic
    <cr>

# sh vmps
VQP Client Status:
-----
VMPS VQP Version: 1

```

```
Reconfirm Interval: 10 min
Server Retry Count: 8
VMPS domain server: 1.2.3.4
                   1.2.3.5 (primary, current)
```

```
Reconfirmation status
-----
```

```
VMPS Action:          No Dynamic Port
```

In this example the FA0/1 VLAN will be configured for its VLAN membership from the VMPS server.

Cisco Switch Challenge 27

Outline

This challenge involves the configuration of an access-map

Objectives

The objectives of this challenge are to:

- Define an access list to permit a range of addresses.
- Define an access-map.
- Apply the access-map.

```
# config t
(config)# vlan 1
(config-vlan)# name utah
(config-vlan)# exit
(config)# access-list 10 permit 20.123.92.0 0.0.0.1
(config)# vlan access-map utah
(config-access-map)# action forward
(config-access-map)# match ip access 10
(config-access-map)# exit
(config)# vlan filter utah vlan-list 1
```

Example

```
# config t
# config t
(config)# vlan 1
(config-vlan)# name utah
(config-vlan)# exit
(config)# access-list 10 permit ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address
(config)# access-list 10 permit 20.123.92.0 0.0.0.1
(config)# vlan access-map ?
  WORD  Vlan access map tag
(config)# vlan access-map utah
(config-access-map)# ?
  action  Take the action
```

```

default Set a command to its defaults
exit Exit from vlan access-map configuration mode
match Match values.
no Negate a command or set its defaults
(config-access-map)# action ?
drop Drop packets
forward Forward packets
(config-access-map)# action forward
(config-access-map)# match ?
ip IP based match
mac MAC based match

(config-access-map)# match ip ?
address Match IP address to access control.

(config-access-map)# match ip access ?
<1-199> IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
WORD Access-list name
<cr>
(config-access-map)# match ip access 10
(config-access-map)# exit
(config)# vlan ?
WORD ISL VLAN IDs 1-4094
access-map Create vlan access-map or enter vlan access-map command mode
dot1q dot1q parameters
filter Apply a VLAN Map
internal internal VLAN
(config)# vlan filter ?
WORD VLAN map name
(config)# vl filter utah ?
vlan-list VLANs to apply filter to
(config)#vl filter utah vlan-list ?
<1-4094> VLAN id
all Remove this filter from all VLANs
(config)# vlan filter utah vlan-list 1

```

Cisco Switch Challenge 28

Outline

This challenge involves the configuration VLAN filtering to drop TCP packets.

Objectives

The objectives of this challenge are to:

- Define an extended named ACL.
- Define the packets to be dropped by the VLAN.

Example

```

Switch(config)# ip access-list extended test
Switch(config-ext-nacl)# ?
Ext Access List configuration commands:

```

```

default    Set a command to its defaults
deny      Specify packets to reject
dynamic   Specify a DYNAMIC list of PERMITs or DENYs
evaluate  Evaluate an access list
exit      Exit from access-list configuration mode
no        Negate a command or set its defaults
permit    Specify packets to forward
remark    Access list entry comment
Switch(config-ext-nacl)# permit any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map London 10
Switch(config-access-map)# ?
Vlan access-map configuration commands:
  action    Take the action
  default   Set a command to its defaults
  exit      Exit from vlan access-map configuration mode
  match     Match values.
  no        Negate a command or set its defaults
Switch(config-access-map)# match ?
  ip       IP based match
  mac      MAC based match

Switch(config-access-map)# match ip ?
  address  Match IP address to access control.

Switch(config-access-map)# match ip address ?
  <1-199>   IP access list (standard or extended)
  <1300-2699> IP expanded access list (standard or extended)
  WORD      Access-list name
  <cr>

Switch(config-access-map)# match ip address test
Switch(config-access-map)# action ?
  drop      Drop packets
  forward   Forward packets

Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vl ?
  WORD      ISL VLAN IDs 1-4094
  access-map Create vlan access-map or enter vlan access-map command mode
  dot1q     dot1q parameters
  filter    Apply a VLANMap
  internal  internal VLAN
Switch(config)# vlan filter ?
  WORD      VLAN map name
Switch(config)# vl f test ?
  vlan-list VLANs to apply filter to
Switch(config)# vlan filter test vlan-list 10

```

Cisco Switch Challenge 29

Outline

This challenge involves the configuration VLAN filtering to forward TCP packets.

Objectives

The objectives of this challenge are to:

- Define an extended named ACL.
- Define the packets to be forwarded by the VLAN.

Example

```
Switch(config)# ip access-list extended test
```

```
Switch(config-ext-nacl)# ?
```

```
Ext Access List configuration commands:
```

```
default    Set a command to its defaults
deny       Specify packets to reject
dynamic    Specify a DYNAMIC list of PERMITs or DENYs
evaluate   Evaluate an access list
exit       Exit from access-list configuration mode
no         Negate a command or set its defaults
permit     Specify packets to forward
remark     Access list entry comment
```

```
Switch(config-ext-nacl)# permit any any
```

```
Switch(config-ext-nacl)# exit
```

```
Switch(config)# vlan access-map London 10
```

```
Switch(config-access-map)# ?
```

```
Vlan access-map configuration commands:
```

```
action     Take the action
default    Set a command to its defaults
exit       Exit from vlan access-map configuration mode
match      Match values.
no         Negate a command or set its defaults
```

```
Switch(config-access-map)# match ?
```

```
ip        IP based match
mac       MAC based match
```

```
Switch(config-access-map)# match ip ?
```

```
address   Match IP address to access control.
```

```
Switch(config-access-map)# match ip address ?
```

```
<1-199>   IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
WORD      Access-list name
<cr>
```

```
Switch(config-access-map)# match ip address test
```

```
Switch(config-access-map)# action ?
```

```
drop      Drop packets
forward   Forward packets
```

```
Switch(config-access-map)# action forward
```

```
Switch(config-access-map)# exit
```

```
Switch(config)# vl ?
```

```
WORD      ISL VLAN IDs 1-4094
access-map Create vlan access-map or enter vlan access-map command mode
dot1q     dot1q parameters
```

```

filter      Apply a VLAN Map
internal    internal VLAN
Switch(config)# vlan filter ?
WORD       VLAN map name
Switch(config)# vl f test ?
vlan-list  VLANs to apply filter to
Switch(config)# vlan filter test vlan-list 10

```

Cisco Switch Challenge 30

Outline

This challenge involves the configuration of VTP.

Objectives

The objectives of this challenge are to:

- Define VTP details.
- Enable VTP pruning.

Example

```

# config t
(config)# vtp ?
domain      Set the name of the VTP administrative domain.
file        Configure IFS filesystem file where VTP configuration is stored.
interface   Configure interface as the preferred source for the VTP IP updater
            address.
mode        Configure VTP device mode
password    Set the password for the VTP administrative domain
pruning     Set the administrative domain to permit pruning
version     Set the administrative domain to VTP version
(config)# vtp domain ?
WORD        The ascii name for the VTP administrative domain.
(config)# vtp domain ?
WORD        The ascii name for the VTP administrative domain.
(config)# vtp domain samoa
Changing VTP domain name from NULL to samoa
(config)# vtp password ?
WORD        The ascii password for the VTP administrative domain.
(config)# vtp password orange
Setting device VLAN database password to orange
(config)# vtp mode server
Setting device to VTP SERVER mode.
(config)# vtp pruning ?
<cr>
(config)# vtp pruning
Pruning switched ON
(config)# vtp version ?
<1-2>      Set the administrative domain VTP version number
(config)# vtp version 2

```

Otherwise the VLAN configuration mode can be used, such as:

```
# vlan database
(vlan)# vtp ?
  client      Set the device to client mode.
  domain      Set the name of the VTP administrative domain.
  password    Set the password for the VTP administrative domain.
  pruning     Set the administrative domain to permit pruning.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.
  v2-mode     Set the administrative domain to V2 mode.
(vlan)# vtp domain ?
  WORD The ascii name for the VTP administrative domain.
(vlan)# vtp domain samoa
Changing VTP domain name from NULL to samoa
(vlan)# vtp password ?
  WORD The ascii password for the VTP administrative
      domain.
(vlan)# vtp password orange
Setting device VLAN database password to orange
(vlan)# vtp server
Setting device to VTP SERVER mode.
(vlan)# vtp pruning
Pruning switched ON
```

Cisco Switch Challenge 31

Area: Switches – VTP Server

Outline

VTP (VLAN Trunking Protocol) maintains the consistency of VLANs across a domain. This includes the addition, deletion and renaming of VLANs across the complete network. One or more changes are automatically updated across the entire network, and thus minimizing configuration errors. There is no way to send VLAN information to other switches, unless VTP is enabled. Only standard-range VLANs are supported (1-1005). Also a trunk route must be enabled for advertisements to be sent.

Domain. If it is enabled the domain name is set, and the switch will listen to broadcasts for this domain name, otherwise it will ignore them.

Mode. If VTP is disabled the mode is set to **transparent**. Any changes in VLANs will not be transmitted to other switches. With a **server** mode, the switch will transmit all changes in VLANs where as the **client** mode acts the same but it is not possible to create, change or delete VLANs.

Objectives

The objectives of this challenge are to:

- Define VTP server mode.
- Define VTP details.
- Enable a trunk route.

The commands used are:

```
# config t
(config)# vtp mode server
(config)# vtp domain test
(config)# vtp password testing
(config)# vtp version 2
(config)# vtp pruning
```

```
# sh vtp status
```

Example

```
> enable
# config t
(config)# vtp ?
  domain      Set the name of the VTP administrative domain.
  file        Configure IFS filesystem file where VTP configuration is stored.
  interface   Configure interface as the preferred source for the VTP IP updater
              address.
  mode        Configure VTP device mode
  password    Set the password for the VTP administrative domain
  pruning     Set the administrative domain to permit pruning
  version     Set the administrative domain to VTP version

(config)# vt m ?
  client      Set the device to client mode.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.
(config)# vt m server

(config)# vtp domain ?
  WORD       The ascii name for the VTP administrative domain.

(config)# vtp domain test

(config)# vtp password ?
  WORD       The ascii password for the VTP administrative domain.

(config)# vtp password testing

(config)# vtp version 2
(config)# vtp pruning
(config)# exit

Switch#sh vtp ?
  counters   VTP statistics
  password   VTP password
  status     VTP domain status

# sh vtp status
VTP Version           : 2
Configuration Revision : 25
Maximum VLANs supported locally : 1005
Number of existing VLANs : 69
```

```
VTP Operating Mode          : Server
VTP Domain Name            : test
VTP Pruning Mode           : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x59 0xBA 0x92 0xA4 0x74 0xD5 0x42 0x29
Configuration last modified by 0.0.0.0 at 3-1-93 00:18:42
Local updater ID is 10.1.1.59 on interface V11 (lowest numbered VLAN interface found)
```

sh vtp counters

```
VTP statistics:
Summary advertisements received      : 20
Subset advertisements received       : 0
Request advertisements received      : 0
Summary advertisements transmitted  : 11
Subset advertisements transmitted    : 0
Request advertisements transmitted   : 0
Number of config revision errors     : 0
Number of config digest errors       : 0
Number of V1 summary errors          : 0
```

VTP pruning statistics:

Trunk	Join Transmitted	Join Received	Summary advts received from non-pruning-capable device
-----	-----	-----	-----

Note

With VTP, a trunk port must be defined so that advertisements can be sent.

The default details are:

```
VTP name = Null
VTP mode = Server
VTP version = 2
VTP password = None
VTP pruning = Disabled
```

Cisco Switch Challenge 32

Area: Switches – VTP Client

Outline

VTP (VLAN Trunking Protocol) maintains the consistency of VLANs across a domain. This includes the addition, deletion and renaming of VLANs across the complete network. One or more changes are automatically updated across the entire network, and thus minimizing configuration errors. There is no way to send VLAN information to other switches, unless VTP is enabled. Only standard-range VLANs are supported (1-1005). Also a trunk route must be enabled for advertisements to be sent.

Domain. If it is enabled the domain name is set, and the switch will listen to broadcasts for this domain name, otherwise it will ignore them.

Mode. If VTP is disabled the mode is set to **transparent**. Any changes in VLANs will not be transmitted to other switches. With a **server** mode, the switch will transmit all changes in VLANs where as the client mode acts the same but it is not possible to create, change or delete VLANs.

Objectives

The objectives of this challenge are to:

- Define VTP client mode.
- Define VTP details.
- Enable a trunk route.

The commands used are:

```
# config t
(config)# vtp mode client
(config)# vtp domain test
(config)# vtp password testing
(config)# vtp version 2
(config)# vtp pruning
```

```
# sh vtp status
```

Example

```
> enable
# config t
(config)# vtp ?
  domain      Set the name of the VTP administrative domain.
  file        Configure IFS filesystem file where VTP configuration is stored.
  interface   Configure interface as the preferred source for the VTP IP updater
              address.
  mode        Configure VTP device mode
  password    Set the password for the VTP administrative domain
  pruning     Set the administrative domain to permit pruning
  version     Set the administrative domain to VTP version

(config)# vt m ?
  client      Set the device to client mode.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.
(config)# vt m client

(config)# vtp domain ?
  WORD       The ascii name for the VTP administrative domain.

