

# CCNP BCMSN Part 2

## Cisco Switch Challenge 84

### Outline

This challenge involves the setting up multicast routing.

### Objectives

The objectives of this challenge are to:

- Enable multicasting routing.
- Define that the interface port should be defined as a **Layer 3 port** (using **no switchport**).
- Define PIM parameters on an interface port.

### Example

```
> enable
```

```
Switch# config t
Switch(config)# ip multicast
Switch(config)# int fa0/1
Switch(config-if)# no switchport
Switch(config-if)# ip pim ?
  bsr-border      Border of PIM domain
  dense-mode      Enable PIM dense-mode operation
  nbma-mode        Use Non-Broadcast Multi-Access (NBMA) mode on interface
  neighbor-filter PIM peering filter
  query-interval  PIM router query interval
  sparse-dense-mode Enable PIM sparse-dense-mode operation
  sparse-mode      Enable PIM sparse-mode operation
  version          PIM version
<cr>
Switch(config-if)# ip pim version ?
  <1-2> version number
Switch(config-if)# ip pim version 2

Switch(config-if)# ip pim dense-mode ?
  proxy-register Send proxy registers
<cr>
Switch(config-if)# ip pim dense-mode
Switch(config-if)# ip pim bsr-border
```

Note: You will not see the **ip pim** command on an interface unless it is defined as a Layer 3 port.

# Cisco Switch Challenge 85

## Outline

This challenge involves manually defining a rendezvous point (RP) for a multicast group.

## Objectives

The objectives of this challenge are to:

- Enable multicasting routing.
- Define an RP.

## Example

```
> enable
```

```
Switch# config t
Switch(config)# ip multicast
Switch(config)# access-list 1 permit 224.1.1.1 0.0.0.0
Switch(config)# ip pim ?
  accept-register      Registers accept filter
  accept-rp           RP accept filter
  autorp              Configure AutoRP global operations
  bsr-candidate       Candidate bootstrap router (candidate BSR)
  register-rate-limit Rate limit for PIM data registers
  rp-address          PIM RP-address (Rendezvous Point)
  rp-announce-filter  Auto-RP announce message filter
  rp-candidate        To be a PIMv2 RP candidate
  send-rp-announce    Auto-RP send RP announcement
  send-rp-discovery   Auto-RP send RP discovery message (as RP-mapping agent)
  spt-threshold       Source-tree switching threshold
  ssm                 Configure Source Specific Multicast
Switch(config)# ip pim rp-address ?
  A.B.C.D IP address of Rendezvous-point for group

Switch(config)# ip pim rp-address 1.2.3.4 ?
  <1-99>      Access-list reference for group
  <1300-1999> Access-list reference for group (expanded range)
  WORD       IP Named Standard Access list
  override   Overrides Auto RP messages
  <cr>
Switch(config)# ip pim rp-address 1.2.3.4 1
```

# Cisco Switch Challenge 86

## Outline

This challenge involves auto-RP for an existing sparse-mode cloud in mulitcast routing.

## Objectives

The objectives of this challenge are to:

- Enable multicasting routing.
- Define an auto-RP.

## Example

```
> enable
```

```
Switch# config t
```

```
Switch(config)# ip multicast
```

```
Switch(config)# access-list 5 permit 224.1.1.1 0.0.0.0
```

```
Switch(config)# ip pim ?
```

```
accept-register    Registers accept filter
accept-rp          RP accept filter
autorp             Configure AutoRP global operations
bsr-candidate      Candidate bootstrap router (candidate BSR)
register-rate-limit Rate limit for PIM data registers
rp-address         PIM RP-address (Rendezvous Point)
rp-announce-filter Auto-RP announce message filter
rp-candidate       To be a PIMv2 RP candidate
send-rp-announce   Auto-RP send RP announcement
send-rp-discovery  Auto-RP send RP discovery message (as RP-mapping agent)
spt-threshold      Source-tree switching threshold
ssm               Configure Source Specific Multicast
```

```
Switch(config)# ip pi send-rp-announce ?
```

```
Async             Async interface
BVI               Bridge-Group Virtual Interface
Dialer            Dialer interface
FastEthernet      FastEthernet IEEE 802.3
GigabitEthernet  GigabitEthernet IEEE 802.3z
Lex              Lex interface
Loopback         Loopback interface
Multilink        Multilink-group interface
Null             Null interface
Port-channel     Ethernet Channel of interfaces
Tunnel           Tunnel interface
Virtual-Template  Virtual Template interface
Virtual-TokenRing Virtual TokenRing
Vlan             Catalyst Vlans
```

```
Switch(config)# ip pim send-rp-announce fa0/1 ?
```

```
Switch(config)# ip pim send-rp-announce fa0/1 ?
```

```
scope RP announcement scope
```

```
Switch(config)# ip pim send-rp-announce fa0/1 scope ?
```

```
<1-255> TTL of the RP announce packet
```

```
Switch(config)# ip pim send-rp-announce fa0/1 scope 30 ?
```

```
group-list Group access-list
interval   RP announcement interval
<cr>
```

```
Switch(config)# ip pim send-rp-announce fa0/1 scope 30 group-list ?
```

```
<1-99> Access-list reference for multicast groups
```

```

WORD      IP Named Standard Access list

Switch(config)# ip pim send-rp-announce fa0/1 scope 30 group-list 5 ?
interval  RP announcement interval
<cr>

Switch(config)# ip pim send-rp-announce fa0/1 scope 30 group-list 5
Switch(config)# ip pim accept-rp ?
A.B.C.D  IP address of RP for group
auto-rp  only RP-mapping from Auto-RP
Switch(config)# ip pim accept-rp 1.2.3.4 ?
<1-99>   Access-list reference for group
<1300-1999> Access-list reference for group (expanded range)
WORD     IP Named Standard Access list
<cr>

Switch(config)# ip pim accept-rp 1.2.3.4 5
Switch(config)# int fa0/1
Switch(config-if)# no switchport

```

# Cisco Switch Challenge 87

## Outline

This challenge involves preventing candidate RP spoofing.

## Objectives

The objectives of this challenge are to:

- Enable multicasting routing.
- Define an auto-RP.

## Example

```

> enable

Switch# config t
Switch(config)# ip multicast
Switch(config)# access-list 5 permit 224.1.1.1 0.0.0.0
Switch(config)# access-list 6 permit 19.10.11.12

Switch(config)# ip pim rp-announce-filter ?
group-list  Group address access-list
rp-list     RP address access-list

Switch(config)# ip pim rp-announce-filter rp-list ?
<1-99>     Access-list reference for RP
WORD      IP Named Standard Access list

Switch(config)# ip pim rp-announce-filter rp-list 6 ?
group-list  Group address access-list
<cr>

Switch(config)# ip pim rp-announce-filter rp-list 6 group-list ?

```

```
<1-99> Access-list reference for group
WORD      IP Named Standard Access list
Switch(config)# ip pim rp-announce-filter rp-list 6 group-list 5
```

# Cisco Switch Challenge 88

**Area:** Switches – IP Multicast (PIM)

## Outline

IP Multicast can use several different types of protocols, such as PIM, DVMRP, IGRP and CGMP. This tutorial outlines the configuration of PIM.

## Objectives

The objectives of this challenge are to:

- Define PIM.

The commands used are:

```
# config t
(config)# int fa0/1
(config-if)# no switchport
(config-if)# ip pim version 2
(config-if)# ip pim dense-mode
(config-if)# ip pim bsr-border
(config-if)# ip multicast boundary 11
(config-if)# exit

(config)# access-list 10 permit 220.1.1.1 0.0.0.0
(config)# access-list 11 deny 220.1.1.1 0.0.0.0

(config)# ip pim rp-address 192.168.1.1 10
(config)# ip pim send-rp-announce fa0/1 scope 30 group-list 5
(config)# ip pim accept-rp 1.2.3.4 10
(config)# ip pim send-rp-discovery scope 10
(config)# ip pim rp-announce-filter rp-list 2 group-list 1
```

## Example

```
# config t
(config)# int fa0/1
(config-if)# no switchport
(config-if)# ip pim ?
  bsr-border      Border of PIM domain
  dense-mode      Enable PIM dense-mode operation
  nbma-mode        Use Non-Broadcast Multi-Access (NBMA) mode on interface
  neighbor-filter PIM peering filter
  query-interval  PIM router query interval
  sparse-dense-mode Enable PIM sparse-dense-mode operation
  sparse-mode      Enable PIM sparse-mode operation
  version          PIM version
```

```

<cr>
(config-if)# ip pim sparse-mode

(config-if)# ip pim version ?
<1-2> version number

(config-if)# ip pim version 2

(config-if)# ip pim bsr-border

(config-if)# ip multicast ?
boundary          Boundary for administratively scoped multicast addresses
helper-map        Broadcast to Multicast map OR Multicast to Broadcast map
rate-limit        Rate limit multicast data packets
ttl-threshold     TTL threshold for multicast packets

(config-if)# ip multicast boundary ?
<1-99>            Access-list number
<1300-1999>      <access-list> (expanded range)
WORD              IP Named Standard Access list

(config-if)# ip multicast boundary 10

(config-if)# exit

(config)# access-list 10 permit 220.1.1.1 0.0.0.0

(config)# ip pim ?
accept-register   Registers accept filter
accept-rp         RP accept filter
autorp            Configure AutoRP global operations
bsr-candidate     Candidate bootstrap router (candidate BSR)
register-rate-limit Rate limit for PIM data registers
rp-address        PIM RP-address (Rendezvous Point)
rp-announce-filter Auto-RP announce message filter
rp-candidate      To be a PIMv2 RP candidate
send-rp-announce  Auto-RP send RP announcement
send-rp-discovery Auto-RP send RP discovery message (as RP-mapping agent)
spt-threshold     Source-tree switching threshold
ssm               Configure Source Specific Multicast

(config)# ip pim rp-address ?
A.B.C.D          IP address of Rendezvous-point for group

(config)# ip pim rp-address 192.168.1.1 ?
<1-99>           Access-list reference for group
<1300-1999>     Access-list reference for group (expanded range)
WORD            IP Named Standard Access list
override        Overrides Auto RP messages
<cr>

(config)# ip pim rp-address 192.168.1.1 10

(config)# ip pim send-rp-announce fa0/1 ?
(config)# ip pim send-rp-announce fa0/1 ?
scope          RP announcement scope

(config)# ip pim send-rp-announce fa0/1 scope ?
<1-255>       TTL of the RP announce packet

(config)# ip pim send-rp-announce fa0/1 scope 30 ?
group-list     Group access-list