(config)# vtp domain test

(config)# vtp password ?
  WORD       The ascii password for the VTP administrative domain.
```

```
(config)# vtp password testing
```

```
(config)# vtp version 2
```

```
(config)# vtp pruning
```

```
(config)# exit
```

```
# sh vtp ?
```

```
counters  VTP statistics
password  VTP password
status    VTP domain status
```

```
# sh vtp status
```

```
VTP Version           : 2
Configuration Revision : 25
Maximum VLANs supported locally : 1005
Number of existing VLANs : 69
VTP Operating Mode    : Client
VTP Domain Name      : test
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MD5 digest           : 0x59 0xBA 0x92 0xA4 0x74 0xD5 0x42 0x29
Configuration last modified by 0.0.0.0 at 3-1-93 00:18:42
Local updater ID is 10.1.1.59 on interface V11 (lowest numbered VLAN interface found)
```

```
# sh vtp counters
```

```
VTP statistics:
Summary advertisements received : 20
Subset advertisements received  : 0
Request advertisements received  : 0
Summary advertisements transmitted : 11
Subset advertisements transmitted : 0
Request advertisements transmitted : 0
Number of config revision errors  : 0
Number of config digest errors    : 0
Number of V1 summary errors       : 0
```

```
VTP pruning statistics:
```

```
Trunk          Join Transmitted Join Received      Summary advts received from
-----          -----          -----          non-pruning-capable device
```

Note

With VTP, a trunk port must be defined so that advertisements can be sent.

The default details are:

VTP name = Null

VTP mode = Server

VTP version = 2

VTP password = None

VTP pruning = Disabled

Cisco Switch Challenge 33

Area: Switches – VTP Client – Extended Client

Outline

Mode. If VTP is disabled the mode is set to **transparent**. Any changes in VLANs will not be transmitted to other switches. With a **server** mode, the switch will transmit all changes in VLANs where as the **client** mode acts the same but it is not possible to create, change or delete VLANs.

Objectives

The objectives of this challenge are to:

- Define VTP transparent mode.

The commands used are:

```
# config t
(config)# vtp mode transparent

# sh vtp status
```

Example

```
> enable
# config t
(config)# vtp ?
  domain      Set the name of the VTP administrative domain.
  file        Configure IFS filesystem file where VTP configuration is stored.
  interface   Configure interface as the preferred source for the VTP IP updater
              address.
  mode        Configure VTP device mode
  password    Set the password for the VTP administrative domain
  pruning     Set the administrative domain to permit pruning
  version     Set the administrative domain to VTP version

(config)# vt m ?
  client      Set the device to client mode.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.
```

Cisco Switch Challenge 34

Area: Switches – IEEE 802.1Q/Layer 2 tunnelling

Outline

This challenge involves the configuring of 802.1Q tunnelling on a switch port.

Objectives

The objectives of this challenge are to:

- Define 802.1Q tunneling.
- Define tagging of the VLAN ID.

The commands used are:

```
> enable
# config t
(config)# int vlan 3
(config-vlan)# exit
(config)# int fa0/1
(config-if)# switchport access vlan 3
(config-if)# switchport mode dot1q-tunnel
(config-if)# exit
(config)# vlan dot1q tag native
```

Example

```
> enable
# config t
(config)# int vlan 3
(config-vlan)# exit
(config)# int fa0/1
(config-if)# switchport access ?
    vlan    Set VLAN when interface is in access mode

(config-if)# switchport access vlan ?
    <1-4094> VLAN ID of the VLAN when this port is in access mode
    dynamic  When in access mode, this interfaces VLAN is controlled by VMPS
(config-if)# switchport access vlan 3

(config-if)# switchport mode ?
    access          Set trunking mode to ACCESS unconditionally
    dot1q-tunnel    Set trunking mode to DOT1Q TUNNEL unconditionally
    dynamic         Set trunking mode to dynamically negotiate access or trunk mode
    trunk           Set trunking mode to TRUNK unconditionally

(config-if)# switchport mode dot1q-tunnel ?
    <cr>
(config-if)# switchport mode dot1q-tunnel
(config-if)# exit

(config)# vlan ?
    WORD           ISL VLAN IDs 1-4094
    access-map     Create vlan access-map or enter vlan access-map command mode
    dot1q          dot1q parameters
    filter         Apply a VLAN Map
    internal       internal VLAN
(config)# vlan dot1q ?
    tag    tag parameters

(config)# vlan dot1q tag ?
    native tag native vlan

(config)# vlan dot1q tag native ?
```

<cr>

```
(config)# vlan dot1q tag native
```

Cisco Switch Challenge 35

Area: Switches – IEEE 802.1Q/Layer 2 tunnelling

Outline

This challenge involves the configuring Layer 2 protocol tunneling.

Objectives

The objectives of this challenge are to:

- Define Layer 2 protocols to tunnel

The commands used are:

```
> enable
# config t
(config)# int fa0/1
(config-if)# l2protocol-tunnel cdp
(config-if)# l2protocol-tunnel stp
(config-if)# l2protocol-tunnel shutdown-threshold 100
(config-if)# exit
(config)# l2protocol-tunnel cos 5
```

Example

```
> enable
# config t
(config)# int fa0/1
(config-if)# l2protocol-tunnel ?
  cdp                Cisco Discovery Protocol
  drop-threshold     Set drop threshold for protocol packets
  point-to-point     point-to-point L2 Protocol
  shutdown-threshold Set shutdown threshold for protocol packets
  stp                Spanning Tree Protocol
  vtp                Vlan Trunking Protocol
<cr>
(config-if)# l2protocol-tunnel cdp
(config-if)# l2protocol-tunnel stp
(config-if)# l2protocol-tunnel shutdown-threshold ?
<1-4096>            Packets/sec rate beyond which interface is put to err-disable

  cdp                Cisco Discovery Protocol
  point-to-point     point-to-point L2 Protocol
  stp                Spanning Tree Protocol
  vtp                Vlan Trunking Protocol
(config-if)# l2protocol-tunnel shutdown-threshold 100
```

```
(config)# l2protocol-tunnel ?
cos Class of Service

(config)# l2protocol-tunnel cos ?
<0-7> priority value

(config)# l2protocol-tunnel cos 5
```

Cisco Switch Test 2 (Challenge 36)

Unit 2: VLAN and VTP

The most up-to-date version of this test is at:

<http://networksims.com/sw02.html>

Cisco Switch Challenge 37

Outline

This challenge involves the configuration of spanning-tree options.

Objectives

The objectives of this challenge are to:

- Setup VLANs.
- Define spanning-tree settings.

Example

```
> en
# vlan database
(vlan)# vlan 2 name amsterdam

      VLAN 2 added:

      Name: amsterdam
(vlan)# exit
APPLY completed.
Exiting...
# config t
(config)# int vlan 2

(config-if)# ip address 161.161.238.9 255.255.255.248

(config-if)# exit
```

```

(config)# spanning-tree ?
  backbonefast  Enable BackboneFast Feature
  etherchannel  Spanning tree etherchannel specific configuration
  extend        Spanning Tree 802.1t extensions
  loopguard     Spanning tree loopguard options
  mode          Spanning tree operating mode
  pathcost      Spanning tree pathcost options
  portfast      Spanning tree portfast options
  uplinkfast    Enable UplinkFast Feature
  vlan         VLAN Switch Spanning Tree
(config)# spanning-tree vlan ?
  WORD vlan range, example: 1,3-5,7,9-11
(config)# spanning-tree vlan 2
  forward-time  Set the forward delay for the spanning tree
  hello-time    Set the hello interval for the spanning tree
  max-age       Set the max age interval for the spanning tree
  priority      Set the bridge priority for the spanning tree
  root         Configure switch as root
<cr>
(config)# spanning-tree vlan 2 root ?
  primary      Configure this switch as primary root for this spanning tree
  secondary    Configure switch as secondary root

(config)# spanning-tree vlan 2 root primary
(config)# int fa0/1
(config-if)# spanning-tree cost 32
(config)# int fa0/2
(config-if)# spanning-tree cost 31
(config)# int fa0/3
(config-if)# spanning-tree cost 35

```

Cisco Switch Challenge 38

Outline

This challenge involves enabling port security and the BPDU guard (to defend against spanning-tree attacks).

Objectives

The objectives of this challenge are to:

- Enable BPDU guard.
- Enable port-security.
- Define a maximum number of MAC addresses on a port.
- Define a MAC address on a port.

Example

```

> en
# config t
Switch(config)# spanning-tree ?

```

```

backbonefast  Enable BackboneFast Feature
etherchannel  Spanning tree etherchannel specific configuration
extend        Spanning Tree 802.1t extensions
loopguard     Spanning tree loopguard options
mode          Spanning tree operating mode
mst           Multiple spanning tree configuration
pathcost      Spanning tree pathcost options
portfast      Spanning tree portfast options
uplinkfast    Enable UplinkFast Feature
vlan          VLAN Switch Spanning Tree

```

Switch(config)# spanning-tree portfast ?

```

bpdufilter  Enable portfast bpdu filter on this switch
bpduguard   Enable portfast bpdu guard on this switch
default     Enable portfast by default on all access ports

```

Switch(config)# spanning-tree portfast bpduguard ?

```

default  Enable bpdu guard by default on all portfast ports

```

Switch(config)# spanning-tree portfast bpduguard def ?

```

<cr>

```

Switch(config)# spanning-tree portfast bpduguard def

Switch(config)# int fa0/1

Switch(config-if)# sw po ?

```

aging          Port-security aging commands
mac-address    Secure mac address
maximum        Max secure addr
violation      Security Violation Mode

```

```

<cr>

```

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security max ?

```

<1-5120> Maximum addresses

```

Switch(config-if)# switchport port-security maximum 5

Switch(config-if)# switchport port-security mac-address ?

```

H.H.H  48 bit mac address

```

```

sticky  Configure dynamic secure addresses as sticky

```

Switch(config-if)# switchport port-security mac-address 0000.1111.2222

Cisco Switch Challenge 39

Outline

This challenge involves the setting up UDLD (Unidirectional Link Detection) which monitors the condition of a link, and identifies if it detects a unidirectional link, on which it can shut down the link, and display a message.

Objectives

The objectives of this challenge are to:

- Enable UDLD.
- Apply it on an interface.

Example

```
> enable
# config t
(config)# udld ?
    aggressive  Enable UDLD protocol in aggressive mode on fiber ports except
                  where locally configured
    enable      Enable UDLD protocol on fiber ports except where locally
                  configured
    message     Set UDLD message parameters
(config)# udld enable
(config)# int fa0/1
(config-if)# udld ?
    port       Enable UDLD protocol on this interface

(config-if)# udld port ?
    aggressive Enable UDLD protocol in aggressive mode on this interface
    <cr>
(config-if)# udld port
(config-if)# exit
(config)# exit
# sh udld

Interface Fa0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 7
Time out interval: 5
No neighbor cache information stored

Interface Fa0/2
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/3
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/4
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/5
---
```

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/6

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/7

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/8

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/9

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/10

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/11

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/12

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/13

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/14

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/15

Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

```
Interface Fa0/16
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/17
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/18
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/19
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/20
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/21
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/22
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Fa0/23
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown
```

Cisco Switch Challenge 40

Outline

This challenge involves the setting up UDLD (Unidirectional Link Detection) which monitors the condition of a link, and identifies if it detects a unidirectional link, on which it can shut down the link, and display a message.

Objectives

The objectives of this challenge are to:

- Enable UDLD.
- Apply it on an interface.

Example

```
> enable
# config t
(config)# rm ?
    alarm  Configure an rmon alarm
    event  Configure an RMON event

(config)# rm a ?
    <1-65535>  alarm number

(config)# rmon a 10 ?
    WORD  MIB object to monitor

(config)# rmon a 10 ifEntry.20.1 ?
    <1-2147483647>  Sample interval

(config)# rmon a 10 ifEntry.20.1 20 ?
    absolute  Test each sample directly
    delta     Test delta between samples

(config)# rmon a 10 ifEntry.20.1 20 de ?
    rising-threshold  Configure the rising threshold

(config)# rmon a 10 ifEntry.20.1 20 de ris ?
    <-2147483648 - 2147483647>  rising threshold value

(config)# rmon a 10 ifEntry.20.1 20 de ris ANY ?
    <1-65535>  Event to fire on rising threshold crossing
    falling-threshold  Configure the falling threshold

(config)# rmon a 10 ifEntry.20.1 20 de ris ANY fal ?
    <-2147483648 - 2147483647>  falling threshold value

(config)# rmon a 10 ifEntry.20.1 20 de ris ANY fal 0 ?
    <1-65535>  Event to fire on falling threshold crossing
    owner    Specify an owner for the alarm
    <cr>

(config)# rmon a 10 ifEntry.20.1 20 de ris ANY fal ANY own ?
    WORD  Alarm owner

(config)# rmon a 10 ifEntry.20.1 20 de ris ANY fal ANY own ANY ?
    <cr>
(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-
threshold 0 owner jjohnson
```

Cisco Switch Challenge 41

Area: Switches – STP (Spanning Tree Protocol)

Outline

This challenge involves disabling spanning-tree on a VLAN.

Objectives

The objectives of this challenge are to:

- Disable spanning-tree on a specific VLAN.

The commands used are:

```
> enable
# config t
(config)# no spanning-tree vlan 1
```

Example

```
> enable
# config t

(config)# no spanning-tree ?
  backbonefast  Enable BackboneFast Feature
  etherchannel  Spanning tree etherchannel specific configuration
  extend        Spanning Tree 802.1t extensions
  loopguard     Spanning tree loopguard options
  mode          Spanning tree operating mode
  mst           Multiple spanning tree configuration
  pathcost      Spanning tree pathcost options
  portfast      Spanning tree portfast options
  uplinkfast    Enable UplinkFast Feature
  vlan          VLAN Switch Spanning Tree

(config)# no spanning-tree vlan ?
  WORD vlan range, example: 1,3-5,7,9-11

(config)# no spanning-tree vlan 1 ?
  forward-time  Set the forward delay for the spanning tree
  hello-time    Set the hello interval for the spanning tree
  max-age       Set the max age interval for the spanning tree
  priority      Set the bridge priority for the spanning tree
  root          Configure switch as root
  <cr>

(config)# no spanning-tree vlan 1
```

Cisco Switch Challenge 42

Area: Switches – STP (Spanning Tree Protocol)

Outline

This challenge involves defining a primary root switch.

Objectives

The objectives of this challenge are to:

- Define a primary root switch.

The commands used are:

```
> enable
# config t
(config)# spanning-tree vlan 1 root primary
```

Example

```
> enable
# config t

(config)# spanning-tree ?
  backbonefast  Enable BackboneFast Feature
  etherchannel  Spanning tree etherchannel specific configuration
  extend        Spanning Tree 802.1t extensions
  loopguard     Spanning tree loopguard options
  mode          Spanning tree operating mode
  mst           Multiple spanning tree configuration
  pathcost      Spanning tree pathcost options
  portfast      Spanning tree portfast options
  uplinkfast    Enable UplinkFast Feature
  vlan         VLAN Switch Spanning Tree
(config)# spanning-tree vlan ?
  WORD vlan range, example: 1,3-5,7,9-11
(config)# spanning-tree vlan 1 root ?
  primary       Configure this switch as primary root for this spanning tree
  secondary     Configure switch as secondary root

(config)# spanning-tree vlan 1 root p ?
  diameter     Network diameter of this spanning tree
  <cr>
(config)# spanning-tree v 1 r p ?
(config)# spanning-tree vlan 1 root primary
```

Cisco Switch Challenge 43

Area: Switches – STP (Spanning Tree Protocol)

Outline

This challenge involves defining a secondary root switch which will take over from the primary root switch if it fails.

Objectives

The objectives of this challenge are to:

- Define a secondary root switch.

The commands used are:

```
> enable
# config t
(config)# spanning-tree vlan 1 root secondary
```

Example

```
> enable
# config t

(config)# spanning-tree ?
  backbonefast  Enable BackboneFast Feature
  etherchannel  Spanning tree etherchannel specific configuration
  extend        Spanning Tree 802.1t extensions
  loopguard     Spanning tree loopguard options
  mode          Spanning tree operating mode
  mst           Multiple spanning tree configuration
  pathcost      Spanning tree pathcost options
  portfast      Spanning tree portfast options
  uplinkfast    Enable UplinkFast Feature
  vlan          VLAN Switch Spanning Tree
(config)# spanning-tree vlan ?
  WORD vlan range, example: 1,3-5,7,9-11
(config)# spanning-tree vlan 1 root ?
  primary       Configure this switch as primary root for this spanning tree
  secondary     Configure switch as secondary root

(config)# spanning-tree vlan 1 root secondary ?
  diameter      Network diameter of this spanning tree
  <cr>
(config)# spanning-tree vlan 1 root secondary
```

Cisco Switch Challenge 44

Area: Switches – STP (Spanning Tree Protocol)

Outline

This challenge involves defining port-priority and path cost for spanning-tree.

Objectives

The objectives of this challenge are to:

- Define port-priority for spanning-tree.
- Define path cost for spanning-tree.

The commands used are:

```
> enable
# config t
(config-if)# spanning-tree cost 100
(config-if)# spanning-tree vlan 1 cost 100
(config-if)# spanning-tree vlan 1 port-priority 100
(config-if)# spanning-tree port-priority 100
```

Example

```
> enable
# config t

(config)# int fa0/1
Switch(config-if)# spanning-tree ?
  bpdufilter      Don't send or receive BPDUs on this interface
  bpduguard       Don't accept BPDUs on this interface
  cost            Change an interface's spanning tree port path cost
  guard          Change an interface's spanning tree guard mode
  link-type       Specify a link type for spanning tree protocol use
  mst            Multiple spanning tree
  port-priority   Change an interface's spanning tree port priority
  portfast       Enable an interface to move directly to forwarding on link up
  stack-port     Enable stack port
  vlan           VLAN Switch Spanning Tree
(config-if)# spanning-tree cost ?
<1-200000000> port path cost
(config-if)# spanning-tree cost 100

(config-if)# spanning-tree v 1 ?
  cost           Change an interface's per VLAN spanning tree path cost
  port-priority  Change an interface's spanning tree port priority

(config-if)# spanning-tree vlan 1 cost ?
<1-200000000> Change an interface's per VLAN spanning tree path cost
(config-if)# spanning-tree vlan 1 cost 100

(config-if)# spanning-tree port- ?
<0-240> port priority in increments of 16
(config-if)# spanning-tree port-priority 100

(config-if)# spanning-tree vlan 1 p ?
<0-240> port priority in increments of 16
(config-if)# spanning-tree vlan 1 port-priority 100
```

Cisco Switch Challenge 45

Area: Switches – STP (Spanning Tree Protocol)

Outline

This challenge involves defining port-priority and path cost for spanning-tree, and hello-time and forward-time.

Objectives

The objectives of this challenge are to:

- Define port-priority for spanning-tree.
- Define path cost for spanning-tree.
- Define spanning-tree hello-time.
- Define spanning-tree forward-time.

The commands used are:

```
> enable
# config t
(config)# spanning-tree vlan 1 forward-time 10
(config)# spanning-tree vlan 1 hello-time 10
(config)# spanning-tree vlan 1 max-age 10

(config)# int fa0/1
(config-if)# spanning-tree cost 100
(config-if)# spanning-tree vlan 1 cost 100
(config-if)# spanning-tree vlan 1 port-priority 100
(config-if)# spanning-tree port-priority 100
```

Example

```
> enable
# config t

(config)# spanning-tree vlan ?
WORD vlan range, example: 1,3-5,7,9-11

(config)# spanning-tree vlan ANY ?
forward-time Set the forward delay for the spanning tree
hello-time Set the hello interval for the spanning tree
max-age Set the max age interval for the spanning tree
priority Set the bridge priority for the spanning tree
root Configure switch as root
<cr>

(config)# spanning-tree vlan 1 forward-time ?
<4-30> number of seconds for the forward delay timer
(config)# spanning-tree vlan 1 forward-time 10

(config)# spanning-tree vlan 1 hello-time ?
<1-10> number of seconds between generation of config BPDUs
(config)# spanning-tree vlan 1 hello-time 10

(config)# spanning-tree vlan 1 m ?
<6-40> maximum number of seconds the information in a BPDU is valid
```

```

(config)# spanning-tree vlan 1 max-age 10

(config)# int fa0/1
Switch(config-if)# spanning-tree ?
  bpdufilter      Don't send or receive BPDUs on this interface
  bpduguard       Don't accept BPDUs on this interface
  cost            Change an interface's spanning tree port path cost
  guard          Change an interface's spanning tree guard mode
  link-type       Specify a link type for spanning tree protocol use
  mst            Multiple spanning tree
  port-priority   Change an interface's spanning tree port priority
  portfast        Enable an interface to move directly to forwarding on link up
  stack-port      Enable stack port
  vlan           VLAN Switch Spanning Tree
(config-if)# spanning-tree cost ?
<1-200000000> port path cost
(config-if)# spanning-tree cost 100

(config-if)# spanning-tree v 1 ?
  cost           Change an interface's per VLAN spanning tree path cost
  port-priority  Change an interface's spanning tree port priority

(config-if)# spanning-tree vlan 1 cost ?
<1-200000000> Change an interface's per VLAN spanning tree path cost
(config-if)# spanning-tree vlan 1 cost 100

(config-if)# spanning-tree port- ?
<0-240> port priority in increments of 16
(config-if)# spanning-tree port-priority 100

(config-if)# spanning-tree vlan 1 p ?
<0-240> port priority in increments of 16
(config-if)# spanning-tree vlan 1 port-priority 100

```

Cisco Switch Challenge 46 (MSTP/RSTP)

Area: Switches - RSTP and MSTP

Outline

This challenge involves configuring MSTP and RSTP. RSTP (Rapid Spanning Tree Protocol – IEEE 802.1W) and MSTP (Multiple STP – IEEE 802.1S) are used to provide rapid convergence of the spanning-tree protocol. **RSTP** is the part that allows for rapid convergence and **MSTP** is used to group VLANs into a single spanning-tree instance. RSTP can converge the spanning-tree instance in less than a second, as apposed to almost 50 seconds for standard 802.1D spanning tree). This type of setup is important in real-time applications such as voice and video traffic.

Objectives

The objectives of this challenge are to:

- Define MST details.

- Enable MSTP and RSTP for rapid convergence of the spanning-tree.

The commands used are:

```
> enable
# config t
(config)# spanning-tree mst configuration
(config-mst)# instance 1 v 1
(config-mst)# name fred
(config-mst)# revision 1
(config-mst)# exit
(config)# spanning-tree mode mst
```

Example

```
> enable
# config t

(config)# spanning-tree ?
  backbonefast  Enable BackboneFast Feature
  etherchannel  Spanning tree etherchannel specific configuration
  extend        Spanning Tree 802.1t extensions
  loopguard     Spanning tree loopguard options
  mode          Spanning tree operating mode
  mst           Multiple spanning tree configuration
  pathcost      Spanning tree pathcost options
  portfast      Spanning tree portfast options
  uplinkfast    Enable UplinkFast Feature
  vlan         VLAN Switch Spanning Tree
(config)# spanning-tree mst ?
  WORD          MST instance range, example: 0-3,5,7-9
  configuration  Enter MST configuration submode
  forward-time  Set the forward delay for the spanning tree
  hello-time    Set the hello interval for the spanning tree
  max-age       Set the max age interval for the spanning tree
  max-hops      Set the max hops value for the spanning tree

(config)# spanning-tree mst configuration ?
  <cr>
(config)# spanning-tree mst configuration

(config-mst)# ?
  abort        Exit region configuration mode, aborting changes
  exit         Exit region configuration mode, applying changes
  instance     Map vlans to an MST instance
  name         Set configuration name
  no           Negate a command or set its defaults
  private-vlan Set private-vlan synchronization
  revision     Set configuration revision number
  show        Display region configurations

(config-mst)# instance ?
  <0-15> MST instance id

(config-mst)# instance 1 ?
  vlan Range of vlans to add to the instance mapping

(config-mst)# instance 1 vlan ?
  LINE vlan range ex: 1-65, 72, 300 -200
(config-mst)# instance 1 vlan 1
```

```
(config-mst)# name ?  
WORD Configuration name  
(config-mst)# name fred  
  
(config-mst)# revision ?  
<0-65535> Configuration revision number  
(config-mst)# revision 1  
  
(config-mst)# exit  
  
(config)# spanning-tree mode ?  
mst Multiple spanning tree mode  
pvst Per-Vlan spanning tree mode  
rapid-pvst Per-Vlan rapid spanning tree mode  
(config)# spanning-tree mode mst
```

Notes

The command:

```
(config)# spanning-tree mode mst
```

enables both MSTP and RSTP. All the switches in the MST region require the same configuration for their MST settings.

The default parameters for RSTP and MSTP are:

Spanning-tree mode: PVST (MSTP and RSTP disabled)
Switch priority 32768
Spanning tree priority: 128
Spanning-tree cost: 4 (1Gbps), 19 (100Mbps), 100 (10Mbps)
Hello time: 2 seconds
Forward-delay time: 15 seconds
Maximum-aging time: 20 seconds
Maximum hop count: 20 hops

Cisco Switch Challenge 47 (Primary root switch)

Area: Switches - RSTP and MSTP

Outline

This challenge involves configuring a primary root switch for a given instance.

Objectives

The objectives of this challenge are to:

- Define a primary root.
- Define MST parameters on the interface, such as cost and port-priority.
- Define global MST parameters, such as hello time, forward-time, maximum age, maximum hops and priority.

The commands used are:

```
> enable
# config t
(config)# spanning-tree mst 1 root primary
(config)# spanning-tree mst hello-time 10
(config)# spanning-tree mst forward-time 10
(config)# spanning-tree mst 1 priority 10
(config)# spanning-tree mst max-age 10
(config)# spanning-tree mst max-hops 10
(config)# int fa0/1
(config-if)# spanning-tree mst 1 cost 10
(config-if)# spanning-tree mst 1 port-priority 10
```

Example

```
> enable
# config t
(config)# spanning-tree mst ?
WORD MST instance range, example: 0-3,5,7-9
configuration Enter MST configuration submode
forward-time Set the forward delay for the spanning tree
hello-time Set the hello interval for the spanning tree
max-age Set the max age interval for the spanning tree
max-hops Set the max hops value for the spanning tree
(config)# spanning-tree mst 1 ?
priority Set the bridge priority for the spanning tree
root Configure switch as root
(config)# spanning-tree mst 1 root ?
primary Configure this switch as primary root for this spanning tree
secondary Configure switch as secondary root
(config)# spanning-tree mst 1 root primary
(config)# spanning-tree mst hello-time ?
<1-10> number of seconds between generation of config BPDUs
(config)# spanning-tree mst hello-time 10
(config)# spanning-tree mst forward-time ?
<4-30> number of seconds for the forward delay timer
(config)# spanning-tree mst forward-time 10
(config)# spanning-tree mst 1 ?
priority Set the bridge priority for the spanning tree
root Configure switch as root
(config)# spanning-tree mst 1 priority ?
<0-61440> bridge priority in increments of 4096
(config)# spanning-tree mst 1 priority 10
(config)# spanning-tree mst max-age ?
<6-40> maximum number of seconds the information in a BPDU is valid

(config)# spanning-tree mst max-hops ?
<1-40> maximum number of hops a BPDU is valid
(config)# spanning-tree mst max-age 10
```

```

(config)# spanning-tree mst max-hops 10

(config)# int fa0/1
(config-if)# spanning-tree mst ?
WORD MST instance list, example 0,2-4,6,8-12
(config-if)# spanning-tree mst 1 ?
cost Change the interface spanning tree path cost for an instance
port-priority Change the spanning tree port priority for an instance
(config-if)# spanning-tree mst 1 cost ?
<1-200000000> Change the interface spanning tree path cost for an instance
(config-if)# spanning-tree mst 1 port-priority ?
<0-240> port priority in increments of 16
(config-if)# spanning-tree mst 1 cost 10
(config-if)# spanning-tree mst 1 port-priority 10

```

Cisco Switch Challenge 48 (Secondary root switch)

Area: Switches - RSTP and MSTP

Outline

This challenge involves configuring a secondary root switch for a given instance.

Objectives

The objectives of this challenge are to:

- Define a secondary root.
- Define MST parameters on the interface, such as cost and port-priority.
- Define global MST parameters, such as hello time, forward-time, maximum age, maximum hops and priority.

The commands used are:

```

> enable
# config t
(config)# spanning-tree mst 1 root secondary
(config)# spanning-tree mst hello-time 10
(config)# spanning-tree mst forward-time 10
(config)# spanning-tree mst 1 priority 10
(config)# spanning-tree mst max-age 10
(config)# spanning-tree mst max-hops 10
(config)# int fa0/1
(config-if)# spanning-tree mst 1 cost 10
(config-if)# spanning-tree mst 1 port-priority 10

```

Example

```
> enable
```

```

# config t
(config)# spanning-tree mst ?
WORD MST instance range, example: 0-3,5,7-9
configuration Enter MST configuration submode
forward-time Set the forward delay for the spanning tree
hello-time Set the hello interval for the spanning tree
max-age Set the max age interval for the spanning tree
max-hops Set the max hops value for the spanning tree
(config)# spanning-tree mst 1 ?
priority Set the bridge priority for the spanning tree
root Configure switch as root
(config)# spanning-tree mst 1 root ?
primary Configure this switch as primary root for this spanning tree
secondary Configure switch as secondary root
(config)# spanning-tree mst 1 root secondary
(config)# spanning-tree mst hello-time ?
<1-10> number of seconds between generation of config BPDUs
(config)# spanning-tree mst hello-time 10
(config)# spanning-tree mst forward-time ?
<4-30> number of seconds for the forward delay timer
(config)# spanning-tree mst forward-time 10
(config)# spanning-tree mst 1 ?
priority Set the bridge priority for the spanning tree
root Configure switch as root
(config)# spanning-tree mst 1 priority ?
<0-61440> bridge priority in increments of 4096
(config)# spanning-tree mst 1 priority 10
(config)# spanning-tree mst max-age ?
<6-40> maximum number of seconds the information in a BPDU is valid

(config)# spanning-tree mst max-hops ?
<1-40> maximum number of hops a BPDU is valid
(config)# spanning-tree mst max-age 10
(config)# spanning-tree mst max-hops 10

(config)# int fa0/1
(config-if)# spanning-tree mst ?
WORD MST instance list, example 0,2-4,6,8-12
(config-if)# spanning-tree mst 1 ?
cost Change the interface spanning tree path cost for an instance
port-priority Change the spanning tree port priority for an instance
(config-if)# spanning-tree mst 1 cost ?
<1-200000000> Change the interface spanning tree path cost for an instance
(config-if)# spanning-tree mst 1 port-priority ?
<0-240> port priority in increments of 16
(config-if)# spanning-tree mst 1 cost 10
(config-if)# spanning-tree mst 1 port-priority 10

```

Cisco Switch Challenge 49

Area: Switches – Load Sharing with STP port-priorities

Outline

It is possible to create more than one trunk routes, and share traffic between them. Unfortunately loops can occur so STP is used to avoid these. In this case port-priorities are defined for each VLAN, so that specific VLANs take one of the trunk routes.

Objectives

The objectives of this challenge are to:

- Define VTP details.
- Define trunk ports (two, in this case).
- Define port-priority for the trunk ports.

The commands used are:

```
> enable
# config t
(config)# vtp domain test
(config)# vtp mode server
(config)# int fa0/6
(config-if)# spanning-tree vlan 10 port-priority 10
(config-if)# spanning-tree vlan 11 port-priority 10
(config-if)# spanning-tree vlan 12 port-priority 10
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk
(config-if)# exit
(config)# int fa0/10
(config-if)# spanning-tree vlan 13 port-priority 10
(config-if)# spanning-tree vlan 14 port-priority 10
(config-if)# spanning-tree vlan 15 port-priority 10
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk
```

Example