```

```

interval    RP announcement interval
<cr>

(config)# ip pim send-rp-announce fa0/1 scope 30 group-list ?
<1-99>      Access-list reference for multicast groups
WORD       IP Named Standard Access list

(config)# ip pim send-rp-announce fa0/1 scope 30 group-list 5 ?
interval    RP announcement interval
<cr>

(config)# ip pim send-rp-announce fa0/1 scope 30 group-list 5

(config)# ip pim accept-rp ?
A.B.C.D     IP address of RP for group
auto-rp     only RP-mapping from Auto-RP
(config)# ip pim accept-rp 1.2.3.4 ?
<1-99>      Access-list reference for group
<1300-1999> Access-list reference for group (expanded range)
WORD       IP Named Standard Access list
<cr>

(config)# ip pim accept-rp 1.2.3.4 10

(config)# ip pim send-rp-discovery ?
Async       Async interface
BVI         Bridge-Group Virtual Interface
Dialer      Dialer interface
FastEthernet FastEthernet IEEE 802.3
GigabitEthernet GigabitEthernet IEEE 802.3z
Lex         Lex interface
Loopback    Loopback interface
Multilink   Multilink-group interface
Null        Null interface
Port-channel Ethernet Channel of interfaces
Tunnel      Tunnel interface
Virtual-Template Virtual Template interface
Virtual-TokenRing Virtual TokenRing
Vlan        Catalyst Vlans
scope       Scope of the RP discovery packets

(config)# ip pi send-rp-d s ?
<1-255>     TTL

(config)# ip pi send-rp-d scope 10

(config)# ip pim rp-ann ?
group-list  Group address access-list
rp-list     RP address access-list

(config)# ip pim rp-ann rp- ?
<1-99>      Access-list reference for RP
WORD       IP Named Standard Access list

(config)# ip pim rp-ann rp- 10 ?
group-list  Group address access-list
<cr>

(config)# ip pim rp-ann rp- 10 gr ?
<1-99>      Access-list reference for group
WORD       IP Named Standard Access list

```

```
(config)# ip pim rp-announce-filter rp-list 10 group-list 1
```

# Cisco Switch Challenge 89

Area: Switches – IGMP

## Outline

This challenge defines some IGMP parameters on interfaces.

## Objectives

The objectives of this challenge are to:

- Define IGMP.

The commands used are:

```
# config t
(config)# int fa0/1
(config-if)# no switchport
(config-if)# ip igmp join-group 224.0.0.1
(config-if)# ip igmp querier-timeout 10
(config-if)# ip igmp query-interval 10
(config-if)# ip igmp query-max-response-time 10
(config-if)# ip igmp version 2
```

## Notes

```
# config t
(config)# int fa0/1
(config-if)# no switchport

(config-if)# ip igmp ?
  access-group          IGMP group access group
  helper-address        IGMP helper address
  immediate-leave       Leave groups immediately without sending last
                        member query, use for one host network only
  join-group            IGMP join multicast group
  last-member-query-interval IGMP last member query interval
  querier-timeout       IGMP previous querier timeout
  query-interval        IGMP host query interval
  query-max-response-time IGMP max query response value
  static-group          IGMP static multicast group
  tcn                   IGMP TCN configuration
  unidirectional-link  IGMP unidirectional link multicast routing
  v3lite               Enable/Disable IGMPv3 Lite
  version               IGMP version

(config-if)# ip igmp jo ?
  A.B.C.D IP group address
```

```

(config-if)# ip igmp jo 224.0.0.1

(config-if)# ip igmp querier- ?
    <60-300>  timeout value in seconds

(config-if)# ip igmp querier- 10

(config-if)# ip igmp query-m ?
    <1-25>  query response value in seconds

(config-if)# ip igmp query-m 10

(config-if)# ip igmp ve ?
    <1-3>  version number

(config-if)# ip igmp ve 2

```

# Cisco Switch Challenge 90

**Area:** Switches – IGMP: Controlling access to IP Multicast Groups

## Outline

This challenge defines a mulitcast ACL, and restricts IP Multicast.

## Objectives

The objectives of this challenge are to:

- Define IGMP restriction.

The commands used are:

```

# config t
(config)# access-list 101 deny host 225.5.5.5 0.0.0.0
(config)# access-list 101 permit any any
(config)# int fa0/1
(config-if)# no switchport
(config-if)# ip igmp access-group 101
(config-if)# ip igmp join-group 224.0.0.1
(config-if)# ip igmp querier-timeout 10
(config-if)# ip igmp query-interval 10
(config-if)# ip igmp query-max-response-time 10
(config-if)# ip igmp version 2

```

## Notes

```

# config t
(config)# access-list 101 deny host 225.5.5.5 0.0.0.0
(config)# access-list 101 permit any any

(config)# int fa0/1
(config-if)# no switchport

```

```
(config-if)# ip igmp ?
access-group          IGMP group access group
helper-address        IGMP helper address
immediate-leave       Leave groups immediately without sending last
                      member query, use for one host network only

join-group            IGMP join multicast group
last-member-query-interval IGMP last member query interval
querier-timeout       IGMP previous querier timeout
query-interval        IGMP host query interval
query-max-response-time IGMP max query response value
static-group          IGMP static multicast group
tcn                   IGMP TCN configuration
unidirectional-link   IGMP unidirectional link multicast routing
v3lite                Enable/Disable IGMPv3 Lite
version               IGMP version
```

```
(config-if)# ip igmp access-group 101
(config-if)# ip igmp join-group 224.0.0.1
(config-if)# ip igmp querier-timeout 10
(config-if)# ip igmp query-interval 10
(config-if)# ip igmp query-max-response-time 10
(config-if)# ip igmp version 2
```

# Cisco Switch Challenge 91

**Area:** Switches – CGMP

## Outline

This challenge defines setting up a CGMP server on the switch.

## Objectives

The objectives of this challenge are to:

- Define CGMP servers.

The commands used are:

```
# config t
(config)# int fa0/1
(config-if)# no switchport
(config-if)# ip cgmp
(config)# int fa0/2
(config-if)# no switchport
(config-if)# ip cgmp proxy
(config)# int fa0/3
(config-if)# no switchport
(config-if)# ip cgmp router-only
```

## Notes

```
# config t
```

```

(config)# int fa0/1
(config-if)# no switchport
(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
  unreachable Enable sending ICMP Unreachable messages
  urd        Configure URL Rendezvousing
  vrf       VPN Routing/Forwarding parameters on the interface
  wccp     WCCP interface commands
(config-if)# ip cgmp ?
  proxy      CGMP for hosts and proxy for multicast routers
  router-only CGMP proxy for multicast routers only
  <cr>
(config-if)# ip cgmp
(config)# int fa0/2
(config-if)# no switchport
(config-if)# ip cgmp proxy
(config)# int fa0/3
(config-if)# no switchport
(config-if)# ip cgmp router-only

```

## Cisco Switch Challenge 92

## Outline

This challenge involves the using IGMP snooping.

## Objectives

The objectives of this challenge are to:

- Defines VLANs.
- Enable IGMP snooping.

## Example

```
> en
```

```
(vlan)# vlan database
```

```
(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 ?
```

```
<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)
  <cr>
```

```
(vlan)# vlan 1 name ?
```

```
  WORD The ascii name for the VLAN
```

```
(vlan)# vlan 1 name edinburgh
```

```
(vlan)# vlan 2 name glasgow
```

```

(vlan)# exit
# config t
(config)# ip igmp snooping ?
(config)# ip igmp snooping vlan 1 immediate-leave
(config)# ip igmp snooping vlan 2 immediate-leave
(config)# exit
# show ip igmp snoop
Global IGMP Snooping configuration:
-----
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2

Vlan 1:
-----
IGMP snooping                : Enabled
Immediate leave              : Enabled
Multicast router learning mode : pim-dvmrp
Source only learning age timer : 10
CGMP interoperability mode    : IGMP_ONLY

```

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# sh env ?  
  all          Show all environment status  
  fan          Show fan status  
  power        Show power supply status  
  rps          Show RPS status  
  temperature  Show temperature status
```

```
Switch# sh env all  
FAN is OK  
TEMPERATURE is OK  
POWER is OK  
RPS is NOT PRESENT
```

```
Switch# sh env fan  
FAN is OK
```

```
Switch# sh env p  
POWER is OK
```

```
Switch# sh env r  
RPS is NOT PRESENT
```

```
Switch# sh env t  
TEMPERATURE is OK
```

## Cisco Switch Test 7 (Challenge 93)

### Unit 7: Multicast

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

<http://networksims.com/sw07.html>

## Cisco Switch Challenge 94

### Outline

This challenge involves the configuration of QoS.

### Objectives

The objectives of this challenge are to:

- Define interesting traffic with an ACL.
- Define QoS parameters.

## Example