```
> enable
# config t
(config)# vtp ?
  domain      Set the name of the VTP administrative domain.
  file        Configure IFS filesystem file where VTP configuration is stored.
  interface   Configure interface as the preferred source for the VTP IP updater
              address.
  mode        Configure VTP device mode
  password    Set the password for the VTP administrative domain
  pruning     Set the administrative domain to permit pruning
  version     Set the administrative domain to VTP version

(config)# vtp domain ?
  WORD        The ascii name for the VTP administrative domain.
(config)# vtp domain test
(config)# vtp mode ?
  client      Set the device to client mode.
  server      Set the device to server mode.
  transparent Set the device to transparent mode.
(config)# vtp mode server

(config)# int fa0/6
(config-if)# spanning-tree ?
  bpdudfilter Don't send or receive BPDUs on this interface
  bpduguard   Don't accept BPDUs on this interface
  cost        Change an interface's spanning tree port path cost
```

```

guard          Change an interface's spanning tree guard mode
link-type      Specify a link type for spanning tree protocol use
mst            Multiple spanning tree
port-priority  Change an interface's spanning tree port priority
portfast      Enable an interface to move directly to forwarding on link up
stack-port    Enable stack port
vlan          VLAN Switch Spanning Tree
(config-if)# spanning-tree vlan ?
WORD vlan range, example: 1,3-5,7,9-11

(config-if)# spanning-tree vlan 10 ?
cost          Change an interface's per VLAN spanning tree path cost
port-priority Change an interface's spanning tree port priority

(config-if)# spanning-tree vlan 10 cost ?
<1-200000000> Change an interface's per VLAN spanning tree path cost

(config-if)# spanning-tree vlan 10 port-priority ?
<0-240> port priority in increments of 16

(config-if)# spanning-tree vlan 10 port-priority 10
(config-if)# spanning-tree vlan 11 port-priority 10
(config-if)# spanning-tree vlan 12 port-priority 10
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk
(config-if)# exit

(config)# int fa0/10
(config-if)# spanning-tree vlan 13 port-priority 10
(config-if)# spanning-tree vlan 14 port-priority 10
(config-if)# spanning-tree vlan 15 port-priority 10
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk

```

Note the default port-priority is 128. Thus in this example the port priorities for the first trunk will be:

```

VLAN 10 – 10
VLAN 11 – 10
VLAN 12 – 10
VLAN 13 – 128
VLAN 14 – 128
VLAN 15 – 128

```

And for the second trunk:

```

VLAN 10 – 128
VLAN 11 – 128
VLAN 12 – 128
VLAN 13 – 10
VLAN 14 – 10
VLAN 15 – 10

```

Thus the lower priority will be taken, so VLAN 10, 11 and 12 will go through Trunk 1, and VALN 13, 14 and 15 will go through Trunk 2. If either of the trunks fail, the traffic which would normally go through the failed trunk will use the other trunk. In this way there is a fail-back solution, along with load balancing.

Cisco Switch Challenge 50

Area: Switches – Load Sharing with STP costs.

Outline

It is possible to create more than one trunk routes, and share traffic between them. Unfortunately loops can occur so STP is used to avoid these. In this case cost vlans are defined for each VLAN, so that specific VLANs take one of the trunk routes.

Objectives

The objectives of this challenge are to:

- Define VTP details.
- Define trunk ports (two, in this case).
- Define cost values for the trunk ports.

The commands used are:

```
> enable
# config t
(config)# vtp domain test
(config)# vtp mode server
(config)# int fa0/6
(config-if)# spanning-tree vlan 10 cost 10
(config-if)# spanning-tree vlan 11 cost 10
(config-if)# spanning-tree vlan 12 cost 10
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk
(config-if)# exit
(config)# int fa0/10
(config-if)# spanning-tree vlan 13 cost 10
(config-if)# spanning-tree vlan 14 cost 10
(config-if)# spanning-tree vlan 15 cost 10
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk
```

Example

```
> enable
# config t
(config)# vtp domain test
```

```

(config)# vtp mode server

(config)# int fa0/6
(config-if)# spanning-tree vlan 10 cost 10
(config-if)# spanning-tree vlan 11 cost 10
(config-if)# spanning-tree vlan 12 cost 10
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk
(config-if)# exit

(config)# int fa0/10
(config-if)# spanning-tree vlan 13 cost 10
(config-if)# spanning-tree vlan 14 cost 10
(config-if)# spanning-tree vlan 15 cost 10
(config-if)# switchport trunk encapsulation dot1q
(config-if)# switchport mode trunk

```

Note the default cost is 19. Thus in this example the cost for the first trunk will be:

```

VLAN 10 – 10
VLAN 11 – 10
VLAN 12 – 10
VLAN 13 – 19
VLAN 14 – 19
VLAN 15 – 19

```

And for the second trunk:

```

VLAN 10 – 19
VLAN 11 – 19
VLAN 12 – 19
VLAN 13 – 10
VLAN 14 – 10
VLAN 15 – 10

```

Thus the lower cost will be taken, so VLAN 10, 11 and 12 will go through Trunk 1, and VLAN 13, 14 and 15 will go through Trunk 2. If either of the trunks fails, the traffic which would normally go through the failed trunk will use the other trunk. In this way there is a fail-back solution, along with load balancing.

Cisco Switch Challenge 51

Outline

This challenge involves the configuration of MST.

Objectives

The objectives of this challenge are to:

- Define MST.

Example

Switch(config)#spanning-tree mst ?

```
WORD          MST instance range, example: 0-3,5,7-9
configuration  Enter MST configuration submode
forward-time   Set the forward delay for the spanning tree
hello-time     Set the hello interval for the spanning tree
max-age        Set the max age interval for the spanning tree
max-hops       Set the max hops value for the spanning tree
```

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#?

```
abort         Exit region configuration mode, aborting changes
exit          Exit region configuration mode, applying changes
instance      Map vlans to an MST instance
name          Set configuration name
no            Negate a command or set its defaults
private-vlan  Set private-vlan synchronization
revision      Set configuration revision number
show          Display region configurations
```

Switch(config-mst)#instance ?

```
<0-15> MST instance id
```

Switch(config-mst)#instance 1 ?

```
vlan Range of vlans to add to the instance mapping
```

Switch(config-mst)#instance 1 vlan ?

```
LINE vlan range ex: 1-65, 72, 300 -200
```

Switch(config-mst)#instance 1 vlan 10

Switch(config-mst)#name ?

```
WORD Configuration name
```

Switch(config-mst)#name region1

Switch(config-mst)#revision ?

```
<0-65535> Configuration revision number
```

Switch(config-mst)#revision 1

Switch(config-mst)#show pending

```
Pending MST configuration
```

```
Name [region1]
```

```
Revision 1
```

```
Instance Vlans mapped
```

```
-----  
0          1-9,11-4094
```

```
1          10
```

Switch(config-mst)#

Cisco Switch Challenge 52 (Primary root switch)

Area: Switches - RSTP and MSTP

Outline

This challenge involves configuring a primary root switch for a given instance, with a point-to-point link for rapid transitions.

Objectives

The objectives of this challenge are to:

- Define a primary root.
- Define MST parameters on the interface, such as cost and port-priority.
- Define global MST parameters, such as hello time, forward-time, maximum age, maximum hops and priority.
- Define a point-to-point link for rapid transitions.

The commands used are:

```
> enable
# config t
(config)# spanning-tree mst 1 root primary
(config)# spanning-tree mst hello-time 10
(config)# spanning-tree mst forward-time 10
(config)# spanning-tree mst 1 priority 10
(config)# spanning-tree mst max-age 10
(config)# spanning-tree mst max-hops 10
(config)# int fa0/1
(config-if)# spanning-tree mst 1 cost 10
(config-if)# spanning-tree mst 1 port-priority 10
(config-if)# spanning-tree link-type point-to-point
```

Example

```
> enable
# config t
(config)# spanning-tree mst 1 root primary
(config)# spanning-tree mst hello-time 10
(config)# spanning-tree mst forward-time 10
(config)# spanning-tree mst 1 priority 10
(config)# spanning-tree mst max-age 10
(config)# spanning-tree mst max-hops 10
```

```

(config)# int fa0/1
(config-if)# spanning-tree mst 1 cost 10
(config-if)# spanning-tree mst 1 port-priority 10
(config-if)# spanning-tree ?
  bpduguard      Don't send or receive BPDUs on this interface
  bpduguard      Don't accept BPDUs on this interface
  cost           Change an interface's spanning tree port path cost
  guard          Change an interface's spanning tree guard mode
  link-type      Specify a link type for spanning tree protocol use
  mst            Multiple spanning tree
  port-priority  Change an interface's spanning tree port priority
  portfast       Enable an interface to move directly to forwarding on link up
  stack-port     Enable stack port
  vlan           VLAN Switch Spanning Tree
(config-if)# spanning-tree link-type ?
  point-to-point Consider the interface as point-to-point
  shared         Consider the interface as shared
(config-if)# spanning-tree link-type point-to-point

```

Cisco Switch Challenge 53

Outline

This challenge involves the configuration of a Etherchannel.

Objectives

The objectives of this challenge are to:

- Define Etherchannel on ports.

Example

```

# config t
(config)# int fa0/1
(config-if)# channel-group ?
  <1-64> Channel group number
(config-if)# channel-g 3 ?
  mode Etherchannel Mode of the interface
(config-if)# channel-g 3 m ?
  active      Enable LACP unconditionally
  auto        Enable PAGP only if a PAGP device is detected
  desirable   Enable PAGP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected
(config-if)# channel-group 3 mode ?
  active      Enable LACP unconditionally
  auto        Enable PAGP only if a PAGP device is detected
  desirable   Enable PAGP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected
(config-if)# channel-group 3 mode on
(config-if)# int fa0/2
(config-if)# channel-group 4 mode on

```

Cisco Switch Challenge 54

Outline

This challenge involves configuring LACP (Link Aggregation Control Protocol - IEEE 802.3ad). The LACP packets use EtherChannels to intercommunicate, where the neighbours and port group capabilities are learnt and compared with local switch capabilities. In LACP there are roles assigned to the EtherChannel endpoints. Thus the switch with the **lowest system priority** is then elected to make decisions about what ports are actively participating in the EtherChannel.

Objectives

The objectives of this challenge are to:

- Configure for LACP (Link Aggregation Control Protocol).

The commands used are:

```
(config)# lACP system-priority 2
(config)# interface fa0/1
(config-if)# channel-protocol lACP
(config-if)# channel-group 1 mode on
(config-if)# lACP port-priority 1
```

Example

```
(config)# lACP ?
  system-priority  LACP priority for the system

(config)# lACP system-priority ?
  <1-65535>  Priority value
(config)# lACP system-priority 2
(config)# interface fa0/1
(config-if)# channel-protocol ?
  lACP  Prepare interface for LACP protocol
  pAgP  Prepare interface for PAgP protocol

(config-if)# channel-protocol lACP
(config-if)# channel-group ?
  <1-6>  Channel group number

(config-if)# channel-group 1 ?
  mode  Etherchannel Mode of the interface

(config-if)# channel-group 1 mode ?
  active  Enable LACP unconditionally
  auto    Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on      Enable Etherchannel only
  passive  Enable LACP only if a LACP device is detected
```

```
(config-if)# channel-group 1 mode active
(config-if)# lacp ?
    port-priority  LACP priority on this interface

(config-if)# lacp port-priority ?
    <1-65535>  Priority value

(config-if)# lacp port-priority 1
```

Cisco Switch Test 3 (Challenge 55)

Unit 3: STP

The most up-to-date version of this test is at:

<http://networksims.com/sw03.html>

Cisco Switch Challenge 56

Area: Switches – Defining trunk ports

Outline

The Dot1q encapsulation protocol allows for a trunk connection to interconnect VLANs on different switches.

Objectives

The objectives of this challenge are to:

- Define normal switch port.
- Define a trunk port.

The commands used are:

```
> enable
# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# exit
```

```

(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/6
(config-if)# switchport trunk mode dot1q

```

Example

```

> enable
# config t
(config)# int fa0/1
(config-if)# sw ?
    access      Set access mode characteristics of the interface
    block       Disable forwarding of unknown uni/multi cast addresses
    broadcast    Set broadcast suppression level on this interface
    encapsulation Set trunking encapsulation when interface is in trunking mode
    host        Set port host
    mode        Set trunking mode of the interface
    multicast    Set multicast suppression level on this interface
    native      Set trunking native characteristics when interface is in
                trunking mode
    nonegotiate Device will not engage in negotiation protocol on this
                interface
    port-security Security related command
    priority    Set appliance 802.1p priority
    protected   Configure an interface to be a protected port
    pruning     Set pruning VLAN characteristics when interface is in trunking
                mode
    trunk       Set trunking characteristics of the interface
    unicast     Set unicast suppression level on this interface
    voice       Voice appliance attributes
    <cr>
(config-if)# sw mo ?
    access      Set trunking mode to ACCESS unconditionally
    dot1q-tunnel Set trunking mode to DOT1Q TUNNEL unconditionally
    dynamic     Set trunking mode to dynamically negotiate access or trunk mode
    trunk       Set trunking mode to TRUNK unconditionally
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/6
(config-if)# sw t ?
    allowed     Set allowed VLAN characteristics when interface is in trunking
                mode
    encapsulation Set trunking encapsulation when interface is in trunking mode
    native      Set trunking native characteristics when interface is in
                trunking mode

```

```
pruning          Set pruning VLAN characteristics when interface is in trunking
mode
(config-if)# switchport trunk mode dot1q
```

Cisco Switch Challenge 57

Area: Switches – Defining trunk ports

Outline

The Dot1q encapsulation protocol allows for a trunk connection to interconnect VLANs on different switches and define the VLAN to stop trunking on an interface.

Objectives

The objectives of this challenge are to:

- Define normal switch port.
- Define a trunk port.
- Define a port to stop trunking for a given VLAN.

The commands used are:

```
> enable
# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/6
(config-if)# switchport trunk mode dot1q
(config-if)# switchport access vlan 5
(config-if)# switchport trunk native vlan 6
```

Example

```
> enable
```

```

# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/6
(config-if)# switchport trunk mode dot1q
(config-if)# switchport access ?
    vlan    Set VLAN when interface is in access mode

(config-if)# switchport access vlan ?
    <1-4094> VLAN ID of the VLAN when this port is in access mode
    dynamic  When in access mode, this interfaces VLAN is controlled by VMPS

(config-if)# switchport access vlan 5

(config-if)# switchport trunk ?
    allowed      Set allowed VLAN characteristics when interface is in trunking
                  mode
    encapsulation Set trunking encapsulation when interface is in trunking mode
    native       Set trunking native characteristics when interface is in
                  trunking mode
    pruning      Set pruning VLAN characteristics when interface is in trunking
                  mode

(config-if)# switchport trunk native ?
    vlan    Set native VLAN when interface is in trunking mode

(config-if)# switchport trunk native vlan ?
    <1-4094> VLAN ID of the native VLAN when this port is in trunking mode

(config-if)# switchport trunk native vlan 6

```

In this example FA0/6 will **stop** trunking for VLAN 5, and the native VLAN is defined as VLAN 6.

Cisco Switch Challenge 58

Area: Switches – Defining trunk ports

Outline

The Dot1q encapsulation protocol allows for a trunk connection to interconnect VLANs on different switches and define the VLAN to stop trunking on an interface.

Objectives

The objectives of this challenge are to:

- Define normal switch port.
- Define a trunk port.
- Remove a VLAN from trunking.

The commands used are:

```
> enable
# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/6
(config-if)# switchport trunk mode dot1q
(config-if)# switchport trunk allowed vlan remove 2
(config-if)# switchport trunk allowed vlan remove 3
```

Example

```
> enable
# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/6
(config-if)# switchport trunk mode dot1q
(config-if)# switchport t ?
```

```

allowed          Set allowed VLAN characteristics when interface is in trunking
                  mode
encapsulation    Set trunking encapsulation when interface is in trunking mode
native          Set trunking native characteristics when interface is in
                  trunking mode
pruning          Set pruning VLAN characteristics when interface is in trunking
                  mode

(config-if)# switchport t a ?
vlan            Set allowed VLANs when interface is in trunking mode

(config-if)# switchport t a v ?
WORD           VLAN IDs of the allowed VLANs when this port is in trunking mode
add            add VLANs to the current list
all           all VLANs
except        all VLANs except the following
none         no VLANs
remove       remove VLANs from the current list

(config-if)# switchport trunk allowed vlan remove ?
WORD          VLAN IDs of disallowed VLANs when this port is in trunking mode

(config-if)# switchport trunk allowed vlan remove 2
(config-if)# switchport trunk allowed vlan remove 3

```

Cisco Switch Challenge 59

Area: Switches – Defining trunk ports

Outline

The Dot1q encapsulation protocol allows for a trunk connection to interconnect VLANs on different switches and define the VLAN to be removed from VLAN pruning.

Objectives

The objectives of this challenge are to:

- Define normal switch port.
- Define a trunk port.
- Remove a VLAN from pruning.

The commands used are:

```

> enable
# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport mode access
(config-if)# exit

```

```

(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/6
(config-if)# switchport trunk mode dot1q
(config-if)# switchport trunk pruning vlan remove 10

```

Example

```

> enable
# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/2
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/3
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/4
(config-if)# switchport mode access
(config-if)# exit

(config)# int fa0/6
(config-if)# switchport trunk mode dot1q

(config-if)# switchport t ?
    allowed          Set allowed VLAN characteristics when interface is in trunking
                    mode
    encapsulation    Set trunking encapsulation when interface is in trunking mode
    native           Set trunking native characteristics when interface is in
                    trunking mode
    pruning          Set pruning VLAN characteristics when interface is in trunking
                    mode

(config-if)# sw t p ?
    vlan            Set VLANs enabled for pruning when interface is in trunking mode

(config-if)# sw t p v ?
    WORD           VLAN IDs of the allowed VLANs when this port is in trunking mode
    add            add VLANs to the current list
    except         all VLANs except the following
    none           no VLANs
    remove         remove VLANs from the current list

(config-if)# sw t p v r ?
    WORD           VLAN IDs of disallowed VLANs when this port is in trunking mode
(config-if)# switchport trunk pruning vlan remove 10

```

Cisco Switch Test 4 (Challenge 60)

Unit 4: InterVLAN

The most up-to-date version of this test is at:

<http://networksims.com/sw04.html>

Cisco Switch Challenge 61

Area: Switches – IP Unicast Routing

Outline

This challenge involves configuring a port (FA0/1) for Layer 3 access.

Objectives

The objectives of this challenge are to:

- Define Layer 3 access.
- Define an IP address for FA0/1.
- Define classless IP addresses.
- Define zero-subnet.

The commands used are:

```
> enable
# config t
(config)# int fa0/1
(config-if)# no switchport
(config-if)# ip address 1.2.3.4 255.255.0.0
(config-if)# no shutdown
(config-if)# exit
(config)# ip subnet-zero
(config)# ip classless
```

Example

```
> enable
# config t
# int fa0/1
(config-if)# no switchport
(config-if)# ip address ?
  A.B.C.D  IP address
```

```

(config-if)# ip address 1.2.3.4 ?
    A.B.C.D  IP subnet mask
(config-if)# ip address 1.2.3.4 255.255.0.0
(config-if)# no shutdown
(config-if)# exit

```

```

(config)# ip ?

```

```

Global IP configuration subcommands:
  access-list          Named access-list
  accounting-list      Select hosts for which IP accounting information is
                       kept
  accounting-threshold Sets the maximum number of accounting entries
  accounting-transits  Sets the maximum number of transit entries
  alias                Alias an IP address to a TCP port
  as-path              BGP autonomous system path filter
  bgp-community        format for BGP community
  cef                  Cisco Express Forwarding
  classless            Follow classless routing forwarding rules
  community-list       Add a community list entry
  default-gateway      Specify default gateway (if not routing IP)
  default-network      Flags networks as candidates for default routes
  dhcp                 Configure DHCP server, relay and snooping parameters
  dhcp-server          Specify address of DHCP server to use
  domain-list          Domain name to complete unqualified host names.
  domain-lookup        Enable IP Domain Name System hostname translation
  domain-name          Define the default domain name
  dvmrp                DVMRP global commands
  extcommunity-list   Add a extended community list entry
  finger              finger server
  flow-aggregation     Configure flow aggregation
  flow-cache           Configure netflow cache parameters
  flow-export          Specify host/port to send flow statistics
  forward-protocol     Controls forwarding of physical and directed IP
                       broadcasts
  ftp                  FTP configuration commands
  gdp                  Router discovery mechanism
  gratuitous-arps      Generate gratuitous ARPs for PPP/SLIP peer addresses
  host                 Add an entry to the ip hostname table
  host-routing         Enable host-based routing (proxy ARP and redirect)
  hp-host              Enable the HP proxy probe service
  http                 HTTP server configuration
  icmp                 ICMP options
  igmp                 IGMP global configuration
  local                Specify local options
  mrm                  Configure IP Multicast Routing Monitor test parameters
  mroute               Configure static multicast routes
  msdp                 MSDP global commands
  multicast            Global IP Multicast Commands
  multicast-routing    Enable IP multicast forwarding
  name-server          Specify address of name server to use
  ospf                 OSPF
  pim                  PIM global commands
  prefix-list          Build a prefix list
  radius               RADIUS configuration commands
  rcmd                 Rcmd commands
  reflexive-list       Reflexive access list
  route                Establish static routes
  routing              Enable IP routing
  sap                  Global IP Multicast SAP Commands
  sdr                  Global IP Multicast SDR Commands
  security             Specify system wide security information
  source-route         Process packets with source routing header options

```

sticky-arp	Allow the creation of sticky ARP entries
subnet-zero	Allow 'subnet zero' subnets
tacacs	TACACS configuration commands
tcp	Global TCP parameters
telnet	Specify telnet options
tftp	tftp configuration commands
vrf	Configure an IP VPN Routing/Forwarding instance
wccp	Web-Cache Coordination Protocol Commands

```
(config)# ip subnet-zero
(config)# ip classless
```

Cisco Switch Challenge 62

Area: Switches – IP Unicast Routing

Outline

This challenge involves configuring a static ARP cache, and other ARP details.

Objectives

The objectives of this challenge are to:

- Define the default gateway (if routing is not enabled).
- Define a static ARP value.
- Define ARP timeout.

The commands used are:

```
> enable
# config t
(config)# ip default-gateway 1.2.3.4
(config)# arp 1.2.3.4 1.1.1
(config)# int fa0/1
(config-if)# arp timeout 10
(config-if)# ip proxy-arp
(config-if)# arp arpa
```

Example

```
> enable
# config t
(config)# ip default-gateway ?
  A.B.C.D  IP address of default gateway
(config)# ip default-gateway 1.2.3.4

(config)# arp ?
  A.B.C.D  IP address of ARP entry
  vrf     Configure static ARP for a VPN Routing/Forwarding instance

(config)# arp 1.2.3.4 ?
  H.H.H  48-bit hardware address of ARP entry
```

```
(config)# arp 1.2.3.4 1.1.1 ?
```

```
arpa   ARP type ARPA
sap    ARP type SAP (HP's ARP type)
smds   ARP type SMDS
snap   ARP type SNAP (FDDI and TokenRing)
srp-a  ARP type SRP (side A)
srp-b  ARP type SRP (side B)
```

```
(config)# int fa0/1
```

```
(config-if)# arp ?
```

```
arpa           Standard arp protocol
frame-relay    Enable ARP for a frame relay interf
probe          HP style arp protocol
snap           IEEE 802.3 style arp
timeout        Set ARP cache timeout
```

```
(config-if)# arp arpa
```

```
(config-if)# arp t ?
```

```
<0-2147483> Seconds
```

```
(config-if)# arp timeout 10
```

```
(config-if)# ip ?
```

Interface IP configuration subcommands:

```
access-group   Specify access control for packets
accounting     Enable IP accounting on this interface
address        Set the IP address of an interface
authentication authentication subcommands
bandwidth-percent Set EIGRP bandwidth limit
bgp            BGP interface commands
broadcast-address Set the broadcast address of an interface
cef            Cisco Express Forwarding interface commands
cgmp           Enable/disable CGMP
dhcp           Configure DHCP parameters for this interface
directed-broadcast Enable forwarding of directed broadcasts
dvmrp         DVMRP interface commands
hello-interval Configures IP-EIGRP hello interval
helper-address Specify a destination address for UDP broadcasts
hold-time      Configures IP-EIGRP hold time
igmp           IGMP interface commands
irdp           ICMP Router Discovery Protocol
load-sharing   Style of load sharing
local-proxy-arp Enable local-proxy ARP
mask-reply     Enable sending ICMP Mask Reply messages
mrm            Configure IP Multicast Routing Monitor tester
mroute-cache  Enable switching cache for incoming multicast packets
mtu            Set IP Maximum Transmission Unit
multicast     IP multicast interface commands
ospf          OSPF interface commands
pim           PIM interface commands
policy        Enable policy routing
probe         Enable HP Probe support
proxy-arp     Enable proxy ARP
rarp-server   Enable RARP server for static arp entries
redirects     Enable sending ICMP Redirect messages
rgmp          Enable/disable RGMP
rip           Router Information Protocol
route-cache   Enable fast-switching cache for outgoing packets
sap           Session Advertisement Protocol interface commands
sdr           Session Directory Protocol interface commands
security      DDN IP Security Option
split-horizon Perform split horizon
```

```
summary-address      Perform address summarization
unnumbered           Enable IP processing without an explicit address
unreachables         Enable sending ICMP Unreachable messages
urd                  Configure URL Rendezvousing
vrf                  VPN Routing/Forwarding parameters on the interface
wccp                 WCCP interface commands
(config-if)# ip proxy-arp
```

Cisco Switch Challenge 63

Area: Switches – IP Unicast Routing (IDRP)

Outline

This challenge involves configuring ICMP Router Discovery Protocol (IDRP), which can be used to dynamically learn routes to other networks. For this it sends out discovery packets.

Objectives

The objectives of this challenge are to:

- Define Layer 3 operation on FA0/1.
- Enable IDRP.
- Define IDRP details.

The commands used are:

```
> enable
# config t
(config)# int fa0/1
(config)# no switchport
(config-if)# ip irdp ?
(config-if)# ip irdp multicast
(config-if)# ip irdpmaxadvertinterval 10
(config-if)# ip irdpholdtime 10
(config-if)# ip irdpminadvertinterval 5
(config-if)# ip irdppreference 0
```

Example

```
> enable
# config t

(config)# int fa0/1
(config)# no switchport
(config-if)# ip irdp ?
<cr>
address                addresses to proxy-advertise
holdtime                how long a receiver should believe the information
maxadvertinterval      maximum time between advertisements
minadvertinterval      minimum time between advertisements
```

```

multicast          advertisements are sent with multicasts
preference         preference level for this interface
(config-if)# ip irdp ?
(config-if)# ip irdp multicast

(config-if)# ip irdp max ?
0                 advertise only when solicited
<4-1800>          maximum time between advertisements (default 600 seconds)
(config-if)# ip irdp ma ?
0                 advertise only when solicited
<4-1800>          maximum time between advertisements (default 600 seconds)

(config-if)# ip irdp maxadvertinterval 10
(config-if)# ip irdp holdtime ?
<0-9000>          holdtime (default 1800 seconds)
(config-if)# ip irdp holdtime 10
(config-if)# ip irdp minadvertinterval ?
<3-1800>          minimum time between advertisements (default 450 seconds)
(config-if)# ip irdp minadvertinterval 5

(config-if)# ip irdpp ?
<-2147483648 - 2147483647> preference for this address (higher values
                                                                    preferred)
(config-if)# ip irdp preference 0

```

Notes

The **minadvertinterval** and **holdtime** are based on the **maxadvertinterval**, where **minadvertinterval** is, as a default, set to 75% of the **maxadvertinterval**, and the **holdtime** is, by default, set to three times the **maxadvertinterval**. Thus **maxadvertinterval** must be set before the other two, as they will be set automatically to the default. After this the **minadvertinterval** and **holdtime** can then be customized.

Cisco Switch Challenge 64

Area: Switches – IP Unicast Routing (Broadcast handling)

Outline

This challenge involves defining the ports and protocols are used for forwarding broadcast packets (**ip forward-protocol**), and where there is a broadcast-to-physical translation on an interface (**ip directed-broadcast**).

Objectives

The objectives of this challenge are to:

- Define Layer 3 operation on FA0/1.
- Define details for forwarding broadcast packets (**ip forward-protocol**).
- Enable the broadcast-to-physical translation on an interface (**ip directed-broadcast**).

The commands used are:

```

> enable
# config t
(config)# int fa0/1
(config)# no switchport
(config-if)# ip directed-broadcast
(config-if)# exit
(config)# ip forward-protocol udp time
(config)# ip forward-protocol udp echo
(config)# ip forward-protocol udp syslog

```

Example

```

> enable
# config t

(config)# int fa0/1
(config)# no switchport
(config-if)# ip directed-broadcast ?
<1-199>      A standard IP access list number
<1300-2699> A standard IP expanded access list number
<cr>
(config-if)# exit

(config)# ip forward-protocol ?
nd           Sun's Network Disk protocol
sdns         Network Security Protocol
spanning-tree Use transparent bridging to flood UDP broadcasts
turbo-flood  Fast flooding of UDP broadcasts
udp          Packets to a specific UDP port

(config)# ip forward-protocol udp ?
<0-65535>    Port number
biff         Biff (mail notification, comsat, 512)
bootpc       Bootstrap Protocol (BOOTP) client (68)
bootps       Bootstrap Protocol (BOOTP) server (67)
discard      Discard (9)
dnsix        DNSIX security protocol auditing (195)
domain       Domain Name Service (DNS, 53)
echo         Echo (7)
isakmp       Internet Security Association and Key Management Protocol (500)
mobile-ip    Mobile IP registration (434)
nameserver   IEN116 name service (obsolete, 42)
netbios-dgm  NetBios datagram service (138)
netbios-ns   NetBios name service (137)
netbios-ss   NetBios session service (139)
ntp          Network Time Protocol (123)
pim-auto-rp  PIM Auto-RP (496)
rip          Routing Information Protocol (router, in.routed, 520)
snmp         Simple Network Management Protocol (161)
snmptrap     SNMP Traps (162)
sunrpc       Sun Remote Procedure Call (111)
syslog       System Logger (514)
tacacs       TAC Access Control System (49)
talk         Talk (517)
tftp         Trivial File Transfer Protocol (69)
time         Time (37)
who          Who service (rwho, 513)
xdmcp        X Display Manager Control Protocol (177)
<cr>

```

```
(config)# ip forward-protocol udp time
(config)# ip forward-protocol udp echo
(config)# ip forward-protocol udp syslog
```

Cisco Switch Challenge 65

Area: Switches – IP Unicast Routing (Broadcast handling/helper address)

Outline

This challenge involves defining the ports and protocols are used for forwarding broadcast packets (**ip forward-protocol**), and a helper address for broadcasts.

Objectives

The objectives of this challenge are to:

- Define Layer 3 operation on FA0/1.
- Define details for forwarding broadcast packets (**ip forward-protocol**).
- Define a helper-address.
-

The commands used are:

```
> enable
# config t
(config)# ip forward-protocol udp time
(config)# ip forward-protocol udp echo
(config)# ip forward-protocol udp syslog
(config)# int fa0/1
(config)# no switchport
(config-if)# ip helper-address 1.2.3.4
```

Example

```
> enable
# config t
(config)# ip forward-protocol udp time
(config)# ip forward-protocol udp echo
(config)# ip forward-protocol udp syslog

(config)# ip forward-protocol ?
nd                Sun's Network Disk protocol
sdns              Network Security Protocol
spanning-tree    Use transparent bridging to flood UDP broadcasts
turbo-flood      Fast flooding of UDP broadcasts
udp              Packets to a specific UDP port

(config)# ip forward-protocol spanning-tree

(config)# int fa0/1
(config)# no switchport
```

```
(config-if)# ip helper-address ?  
A.B.C.D IP destination address  
(config-if)# ip helper-address 1.2.3.4
```

Cisco Switch Challenge 66

Area: Switches – IP Unicast Routing (Broadcast handling/IP flooding)

Outline

This challenge involves defining an address to deal with broadcasts (**ip broadcast-address**), and the enabling of fast flooding for UDP broadcast (**ip forward-protocol turbo-flood**).

Objectives

The objectives of this challenge are to:

- Define Layer 3 operation on FA0/1.
- Define details for the broadcast address.
- Enable turbo-flooding support.

The commands used are:

```
> enable  
# config t  
(config)# int fa0/1  
(config)# no switchport  
(config-if)# ip broadcast-address 1.2.3.4  
(config-if)# exit  
(config)# ip forward-protocol turbo-flood
```

Example

```
> enable  
# config t  
(config)# ip forward-protocol ?  
nd          Sun's Network Disk protocol  
sdns        Network Security Protocol  
spanning-tree Use transparent bridging to flood UDP broadcasts  
turbo-flood Fast flooding of UDP broadcasts  
udp         Packets to a specific UDP port  
  
(config)# ip forward-protocol turbo-flood  
  
(config)# int fa0/1  
(config)# no switchport  
(config-if)# ip broadcast-address ?  
A.B.C.D IP broadcast address  
(config-if)# ip broadcast-address 1.2.3.4  
(config-if)# exit
```

Cisco Switch Challenge 67

Area: Switches – IP Unicast Routing (IP Routing/ RIP)

Outline

This challenge involves enabling IP routing (ip routing), and configuring RIP.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define RIP details for the network to broadcast into.

The commands used are:

```
> enable
# config t
(config)# ip routing
(config)# router rip
(config-router)# router rip
(config-router)# network 10.0.0.0
(config-router)# neighbor 10.0.0.1
```

Example

```
> enable
# config t
(config)# ip routing

(config)# router ?
  bgp      Border Gateway Protocol (BGP)
  egp      Exterior Gateway Protocol (EGP)
  eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
  igmp     Interior Gateway Routing Protocol (IGMP)
  isis     ISO IS-IS
  iso-igrp IGRP for OSI networks
  mobile   Mobile routes
  odr      On Demand stub Routes
  ospf     Open Shortest Path First (OSPF)
  rip      Routing Information Protocol (RIP)
  static   Static routes
(config)# router rip
Switch(config-router)# ?
Router configuration commands:
  address-family  Enter Address Family command mode
  auto-summary    Enable automatic network number summarization
  default         Set a command to its defaults
  default-information  Control distribution of default information
  default-metric  Set metric of redistributed routes
  distance        Define an administrative distance
```

```

distribute-list      Filter networks in routing updates
exit                Exit from routing protocol configuration mode
flash-update-threshold Specify flash update threshold in second
help               Description of the interactive help system
input-queue        Specify input queue depth
maximum-paths      Forward packets over multiple paths
neighbor           Specify a neighbor router
network            Enable routing on an IP network
no                Negate a command or set its defaults
offset-list        Add or subtract offset from IGRP or RIP metrics
output-delay       Interpacket delay for RIP updates
passive-interface  Suppress routing updates on an interface
redistribute       Redistribute information from another routing
                  protocol
timers             Adjust routing timers
traffic-share      How to compute traffic share over alternate paths
validate-update-source Perform sanity checks against source address of
                  routing updates
version           Set routing protocol version (config-router)
# network ?
  A.B.C.D Network number
(config-router)# network 10.0.0.0
(config-router)# neighbor 10.0.0.1

```

Cisco Switch Challenge 68

Area: Switches – IP Unicast Routing (IP Routing/ RIP)

Outline

This challenge involves enabling IP routing (ip routing), and configuring RIP.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define RIP version.
- Define RIP timers.
- Disable auto-summary.

The commands used are:

```

> enable
# config t
(config)# ip routing
(config)# router rip
(config-router)# version 2
(config-router)# timers basic 10 10 10 10
(config-router)# no auto-summary

```

Example

```

> enable
# config t
(config)# ip routing

(config)# router rip
(config-router)# version ?
<1-2> version

(config-router)# timers ?
basic Basic routing protocol update timers

(config-router)# timers basic ?
<0-4294967295> Interval between updates

(config-router)# timers basic 10 ?
<1-4294967295> Invalid

(config-router)# timers basic 10 10 ?
<0-4294967295> Holddown

(config-router)# timers basic 10 10 10 ?
<1-4294967295> Flush

(config-router)# timers basic 10 10 10 10 ?
<1-4294967295> Sleep time, in milliseconds
<cr>

(config-router)# timers basic 10 10 10 10

(config-router)# no ?
address-family Enter Address Family command mode
auto-summary Enable automatic network number summarization
default-information Control distribution of default information
default-metric Set metric of redistributed routes
distance Define an administrative distance
distribute-list Filter networks in routing updates
flash-update-threshold Specify flash update threshold in second
input-queue Specify input queue depth
maximum-paths Forward packets over multiple paths
neighbor Specify a neighbor router
network Enable routing on an IP network
offset-list Add or subtract offset from IGRP or RIP metrics
output-delay Interpacket delay for RIP updates
passive-interface Suppress routing updates on an interface
redistribute Redistribute information from another routing
protocol
timers Adjust routing timers
traffic-share How to compute traffic share over alternate paths
validate-update-source Perform sanity checks against source address of
routing updates
version Set routing protocol version
(config-router)# no auto-summary

```

Cisco Switch Challenge 69

Area: Switches – IP Unicast Routing (IP Routing/ RIP)

Outline

This challenge involves enabling RIP authentication.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define RIP version.
- Define RIP Version 2.
- Define Authenticated RIP.

The commands used are:

```
> enable
# config t
(config)# ip routing
(config)# key chain test
(config-keychain)# key 1
(config-keychain-key)# key-string mykey
(config-keychain-key)# exit
(config-keychain)# exit
(config)# router rip
(config-router)# version 2
(config)# int fa0/1
(config-if)# ip rip authentication key-chain test
(config-if)# ip rip authentication mode md5
```

Example

```
> enable
# config t
(config)# ip routing

(config)# key ?
  chain      Key-chain management
  config-key Set a private configuration key

(config)# key chain ?
  WORD      Key-chain name

(config)# key chain test
(config-keychain)# ?
Key-chain configuration commands:
  default   Set a command to its defaults
  exit      Exit from key-chain configuration mode
  key       Configure a key
  no        Negate a command or set its defaults
(config-keychain)# key ?
  <0-2147483647> Key identifier
(config-keychain)# key 1
(config-keychain-key)# ?
Key-chain key configuration commands:
  accept-lifetime Set accept lifetime of key
  default         Set a command to its defaults
```

```

exit                Exit from key-chain key configuration mode
key-string          Set key string
no                 Negate a command or set its defaults
send-lifetime       Set send lifetime of key
(config-keychain-key)# key-string ?
<0-7>              Encryption type (0 to disable encryption, 7 for proprietary)
LINE              The key
(config-keychain-key)# key-string mykey
(config-keychain-key)# exit
(config-keychain)# exit

(config)# router rip
(config-router)# version 2
<1-2>              version

(config)# int fa0/1

(config-if)# ip ri ?
authentication      Authentication control
receive             advertisement reception
send                advertisement transmission
v2-broadcast        send ip broadcast v2 update

(config-if)# ip rip a ?
key-chain           Authentication key-chain
mode                Authentication mode

(config-if)# ip rip authentication key-chain ?
LINE               name of key-chain
(config-if)# ip rip authentication key-chain test
(config-if)# ip rip authentication mode ?
md5                Keyed message digest
text               Clear text authentication
(config-if)# ip rip authentication mode md5

```

Cisco Switch Challenge 70

Area: Switches – IP Unicast Routing (IP Routing/ RIP)

Outline

This challenge involves defining summary address and split-horizon.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define a summary address.
- Define no split-horizon.

The commands used are:

```

> enable
# config t
(config)# ip routing
(config)# router rip
(config-router)# network 10.0.0.0
(config-router)# version 2
(config)# int fa0/1
(config-if)# no switchport
(config-if)# ip summary-address rip 1.2.3.4 255.255.0.0
(config-if)# no ip split-horizon

```

Example

```

> enable
# config t
(config)# ip routing
(config)# router rip
(config-router)# network 10.0.0.0
(config-router)# version 2
(config)# int fa0/1
(config-if)# no switchport

(config-if)# ip summary-address ?
    eigrp  Enhanced Interior Gateway Routing Protocol (EIGRP)
    rip    Routing Information Protocol (RIP)
(config-if)# ip summary-address r ?
    A.B.C.D  IP address
(config-if)# ip summary-address r 1.2.3.4 ?
    A.B.C.D  IP network mask
(config-if)# ip summary-address rip 1.2.3.4 255.255.0.0

```

```

(config-if)# no ip ?
Interface IP configuration subcommands:
access-group      Specify access control for packets
accounting        Enable IP accounting on this interface
address           Set the IP address of an interface
authentication    authentication subcommands
bandwidth-percent Set EIGRP bandwidth limit
bgp               BGP interface commands
broadcast-address Set the broadcast address of an interface
cef               Cisco Express Forwarding interface commands
cgmp              Enable/disable CGMP
dhcp              Configure DHCP parameters for this interface
directed-broadcast Enable forwarding of directed broadcasts
dvmrp             DVMRP interface commands
hello-interval    Configures IP-EIGRP hello interval
helper-address    Specify a destination address for UDP broadcasts
hold-time         Configures IP-EIGRP hold time
igmp              IGMP interface commands
irdp              ICMP Router Discovery Protocol
load-sharing      Style of load sharing
local-proxy-arp   Enable local-proxy ARP
mask-reply        Enable sending ICMP Mask Reply messages
mrm               Configure IP Multicast Routing Monitor tester
mroute-cache     Enable switching cache for incoming multicast packets
mtu               Set IP Maximum Transmission Unit
multicast         IP multicast interface commands
ospf              OSPF interface commands
pim               PIM interface commands
policy            Enable policy routing
probe             Enable HP Probe support
proxy-arp         Enable proxy ARP

```

```

rarp-server      Enable RARP server for static arp entries
redirects       Enable sending ICMP Redirect messages
rgmp            Enable/disable RGMP
rip            Router Information Protocol
route-cache     Enable fast-switching cache for outgoing packets
sap            Session Advertisement Protocol interface commands
sdr            Session Directory Protocol interface commands
security       DDN IP Security Option
split-horizon   Perform split horizon
summary-address Perform address summarization
unnumbered     Enable IP processing without an explicit address
unreachables   Enable sending ICMP Unreachable messages
urd            Configure URL Rendezvousing
vrf            VPN Routing/Forwarding parameters on the interface
wccp          WCCP interface commands
(config-if)# no ip split-horizon

```

Cisco Switch Challenge 71

Area: Switches – IP Unicast Routing (IP Routing/IGRP)

Outline

This challenge involves enabling IGRP authentication.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define IGRP details.

The commands used are:

```

> enable
# config t
(config)# ip routing
(config)# router igrp 111
(config-router)# network 1.2.3.0
(config-router)# neighbor 1.2.3.1
(config-router)# metric maximum-hops 10
(config-router)# timers basic 10 10 10 10

```

Example

```

> enable
# config t
(config)# ip routing

(config)# router ?
  bgp      Border Gateway Protocol (BGP)
  egp      Exterior Gateway Protocol (EGP)

```

```

eigrp      Enhanced Interior Gateway Routing Protocol (EIGRP)
igrp       Interior Gateway Routing Protocol (IGRP)
isis       ISO IS-IS
iso-igrp   IGRP for OSI networks
mobile     Mobile routes
odr        On Demand stub Routes
ospf       Open Shortest Path First (OSPF)
rip        Routing Information Protocol (RIP)
static     Static routes
(config)# router igrp ?
<1-65535> Autonomous system number

(config)# router igrp 111
(config-router)# ?
Router configuration commands:
default          Set a command to its defaults
default-information Control distribution of default information
default-metric   Set metric of redistributed routes
distance         Define an administrative distance
distribute-list  Filter networks in routing updates
exit             Exit from routing protocol configuration mode
help            Description of the interactive help system
input-queue      Specify input queue depth
maximum-paths    Forward packets over multiple paths
metric          Modify IGRP routing metrics and parameters
neighbor        Specify a neighbor router
network         Enable routing on an IP network
no              Negate a command or set its defaults
offset-list      Add or subtract offset from IGRP or RIP metrics
passive-interface Suppress routing updates on an interface
redistribute     Redistribute information from another routing
                 protocol
timers          Adjust routing timers
traffic-share    How to compute traffic share over alternate paths
validate-update-source Perform sanity checks against source address of
                 routing updates
variance        Control load balancing variance
(config-router)# network 1.2.3.0
(config-router)# neighbor 1.2.3.1
(config-router)# metric ?
holddown        Enable IGRP holddown
maximum-hops    Advertise IGRP routes greater than <hops> as unreachable
weights        Modify IGRP metric coefficients

(config-router)# metric maximum-hops ?
<1-255> Hop count
(config-router)# metric maximum-hops 10
(config-router)# timers basic 10 10 10 10

```

Cisco Switch Challenge 72

Area: Switches – IP Unicast Routing (IP Routing/OSPF)

Outline

This challenge involves enabling OSPF routing.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define OSPF.
-

The commands used are:

```
> enable
# config t
(config)# ip routing
(config)# router ospf 111
(config-router)# net 1.2.3.4 255.255.255.0 area 0
```

Example