```
> en
# config t
(config)# access-list 108 permit ip 162.78.102.0 0.0.255.255 247.226.90.0
0.0.255.255
(config)# class-map tayside
(config-cmap)# ?
QoS class-map configuration commands:
  description  Class-Map description
  exit         Exit from QoS class-map configuration mode
  match       classification criteria
  no          Negate or set default values of a command
  rename      Rename this class-map
(config-cmap)# match ?
  access-group  Access group
  any           Any packets
  class-map     Class map
  destination-address  Destination address
  input-interface  Select an input interface to match
  ip           IP specific values
  mpls        Multi Protocol Label Switching specific values
  not         Negate this match result
  protocol    Protocol
  source-address  Source address
  vlan       VLANs to match
(config-cmap)# match ac ?
  <1-2699>  Access list index
  name     Named Access List
(config-cmap)# match access-group 108
(config-cmap)# exit
(config)# policy-map ankle
(config-pmap)# ?
QoS policy-map configuration commands:
  class      policy criteria
  description  Policy-Map description
  exit      Exit from QoS policy-map configuration mode
  no       Negate or set default values of a command
  rename   Rename this policy-map
(config-pmap-c)# class tayside
(config-pmap-c)# ?
QoS policy-map class configuration commands:
  bandwidth  Bandwidth
  exit      Exit from QoS class action configuration mode
  no       Negate or set default values of a command
  trust    Set trust value for the class
  <cr>
  police   Police
  set     Set QoS values
(config-pmap-c)# bandwidth 128
(config-pmap-c)# queue-limit 21
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int fa0/1
(config-if)# service-policy ?
  history  Keep history of QoS metrics
```

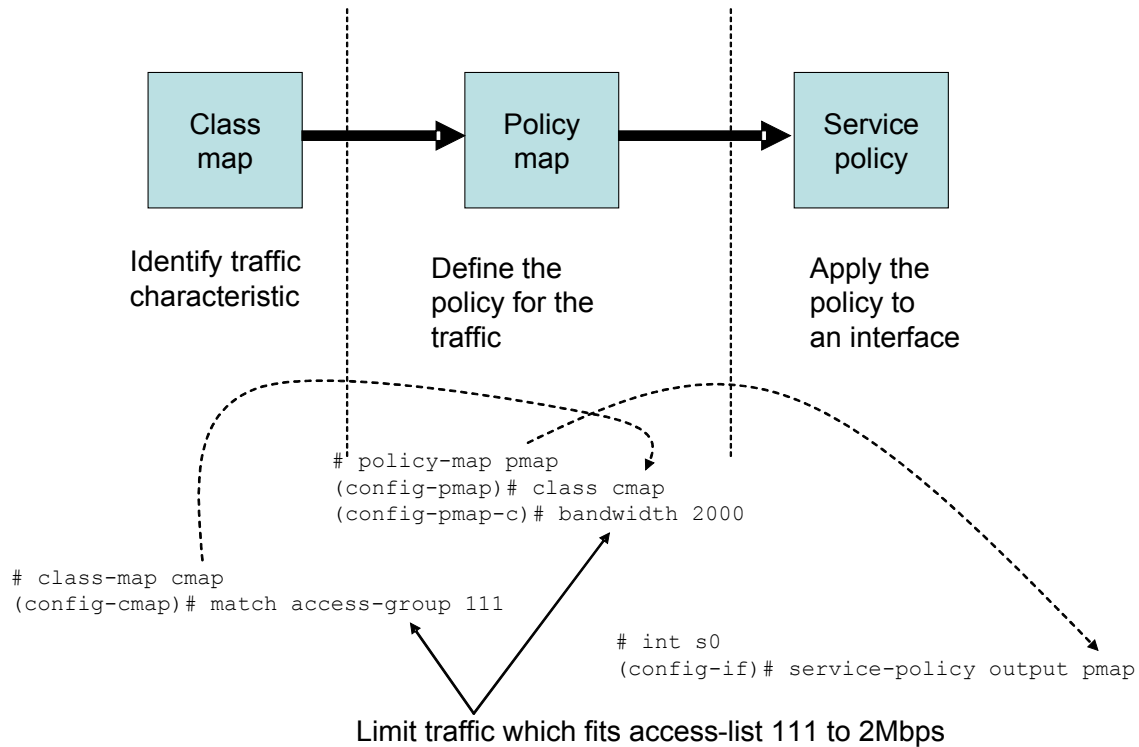
```

input    Assign policy-map to the input of an interface
output   Assign policy-map to the output of an interface
Switch(config-if)# se o ?
WORD    policy-map name
(config-if)# service-policy output ankle

```

### Explanation

The following shows an example of limiting all the traffic which fits access-list 111 to 2Mbps:



### Ref:

<http://www.netcraftsmen.net/welcher/papers/newqos121.html>

# Cisco Switch Challenge 95

### Outline

This challenge involves the configuration of Weighted RR (WRR).

> CCNP ONT Area: Unit 4: Congestion Management and Queuing

### Objectives

The objectives of this challenge are to:

- Enable QoS globally (mls qos).
- Define Layer 3 operation (no switchport).
- Define WRR.

### Example

```
(config)# mls qos
(config)# int fa0/1
(config-if)# no switchport
(config-if)# mls ?
    qos    qos command keyword
(config-if)# mls qos ?
    cos          Configure interface COS parameters
    dscp-mutation Apply DSCP-DSCP map to DSCP trusted port
    monitor      Collect QoS statistics
    trust        Configure trust state of interface
(config-if)# mls qos trust ?
    cos          Classify by packet COS
    device       trusted device class
    dscp         Classify by packet DSCP
    ip-precedence Classify by packet IP precedence
    <cr>
(config-if)# mls qos trust cos
(config-if)# priority-queue ?
    out    egress priority queue
(config-if)# priority-queue out

(config-if)# wrr-queue ?
    bandwidth    Configure WRR bandwidth
    cos-map      Configure cos-map for a queue id
    min-reserve  Configure min-reserve level

(config-if)# wrr-queue bandwidth ?
    <1-65536>   enter bandwidth weight for qid 1