```
> enable
# config t
(config)# ip routing

(config)# router ?
  bgp          Border Gateway Protocol (BGP)
  egp          Exterior Gateway Protocol (EGP)
  eigrp       Enhanced Interior Gateway Routing Protocol (EIGRP)
  igrp        Interior Gateway Routing Protocol (IGRP)
  isis        ISO IS-IS
  iso-igrp    IGRP for OSI networks
  mobile      Mobile routes
  odr         On Demand stub Routes
  ospf        Open Shortest Path First (OSPF)
  rip         Routing Information Protocol (RIP)
  static      Static routes

(config)# router ospf ?
  <1-65535> Process ID
(config)# router ospf 111
(config-router)# ?
Router configuration commands:
  area          OSPF area parameters
  auto-cost     Calculate OSPF interface cost according to bandwidth
  capability    Enable specific OSPF feature
  compatible    OSPF compatibility list
  default       Set a command to its defaults
  default-information Control distribution of default information
  default-metric Set metric of redistributed routes
  discard-route Enable or disable discard-route installation
  distance     Define an administrative distance
  distribute-list Filter networks in routing updates
  domain-id    OSPF domain-id
  domain-tag   OSPF domain-tag
  exit         Exit from routing protocol configuration mode
  help        Description of the interactive help system
  ignore       Do not complain about specific event
  log-adjacency-changes Log changes in adjacency state
  max-metric   Set maximum metric
  maximum-paths Forward packets over multiple paths
  neighbor     Specify a neighbor router
```

```

network          Enable routing on an IP network
no              Negate a command or set its defaults
passive-interface  Suppress routing updates on an interface
redistribute     Redistribute information from another routing protocol
router-id       router-id for this OSPF process
summary-address  Configure IP address summaries
timers          Adjust routing timers
traffic-share    How to compute traffic share over alternate paths
(config-router)# net 1.2.3.4 ?
A.B.C.D  OSPF wild card bits

(config-router)# net 1.2.3.4 255.255.255.0 ?
area  Set the OSPF area ID

(config-router)# net 1.2.3.4 255.255.255.0 a ?
<0-4294967295>  OSPF area ID as a decimal value
A.B.C.D        OSPF area ID in IP address format

(config-router)# net 1.2.3.4 255.255.255.0 a 0 ?
<cr>
(config-router)# net 1.2.3.4 255.255.255.0 area 0

```

Cisco Switch Challenge 73

Area: Switches – IP Unicast Routing (IP Routing/OSPF)

Outline

This challenge involves enabling OSPF routing and interface OSPF details.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define OSPF.
- OSPF details on an interface.

The commands used are:

```

> enable
# config t
(config)# ip routing
(config)# router ospf 111
(config-router)# net 1.2.3.4 255.255.255.0 area 0
(config)# int fa0/1
(config-if)# ip ospf cost 10
(config-if)# ip ospf dead-interval 10
(config-if)# ip ospf hello-interval 10
(config-if)# ip ospf priority 10
(config-if)# ip ospf retransmit-interval 10
(config-if)# ip ospf transmit-delay 10

```

Example

```
> enable
# config t
(config)# ip routing
(config)# router ospf 111
(config-router)# net 1.2.3.4 255.255.255.0 area 0
(config-router)# exit
(config)# int fa0/1
(config-if)# ip ospf ?
  authentication          Enable authentication
  authentication-key      Authentication password (key)
  cost                    Interface cost
  database-filter         Filter OSPF LSA during synchronization and flooding
  dead-interval           Interval after which a neighbor is declared dead
  demand-circuit         OSPF demand circuit
  hello-interval          Time between HELLO packets
  message-digest-key      Message digest authentication password (key)
  mtu-ignore              Ignores the MTU in DBD packets
  network                 Network type
  priority                Router priority
  retransmit-interval    Time between retransmitting lost link state
                        advertisements
  transmit-delay          Link state transmit delay
(config-if)# ip ospf cost ?
  <1-65535> Cost

(config-if)# ip ospf cost 10

(config-if)# ip ospf dead-interval ?
  <1-65535> Seconds

(config-if)# ip ospf dead-interval 10

(config-if)# ip ospf hello-interval ?
  <1-65535> Seconds

(config-if)# ip ospf hello-interval 10

(config-if)# ip ospf priority ?
  <0-255> Priority

(config-if)# ip ospf priority 10

(config-if)# ip ospf retransmit-interval ?
  <1-65535> Seconds

(config-if)# ip ospf retransmit-interval 10

(config-if)# ip ospf transmit-delay ?
  <1-65535> Seconds

(config-if)# ip ospf transmit-delay 10
```

Cisco Switch Challenge 74

Area: Switches – IP Unicast Routing (IP Routing/OSPF)

Outline

This challenge involves enabling OSPF routing and area details.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define OSPF.
- OSPF area details.

The commands used are:

```
> enable
# config t
(config)# ip routing
(config)# router ospf 111
(config-router)# net 1.2.3.4 255.255.255.0 area 0
(config-router)# area 1 authentication message-digest
(config-router)# area 1 authentication
(config-router)# area 1 range 192.168.1.1 255.0.0.0

(config)# int fa0/1
(config-if)# ip ospf cost 10
(config-if)# ip ospf dead-interval 10
(config-if)# ip ospf hello-interval 10
(config-if)# ip ospf priority 10
(config-if)# ip ospf retransmit-interval 10
(config-if)# ip ospf transmit-delay 10
```

Example

```
> enable
# config t
(config)# ip routing
(config)# router ospf 111
(config-router)# net 1.2.3.4 255.255.255.0 area 0
(config-router)# exit
(config)# int fa0/1
(config-if)# ip ospf ?
  authentication          Enable authentication
  authentication-key      Authentication password (key)
  cost                    Interface cost
  database-filter         Filter OSPF LSA during synchronization and flooding
  dead-interval           Interval after which a neighbor is declared dead
  demand-circuit         OSPF demand circuit
  hello-interval          Time between HELLO packets
  message-digest-key      Message digest authentication password (key)
  mtu-ignore              Ignores the MTU in DBD packets
  network                 Network type
  priority                Router priority
  retransmit-interval    Time between retransmitting lost link state
                        advertisements
  transmit-delay          Link state transmit delay
```

```

(config-router)# ar ?
<0-4294967295> OSPF area ID as a decimal value
A.B.C.D         OSPF area ID in IP address format

Switch(config-router)# ar 1 authentication ?
message-digest Use message-digest authentication
<cr>
(config-router)# area 1 authentication message-digest
(config-router)# area 1 authentication
(config-router)# ar 1 r ?
A.B.C.D IP address to match
(config-router)# area 1 range 192.168.1.1 255.0.0.0

```

Cisco Switch Challenge 75

Area: Switches – IP Unicast Routing (IP Routing/EIGRP)

Outline

This challenge involves enabling EIGRP authentication.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define EIGRP details.

The commands used are:

```

> enable
# config t
(config)# ip routing
(config)# router eigrp 111
(config-router)# eigrp log-neighbor-changes
(config-router)# network 10.0.0.0
(config-router)# exit

(config)# int fa0/1
(config-if)# int fa0/1
(config-if)# ip summary-address eigrp 100 1.2.3.0
(config-if)# ip hello-interval e 100 5
(config-if)# ip hold-time eigrp 10

```

Example

```

> enable
# config t
(config)# ip routing

(config)# router ?
bgp      Border Gateway Protocol (BGP)

```

```

    egp      Exterior Gateway Protocol (EGP)
    eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
    igrp     Interior Gateway Routing Protocol (IGRP)
    isis     ISO IS-IS
    iso-igrp IGRP for OSI networks
    mobile   Mobile routes
    odr      On Demand stub Routes
    ospf     Open Shortest Path First (OSPF)
    rip      Routing Information Protocol (RIP)
    static   Static routes
(config)# router eigrp ?
    <1-65535> Autonomous system number

(config)# router eigrp 111
(config-router)# ?
Router configuration commands:
  auto-summary      Enable automatic network number summarization
  default           Set a command to its defaults
  default-information Control distribution of default information
  default-metric    Set metric of redistributed routes
  distance          Define an administrative distance
  distribute-list   Filter networks in routing updates
  eigrp            EIGRP specific commands
  exit             Exit from routing protocol configuration mode
  help            Description of the interactive help system
  maximum-paths    Forward packets over multiple paths
  metric           Modify IGRP routing metrics and parameters
  neighbor         Specify a neighbor router
  network          Enable routing on an IP network
  no              Negate a command or set its defaults
  offset-list      Add or subtract offset from IGRP or RIP metrics
  passive-interface Suppress routing updates on an interface
  redistribute      Redistribute information from another routing protocol
  timers           Adjust routing timers
  traffic-share    How to compute traffic share over alternate paths
  variance         Control load balancing variance
(config-router)# eigrp ?
  log-neighbor-changes Enable/Disable IP-EIGRP neighbor logging
  log-neighbor-warnings Enable/Disable IP-EIGRP neighbor warnings
  router-id          router-id for this EIGRP process
  stub              Set IP-EIGRP as stubbed router
(config-router)# eigrp log-neighbor-changes
(config-router)# network 10.0.0.0
(config-router)# exit

(config)# int fa0/1
(config-if)# int fa0/1
(config-if)# ip summary-address ?
  eigrp Enhanced Interior Gateway Routing Protocol (EIGRP)
  rip   Routing Information Protocol (RIP)

(config-if)# ip summary-address eigrp ?
    <1-65535> Autonomous system number
(config-if)# ip summary-address eigrp 100 1.2.3.0
(config-if)# ip hello-interval ?
  eigrp Enhanced Interior Gateway Routing Protocol (EIGRP)

(config-if)# ip hello-interval e ?
    <1-65535> Autonomous system number
(config-if)# ip hello-interval e 100 5

(config-if)# ip hold-time ?
  eigrp Enhanced Interior Gateway Routing Protocol (EIGRP)

```

```
(config-if)# ip hold-time eigrp ?
<1-65535> Autonomous system number

(config-if)# ip hold-time eigrp 10 ?
<1-65535> Seconds before neighbor is considered down
(config-if)# ip hold-time eigrp 10
```

Cisco Switch Challenge 76

Area: Switches – IP Unicast Routing (IP Routing/BGP)

Outline

This challenge involves enabling BGP routing.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define BGP.
- BGP AS details.

The commands used are:

```
> enable
# config t
(config)# ip routing
(config)# router bgp 111
(config-router)# network 1.2.3.0
(config-router)# neighbor 1.2.3.4 remote-as 130
(config-router)# exit
(config)# int fa0/1
```

Example

```
> enable
# config t
(config)# ip routing
(config)# router bgp 111
(config-router)# ?
Router configuration commands:
  address-family      Enter Address Family command mode
  aggregate-address   Configure BGP aggregate entries
  auto-summary        Enable automatic network number summarization
  bgp                  BGP specific commands
```

```

default                Set a command to its defaults
default-information    Control distribution of default information
default-metric        Set metric of redistributed routes
distance              Define an administrative distance
distribute-list       Filter networks in routing updates
exit                  Exit from routing protocol configuration mode
help                  Description of the interactive help system
maximum-paths         Forward packets over multiple paths
neighbor              Specify a neighbor router
network               Specify a network to announce via BGP
no                    Negate a command or set its defaults
redistribute          Redistribute information from another routing protocol
synchronization       Perform IGP synchronization
table-map             Map external entry attributes into routing table
timers                Adjust routing timers

(config-router)# net ?
  A.B.C.D Network number
(config-router)# net 1.2.3.40
(config-router)# nei ?
  A.B.C.D Neighbor address
  WORD Neighbor tag
(config-router)# nei 1.2.3.4 ?
  activate            Enable the Address Family for this Neighbor
  advertise-map       specify route-map for conditional advertisement
  advertisement-interval Minimum interval between sending BGP routing updates
  allowas-in          Accept as-path with my AS present in it
  default-originate  Originate default route to this neighbor
  description         Neighbor specific description
  disable-connected-check one-hop away EBGP peer using loopback address
  distribute-list     Filter updates to/from this neighbor
  ebgp-multihop      Allow EBGP neighbors not on directly connected
                    networks
  filter-list         Establish BGP filters
  local-as            Specify a local-as number
  maximum-prefix      Maximum number of prefix accept from this peer
  next-hop-self       Disable the next hop calculation for this neighbor
  next-hop-unchanged Propagate the iBGP paths's next hop unchanged for
                    this neighbor
  password            Set a password
  peer-group          Member of the peer-group
  prefix-list         Filter updates to/from this neighbor
  remote-as           Specify a BGP neighbor
  remove-private-AS  Remove private AS number from outbound updates
  route-map           Apply route map to neighbor
  route-reflector-client Configure a neighbor as Route Reflector client
  send-community      Send Community attribute to this neighbor
  shutdown            Administratively shut down this neighbor
  soft-reconfiguration Per neighbor soft reconfiguration
  timers              BGP per neighbor timers
  translate-update    Translate Update to MBGP format
  unsuppress-map     Route-map to selectively unsuppress suppressed
                    routes
  update-source       Source of routing updates
  version             Set the BGP version to match a neighbor
  weight             Set default weight for routes from this neighbor

(config-router)# nei 1.2.3.4 remote-a ?
  <1-65535> AS of remote neighbor

(config-router)#nei 1.2.3.4 remote-as 130 ?
  <cr>

(config-router)# nei 1.2.3.4 remote-as 130

```

```
(config-router)# exit
(config)# int fa0/1
```

Cisco Switch Challenge 77

Area: Switches – IP Unicast Routing (IP Routing/BGP)

Outline

This challenge involves enabling BGP routing.

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define BGP.
- BGP neighbor details.

The commands used are:

```
> enable
# config t
(config)# ip routing
(config)# router bgp 111
(config-router)# network 1.2.3.0
(config-router)# neighbor 1.2.3.4 remote-as 130
(config-router)# neighbor 1.2.3.4 next-hop-self
(config-router)# neighbor 1.2.3.4 weight 10
(config-router)# exit
(config)# int fa0/1
```

Example

```
> enable
# config t
(config)# ip routing
(config)# router bgp 111
(config-router)# ?
Router configuration commands:
  address-family      Enter Address Family command mode
  aggregate-address   Configure BGP aggregate entries
  auto-summary        Enable automatic network number summarization
  bgp                  BGP specific commands
  default              Set a command to its defaults
  default-information Control distribution of default information
  default-metric       Set metric of redistributed routes
  distance             Define an administrative distance
  distribute-list      Filter networks in routing updates
  exit                 Exit from routing protocol configuration mode
  help                 Description of the interactive help system
```

```

maximum-paths      Forward packets over multiple paths
neighbor           Specify a neighbor router
network            Specify a network to announce via BGP
no                 Negate a command or set its defaults
redistribute        Redistribute information from another routing protocol
synchronization    Perform IGP synchronization
table-map           Map external entry attributes into routing table
timers             Adjust routing timers

(config-router)# net ?
  A.B.C.D Network number
(config-router)# net 1.2.3.40
(config-router)# nei ?
  A.B.C.D Neighbor address
  WORD Neighbor tag
(config-router)# nei 1.2.3.4 ?
  activate          Enable the Address Family for this Neighbor
  advertise-map      specify route-map for conditional advertisement
  advertisement-interval Minimum interval between sending BGP routing updates
  allowas-in         Accept as-path with my AS present in it
  default-originate Originate default route to this neighbor
  description        Neighbor specific description
  disable-connected-check one-hop away EBGP peer using loopback address
  distribute-list     Filter updates to/from this neighbor
  ebgp-multihop      Allow EBGP neighbors not on directly connected
                    networks
  filter-list        Establish BGP filters
  local-as           Specify a local-as number
  maximum-prefix      Maximum number of prefix accept from this peer
  next-hop-self       Disable the next hop calculation for this neighbor
  next-hop-unchanged Propagate the iBGP paths's next hop unchanged for
                    this neighbor
  password           Set a password
  peer-group          Member of the peer-group
  prefix-list         Filter updates to/from this neighbor
  remote-as           Specify a BGP neighbor
  remove-private-AS   Remove private AS number from outbound updates
  route-map           Apply route map to neighbor
  route-reflector-client Configure a neighbor as Route Reflector client
  send-community      Send Community attribute to this neighbor
  shutdown            Administratively shut down this neighbor
  soft-reconfiguration Per neighbor soft reconfiguration
  timers             BGP per neighbor timers
  translate-update    Translate Update to MBGP format
  unsuppress-map      Route-map to selectively unsuppress suppressed
                    routes
  update-source       Source of routing updates
  version             Set the BGP version to match a neighbor
  weight             Set default weight for routes from this neighbor

(config-router)# nei 1.2.3.4 remote-a ?
  <1-65535> AS of remote neighbor

(config-router)# nei 1.2.3.4 remote-as 130 ?
  <cr>

(config-router)# nei 1.2.3.4 remote-as 130
(config-router)# nei 1.2.3.4 next-hop-self

(config-router)# nei 1.2.3.4 w ?
  <0-65535> default weight
(config-router)# nei 1.2.3.4 weight 10

(config-router)# exit

```

```
(config)# int fa0/1
```

Cisco Switch Challenge 78

Area: Switches – IP Unicast Routing (IP Routing/BGP)

Outline

This challenge involves enabling BGP routing with a route-map

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define BGP.
- BGP neighbor details with a route-map

The commands used are:

```
> enable
# config t
(config)# ip routing
(config)# route-map TESTING permit 10
(config-route-map)# match community test
(config-route-map)# set community new
(config-route-map)# exit
(config)# router bgp 111
(config-router)# neighbor 1.2.3.4 route-map TESTING in
```

Example

```
> enable
# config t
(config)# ip routing
(config)# route-map TESTING permit 10
(config-route-map)# ?
Route Map configuration commands:
  default      Set a command to its defaults
  description  Route-map comment
  exit         Exit from route-map configuration mode
  help        Description of the interactive help system
  match       Match values from routing table
  no          Negate a command or set its defaults
  set         Set values in destination routing protocol
(config-route-map)# match ?
  as-path     Match BGP AS path list
  community   Match BGP community list
  extcommunity Match BGP/VPN extended community list
  interface   Match first hop interface of route
  ip         IP specific information
  length     Packet length
```

```

metric          Match metric of route
route-type      Match route-type of route
tag             Match tag of route
(config-route-map)# match community ?
<1-99>         Community-list number (standard)
<100-199>     Community-list number (expanded)
WORD           Community-list name
(config-route-map)# match community test

(config-route-map)# set ?
as-path        Prepend string for a BGP AS-path attribute
automatic-tag  Automatically compute TAG value
comm-list      set BGP community list (for deletion)
community      BGP community attribute
dampening      Set BGP route flap dampening parameters
default        Set default information
extcommunity   BGP extended community attribute
interface      Output interface
ip             IP specific information
level          Where to import route
local-preference BGP local preference path attribute
metric         Metric value for destination routing protocol
metric-type    Type of metric for destination routing protocol
origin         BGP origin code
tag            Tag value for destination routing protocol
traffic-index  BGP traffic classification number for accounting
weight         BGP weight for routing table
(config-route-map)# set community ?
<1-4294967295> community number
aa:nn         community number in aa:nn format
additive      Add to the existing community
internet      Internet (well-known community)
local-AS      Do not send outside local AS (well-known community)
no-advertise  Do not advertise to any peer (well-known community)
no-export     Do not export to next AS (well-known community)
none         No community attribute
<cr>
(config-route-map)# set community new
(config-route-map)# exit

(config)# router bgp 111
(config-router)# neighbor ?
A.B.C.D      Neighbor address
WORD         Neighbor tag
(config-router)# neighbor 1.2.3.4 ?
activate     Enable the Address Family for this Neighbor
advertise-map specify route-map for conditional advertisement
advertisement-interval Minimum interval between sending BGP routing updates
allowas-in   Accept as-path with my AS present in it
default-originate Originate default route to this neighbor
description  Neighbor specific description
disable-connected-check one-hop away EBGp peer using loopback address
distribute-list Filter updates to/from this neighbor
ebgp-multihop Allow EBGp neighbors not on directly connected networks
filter-list  Establish BGP filters
local-as     Specify a local-as number
maximum-prefix Maximum number of prefix accept from this peer
next-hop-self Disable the next hop calculation for this neighbor
next-hop-unchanged Propagate the iBGP paths's next hop unchanged for this neighbor
password     Set a password
peer-group   Member of the peer-group

```

prefix-list	Filter updates to/from this neighbor
remote-as	Specify a BGP neighbor
remove-private-AS	Remove private AS number from outbound updates
route-map	Apply route map to neighbor
route-reflector-client	Configure a neighbor as Route Reflector client
send-community	Send Community attribute to this neighbor
shutdown	Administratively shut down this neighbor
soft-reconfiguration	Per neighbor soft reconfiguration
timers	BGP per neighbor timers
translate-update	Translate Update to MBGP format
unsuppress-map	Route-map to selectively unsuppress suppressed routes
update-source	Source of routing updates
version	Set the BGP version to match a neighbor
weight	Set default weight for routes from this neighbor

```
(config-router)# neighbor 1.2.3.4 route-m ?
WORD Name of route map
```

```
(config-router)# neighbor 1.2.3.4 route-m TESTING
```

Cisco Switch Challenge 79

Area: Switches – IP Unicast Routing (IP Routing/BGP)

Outline

This challenge involves enabling VRF (VPN Routing Forwarding).

Objectives

The objectives of this challenge are to:

- Enable IP routing.
- Define VRF.
- Apply VRF forwarding on an interface.

The commands used are:

```
> enable
# config t
(config)# ip routing
(config)# route-map TESTING permit 10
(config)# ip vrf NEWV
(config-vrf)# input m TESTING
(config-vrf)# rd 192.168.1.1:12
(config-vrf)# exit
(config)# int fa0/1
(config-if)# ip vrf forwarding NEWV
```

Example

```

> enable
# config t
(config)# ip routing
(config)# route-map TESTING permit 10

(config)# ip vrf NEWV
(config-vrf)# ?
IP VPN Routing/Forwarding instance configuration commands:
  default      Set a command to its defaults
  description  VRF specific description
  exit         Exit from VRF configuration mode
  export       VRF export
  import       VRF import
  maximum      Set a limit
  no          Negate a command or set its defaults
  rd          Specify Route Distinguisher
  route-target Specify Target VPN Extended Communities

(config-vrf)# input ?
  map Route-map based VRF import

(config-vrf)# input m ?
  WORD VRF import route-map name

(config-vrf)# input m TESTING

(config-vrf)# rd ?
  ASN:nn or IP-address:nn VPN Route Distinguisher

(config-vrf)# rd 192.168.1.1:12 ?
  <cr>
(config-vrf)# rd 192.168.1.1:12

(config-vrf)# exit

(config)# int fa0/1

(config-if)# ip vrf ?
  forwarding Configure forwarding table
  sitemap     Configure route-map for routes received from this site

(config-if)# ip vrf forwarding ?
  WORD Table name

(config-if)# ip vrf forwarding NEWV

```

Cisco Switch Test 5 (Challenge 80)

Unit 5: Multilayer Switching

The most up-to-date version of this test is at:

<http://networksims.com/sw05.html>

Cisco Switch Challenge 81

Outline

This challenge involves the configuration hot standby (HSRP).

Objectives

The objectives of this challenge are to:

- Define the standby port.
- Define HSRP parameters.

Example

```
Switch# config t
Switch(config)# int fa0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ?
    <0-255>      group number
authentication  Authentication
delay          HSRP initialisation delay
ip            Enable HSRP and set the virtual IP address
name          Redundancy name string
preempt       Overthrow lower priority designated routers
priority      Priority level
timers        Hello and hold timers
track         Priority tracking
Switch(config-if)# standby ip ?
    A.B.C.D    Virtual IP address
    <cr>
Switch(config-if)# standby ip 192.168.128.3
Switch(config-if)# standby priority ?
    <0-255>    Priority value

Switch(config-if)# standby priority 120 ?
    preempt    Overthrow lower priority designated routers
    <cr>
Switch(config-if)# standby priority 120 preempt ?
    delay      Wait before preempting
    <cr>

Switch(config-if)# standby priority 120 preempt delay ?
    <0-3600>    Number of seconds to delay
    minimum    Delay at least this long
    sync       Wait for IP redundancy clients
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch# sh sta
FastEthernet0/1 - Group 0
    Local state is Init (interface down), priority 120, may preempt
    Preemption delayed for at least 300 secs
```

```
Hellotime 3 sec, holdtime 10 sec
Virtual IP address is 192.168.128.3 configured
Active router is unknown
Standby router is unknown
0 state changes, last state change never
IP redundancy name is "hsrp-Fa0/1-0" (default)
```

1.1 Explanation

HSRP uses an active router, a standby router, and a virtual router. The active router is the normal routing device, and the standby router listens to all the traffic going to and from the active device, as well as sending HELLO packets. If it detects a failure of the active device it takes over its IP address and MAC address, so that hosts do not notice the failure of the main device. The objective is thus to provide a consistent gateway address for the hosts.

HSRP allows the switch to provide failover for another device. To activate HSRP the **standby ip** interface configuration command is used. If there is an IP address in this command, it will be used as a standby address, otherwise it will be learned through the standby function.

Ref:

http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_guide_chapter09186a008047646d.html#wp1059790

Cisco Switch Challenge 82

Outline

This challenge involves the configuration of multiple hot standby (MHSRP).

Objectives

The objectives of this challenge are to:

- Define the standby port.
- Define MHSRP parameters.

Example

```
Switch# config t
Switch(config)# interface fa0/1
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip 10.0.0.3
```

```
Switch(config-if)# standby 1 priority 110
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

Cisco Router Challenge 209

Outline

Gateway Load Balancing Protocol (GLBP) in the same way as Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) provides an alternative route for network traffic from a failed router or circuit. It also supports load sharing between a group of redundant routers. This challenge involves the configuration of GLBP.

Objectives

The objectives of this challenge are to:

- Define GLBP details.
- Enable GLBP.

Outline

```
(config)# interface fa0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# glbp 10 authentication text testing
(config-if)# glbp 10 forwarder preempt delay minimum 60
(config-if)# glbp 10 load-balancing host-dependent
(config-if)# glbp 10 preempt delay minimum 60
(config-if)# glbp 10 priority 254
(config-if)# glbp 10 timers 5 18
(config-if)# glbp 10 ip 192.168.0.2
```

Example

```
(config)# interface fa0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# glbp ?
  <0-1023>  Group number

(config-if)# glbp 10 ?
  authentication  Authentication method
  forwarder      Forwarder configuration
  ip             Enable group and set virtual IP address
  load-balancing Load balancing method
  name          Redundancy name
  preempt       Overthrow lower priority designated routers
  priority      Priority level
  timers        Adjust GLBP timers
  weighting     Gateway weighting and tracking
```

```

(config-if)# glbp 10 authentication ?
md5    MD5 authentication
text   Plain text authentication

(config-if)# glbp 10 authentication text ?
WORD   Text authentication string

(config-if)# glbp 10 authentication text testing
(config-if)# gl 10 forwarder ?
preempt Overthrow lower priority active forwarders

(config-if)# gl 10 forwarder preempt ?
delay  Wait before preempting
<cr>

(config-if)# gl 10 forwarder preempt delay ?
minimum Delay at least this long

(config-if) glbp 10 forwarder preempt delay minimum ?
<0-3600> Number of seconds for minimum delay
(config-if)# glbp 10 forwarder preempt delay minimum 60
(config-if)# glbp 10 load-balancing ?
host-dependent Load balance equally, source MAC determines forwarder choice
round-robin    Load balance equally using each forwarder in turn
weighted      Load balance in proportion to forwarder weighting
(config-if)# glbp 10 load-balancing host-dependent
(config-if)# glbp 10 pre ?
delay  Wait before preempting
<cr>
(config-if)# glbp 10 preempt delay minimum 60
(config-if)# glbp 10 pri ?
<1-255> Priority value
(config-if)# glbp 10 priority 254
(config-if)# glbp 10 timers ?
<1-60>   Hello interval in seconds
msec    Specify hello interval in milliseconds
redirect Specify time-out values for failed forwarders
(config-if)# glbp 10 timers 5 18
(config-if)# glbp 10 ip ?
A.B.C.D Virtual IP address
(config-if)# glbp 10 ip 192.168.0.2

```

glbp 10 authentication text testing	This command authenticates GLBP packets received from the group of routers.
glbp 10 forwarder preempt delay minimum 60	This command allows the router to take over as AVF (Active Virtual Forwarder) within a GLBP group, if it has a higher priority than the current AVF.
glbp 10 load-balancing host-dependent	This command specifies the load balancing method such as: host-dependent, round-robin or weighted.
glbp 10 preempt delay minimum 60	This command allows the router to take over as AVG (Active Virtual Gateway) with a GLBP group, if it has a higher priority than the current AVG.
glbp 10 priority 254	This command sets up the priority level of

	the gateway within a GLBP group.
<code>glbp 10 timers 5 18</code>	This command configures the interval between hello packets sent by the AVG within the GLBP group. The parameters include the holdtime which specifies time before the virtual gateway and virtual forwarder information is considered invalid.
<code>glbp 10 ip 192.168.0.2</code>	Enable GLBP and define a virtual interface address.

Cisco Router Challenge 210

Outline

Virtual Router Redundancy Protocol (VRRP) in the same way as Hot Standby Router Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP). It provides an alternative route for network traffic from a failed router or circuit.. This challenge involves the configuration of VRRF.

Objectives

The objectives of this challenge are to:

- Define VRRF details.
- Enable VRRF.

Outline

```
(config)# interface fa0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# vrrp 10 description text
(config-if)# vrrp 10 priority level
(config-if)# vrrp 10 preempt delay minimum 10
(config-if)# vrrp group timers learn
(config-if)# vrrp IP 192.168.0.2
```

Example

```
(config)# interface fa0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# vrrp 10 description text
(config-if)# vrrp 10 priority level
(config-if)# vrrp 10 preempt delay minimum 10
(config-if)# vrrp group timers learn
(config-if)# vrrp IP 192.168.0.2
```

Cisco Switch Test 6

Unit 6: Availability and Redundancy

The most up-to-date version of this test is at:

<http://networksims.com/sw06.html>