(config-if)# wrr-queue bandwidth 3 ?
    <1-65536>   enter bandwidth weight for qid 2
(config-if)# wrr-queue bandwidth 3 8 ?
    <1-65536>   enter bandwidth weight for qid 3
(config-if)# wrr-queue bandwidth 3 8 10 ?
    <1-65536>   enter bandwidth weight for qid 4
(config-if)# wrr-queue bandwidth 3 8 10 12
```

In this case the bandwidth is:

Queue 1:  $3/(3+8+10+12) = 9.1\%$

Queue 2:  $3/(3+8+10+12) = 24.2\%$

Queue 3:  $3/(3+8+10+12) = 30.3\%$

Queue 4:  $3/(3+8+10+12) = 36.4\%$

```
(config-if)# wrr-queue cos-map ?
<1-4> enter cos-map queue id
(config-if)# wrr-queue cos-map 1 ?
<0-7> 8 cos values separated by spaces
(config-if)# wrr-queue cos-map 3 4 5

(config-if)# wrr-queue cos-map 1 0 1 2 4
(config-if)# wrr-queue cos-map 3 4 5
```

Queue 1 has CoS of 0, 1, 2 and 4 allocated to it  
Queue 3 has CoS of 4 and 5 allocated to it.

```
(config-if)# wrr-queue random-detect 1 max-threshold 50 100
(config-if)# wrr-queue random-detect 3 max-threshold 80 100
```

Queue 1 has a min threshold of 50% and a max of 100%  
Queue 3 has a min threshold of 80% and a max of 100%

## Cisco Switch Challenge 126

### Outline

This challenge involves the configuration of a priority queue (PQ) which has four queues: high, medium, normal and low.

### Objectives

The objectives of this challenge are to:

- Define queue limits
- Define protocols to go into queues.
- Apply PQ.

### Overview

```
(config)# priority-list 1 q 20 40 60 80
(config)# priority-list 1 protocol http high
(config)# priority-list 1 protocol ipx low
(config)# int fa0/1
(config-if)# priority-group 1
```

### Example

```
(config)# priority-list ?
<1-16> Priority list number
(config)# priority-list 1 ?
default      Set priority queue for unspecified datagrams
interface    Establish priorities for packets from a named interface
```

```

protocol      priority queueing by protocol
queue-limit  Set queue limits for priority queues
(config)# priority-list 1 q ?
<0-32767> High limit
(config)# priority-list 1 q 20 ?
<0-32767> Medium limit
(config)# priority-list 1 q 20 40 ?
<0-32767> Normal limit
(config)# priority-list 1 q 20 40 60 ?
<0-32767> Lower limit
(config)# priority-list 1 q 20 40 60 80 ?
<cr>
(config)# priority-list 1 q 20 40 60 80
(config)# prio 1 p ?
  aarp          AppleTalk ARP
  appletalk     AppleTalk
  arp           IP ARP
  bridge        Bridging
  bstun         Block Serial Tunnel
  cdp           Cisco Discovery Protocol
  clns          ISO CLNS
  clns_es       ISO CLNS End System
  clns_is       ISO CLNS Intermediate System
  cmns          ISO CMNS
  compressedtcp Compressed TCP (VJ)
  decnet        DECnet
  decnet_node   DECnet Node
  decnet_router-11 DECnet Router L1
  decnet_router-12 DECnet Router L2
  dlsw          Data Link Switching (Direct encapsulation only)
  http          HTTP
  ip            IP
  ipv6          IPV6
  ipx           Novell IPX
  llc2          llc2
  pad           PAD links
  pppoe         PPP over Ethernet
  qllc          qllc protocol
  rsrp          Remote Source-Route Bridging
  snapshot      Snapshot routing support
  stun          Serial Tunnel

(config)# priority-list 1 protocol http ?
  high
  medium
  normal
  low
(config)# priority-list 1 protocol http high
(config)# priority-list 1 protocol ipx low
(config)# int fa0/1
(config-if)# priority-group 1

```

# Cisco Switch Challenge 127

## Outline

This challenge involves the configuration of a custom queue (CQ). Up to 16 queues can be configured.

## Objectives

The objectives of this challenge are to:

- Define queues.
- Apply CQ.

## Overview

```
(config)# queue-list 1 protocol ip 1 tcp www
(config)# queue-list 1 protocol ip 2 udp rip
(config)# queue-list 1 protocol ip 3
(config)# queue-list 1 queue 1 limit 40
(config)# queue-list 1 queue 2 limit 40
(config)# queue-list 1 queue 3 limit 80
(config)# int vlan1
(config-if)# custom-queue-list 1
```

## Example

```
(config)# queue-list ?
<1-16> Queue list number
```

```
(config)# queue-list 1 ?
default          Set custom queue for unspecified datagrams
interface        Establish priorities for packets from a named interface
lowest-custom    Set lowest number of queue to be treated as custom
protocol         priority queueing by protocol
queue           Configure parameters for a particular queue
stun            Establish priorities for stun packets
```

```
Switch(config)#queue-list 1 protocol ?
arp             IP ARP
bridge         Bridging
cdp            Cisco Discovery Protocol
compressedtcp  Compressed TCP
ip             IP
```

```
Switch(config)# queue-list 1 protocol ip ?
<0-16> queue number
```

```
Switch(config)# queue-list 1 protocol ip 1 ?
fragments      Prioritize fragmented IP packets
```

```

gt          Classify packets greater than a specified size
list        To specify an access list
lt          Classify packets less than a specified size
tcp         Prioritize TCP packets 'to' or 'from' the specified port
udp         Prioritize UDP packets 'to' or 'from' the specified port
(config)# queue-list 1 protocol ip 1

```

```

(config)# queue-list 1 protocol ip 1 tcp ?
<0-65535>   Port number
bgp          Border Gateway Protocol (179)
chargen      Character generator (19)
cmd          Remote commands (rcmd, 514)
daytime      Daytime (13)
discard      Discard (9)
domain       Domain Name Service (53)
echo         Echo (7)
exec         Exec (rsh, 512)
finger       Finger (79)
ftp          File Transfer Protocol (21)
ftp-data     FTP data connections (used infrequently, 20)
gopher       Gopher (70)
hostname     NIC hostname server (101)
ident        Ident Protocol (113)
irc          Internet Relay Chat (194)
klogin       Kerberos login (543)
kshell       Kerberos shell (544)
login        Login (rlogin, 513)
lpd          Printer service (515)
nntp         Network News Transport Protocol (119)
pim-auto-rp  PIM Auto-RP (496)
pop2         Post Office Protocol v2 (109)
pop3         Post Office Protocol v3 (110)
smtp         Simple Mail Transport Protocol (25)
sunrpc       Sun Remote Procedure Call (111)
syslog       Syslog (514)
tacacs       TAC Access Control System (49)
talk         Talk (517)
telnet       Telnet (23)
time         Time (37)
uucp         Unix-to-Unix Copy Program (540)
whois        Nicname (43)
www          World Wide Web (HTTP, 80)

```

```

(config)# queue-list 1 protocol ip 2 tcp www

```

```

(config)# queue-list 1 protocol ip 1 u ?
<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)
(config)# que 1 queue ?
<0-16> queue number

(config)# que 1 q 1 ?
byte-count     Specify size in bytes of a particular queue
limit          Set queue entry limit of a particular queue

(config)# que 1 q 1 limit ?
<0-32767> number of queue entries

(config)# que 1 q 1 l 40 ?
byte-count     Specify size in bytes of a particular queue
<cr>

(config)# que 1 q 1 l 40
(config)# int vlan 1
(config-if)# custom-queue-list ?
<1-16> Custom queue list number
(config-if)# custom-queue-list 1

```

# Cisco Switch Challenge 96

## Outline

This challenge involves configuring Auto QoS on a switch.

## Objectives

The objectives of this challenge are to:

- Define Auto QoS

## Example

```

> en
# config t
(config)# cdp run

(config)# int vlan 10

(config)# int vlan 10
(config-vlan)# exit
(config)# int vlan 20
(config-vlan)# exit

(config)# int fa0/1
(config-if)# cdp enable
(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 10
(config-if)# switchport voice ?
  vlan           Vlan for voice traffic

(config-if)# switchport voice vlan ?
  <1-4094>       Vlan for voice traffic
  dot1p         Priority tagged on PVID
  none          Don't tell telephone about voice vlan
  untagged      Untagged on PVID
(config-if)# switchport voice vlan 20
(config-if)# au ?
  qos           Configure AutoQoS

(config-if)# auto qos ?
  voip          Configure AutoQoS for VoIP

(config-if)# auto qos voip ?
  cisco-phone   Trust the QoS marking of Cisco IP Phone
  trust         Trust the COS marking

```

```
(config-if)# auto qos voip cisco-phone
(config-if)# exit
```

Note:

For Auto QoS VoIP, CDP needs to be enabled.

## Cisco Switch Challenge 97

**Area:** Switches – Voice VLAN

### Outline

This challenge involves the configuring of MLS for Voice in 802.1P priority-tagged frames.

### Objectives

The objectives of this challenge are to:

- Define MLS.
- Apply to FA0/1.
- Define 802.1P frames.

The commands used are:

```
> enable
# config t
(config)# mls qos
(config)# int fa0/1
(config-if)# mls qos trust cos
(config-if)# switchport voice vlan dot1p
```

### Example

```
> enable
# config t
(config)# mls ?
  aclmerge  Modify behavior of ACL merge
  qos       QoS parameters
(config)# mls qos
(config-if)# mls ?
  qos       qos command keyword

(config-if)# mls qos ?
  cos       Configure interface COS parameters
  dscp-mutation  Apply DSCP-DSCP map to DSCP trusted port
  monitor   Collect QoS statistics
  trust     Configure trust state of interface
(config-if)# mls qos trust ?
  cos       Classify by packet COS
  device    trusted device class
```

```

dscp          Classify by packet DSCP
ip-precedence Classify by packet IP precedence
<cr>
(config-if)# mls qos trust cos
(config-if)# switchport voice ?
    vlan      Vlan for voice traffic
(config-if)# switchport voice vlan ?
    <1-4094>   Vlan for voice traffic
    dot1p     Priority tagged on PVID
    none      Don't tell telephone about voice vlan
    untagged  Untagged on PVID
(config-if)# switchport voice vlan dot1p

```

## Cisco Switch Challenge 98

**Area:** Switches – Voice VLAN

### Outline

This challenge involves the configuring of MLS for Voice where the CoS value that is received is overwritten with a new value.

### Objectives

The objectives of this challenge are to:

- Define MLS.
- Define the routing for 802.1Q frames.
- Apply to FA0/1.
- Define the CoS value – 0 lowest priority, 7 highest priority.

The commands used are:

```

# config t
(config)# int vlan 3
(config-vlan)# exit

(config)# mls qos
(config)# int fa0/1
(config-if)# mls qos trust cos
(config-if)# switchport voice vlan 3
(config-if)# switchport priority extended cos 3

```

### Example

```

> enable
# config t
(config)# mls ?
    aclmerge  Modify behavior of ACL merge
    qos       QoS parameters
(config)# mls qos

```

```

(config)# int fa0/1
(config-if)# mls qos trust cos
(config-if)# switchport priority extended ?
    cos      Override 802.1p priority of devices on appliance
    trust    Trust 802.1p priorities of devices on appliance

(config-if)# switchport priority extended cos ?
    <0-7>    Priority for devices on appliance

(config-if)# switchport priority extended cos 3 ?
    <cr>
(config-if)# switchport priority extended cos 3
(config-if)# priority-queue ?
    out      egress priority queue

(config-if)# priority-queue out ?
    <cr>
(config-if)# priority-queue out

```

# Cisco Switch Challenge 99

Area: Switches – Voice VLAN

## Outline

This challenge involves the configuring the switch so that the IP phone trusts the CoS value.

## Objectives

The objectives of this challenge are to:

- Define MLS.
- Define the routing for 802.1Q frames.
- Apply to FA0/1.

The commands used are:

```

# config t
(config)# int vlan 3
(config-vlan)# exit

(config)# mls qos
(config)# int fa0/1
(config-if)# mls qos trust cos
(config-if)# switchport voice vlan 3
(config-if)# switchport extend trust

```

## Example

```

> enable
# config t
(config)# mls ?
    aclmerge  Modify behavior of ACL merge

```

```
    qos      QoS parameters
(config)# mls qos

(config)# int fa0/1
(config-if)# mls qos trust cos
(config-if)# switchport voice vlan 3

(config-if)# switchport priority extended ?
    cos      Override 802.1p priority of devices on appliance
    trust    Trust 802.1p priorities of devices on appliance

(config-if)# switchport extend trust
```

## Cisco Switch Test 8 (Challenge 100)

### Unit 8: QoS

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

<http://networksims.com/sw08.html>

## Cisco Switch Challenge 101

### Outline

This challenge involves the configuration of an access-class.

### Objectives

The objectives of this challenge are to:

- Setup an access-list for a single access to the Web server.
- Apply the access-list to the Web server.

### Example

```
> en
# config t
(config)# access-list 9 permit 193.91.79.4
(config)# access-list 9 deny any
(config)# ip http access-class ?
    <1-99> Access list number
(config)# ip http access-class 9
(config)# ip http server
```

# Cisco Switch Challenge 102

## Outline

This challenge involves the configuration to deny access for a single host to the Web server.

## Objectives

The objectives of this challenge are to:

- Define an access-list which denies a single host.
- Apply the access-list onto the Web server.

## Example

```
> en
# config t
(config)# access-list 11 deny 192.1.179.24
(config)# access-list 11 permit any
(config)# ip http access-class ?
    <1-99> Access list number
(config)# ip http access-class 11
(config)# ip http server
```

# Cisco Switch Challenge 103

## Outline

This challenge involves the configuration which permits a single host access to a Telnet server.

## Objectives

The objectives of this challenge are to:

- Define an access-list which permits a single host access to the Telnet server.
- Apply the access-list onto the Telnet server.

## Example

```
# config t
(config)# access-list 8 permit 205.191.68.8
(config)# access-list 8 deny any
(config)# line vty 0 15
```

```
(config-line)# login
(config-line)# access-list ?
<1-199>      IP access list
<1300-2699>  IP expanded access list
WORD        Access-list name
(config-line)# access-list 8 ?
in  Filter incoming connections
out Filter outgoing connections
(config-line)# access-list 8 in
```

# Cisco Switch Challenge 104

## Outline

This challenge involves the configuration which denies a single host access a Telnet server.

## Objectives

The objectives of this challenge are to:

- Define an access-list which denies a single host access to a Telnet server.
- Apply the access-list to the Telnet server.

## Example

```
# config t
(config)# access-list 8 deny 205.191.68.8
(config)# access-list 8 permit any
(config)# line vty 0 15
(config-line)# login
(config-line)# access-list ?
<1-199>      IP access list
<1300-2699>  IP expanded access list
WORD        Access-list name
(config-line)# access-list 8 ?
in  Filter incoming connections
out Filter outgoing connections
(config-line)# access-list 8 in
```

# Cisco Switch Challenge 105

## Outline

This challenge involves the configuration of an restriction on a user.

## Objectives

The objectives of this challenge are to:

- Define a single host access.
- Link the access to a user.

### Example

```

> en
# config t
(config)# access-list 6 permit 12.84.44.10
(config)# access-list 6 deny any

(config)# username david ?
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 david access-class ?
<1-199>               Access-class number
<1300-2699>           Expanded Access-class number
(config)# username david access-class 6
(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 106

### Outline

This challenge involves the configuration of switchport restrictions.

### Objectives

The objectives of this challenge are to:

- Define port-security.

## Example

```

> en
# 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 access
(config-if)# switchport port-security violation ?
  protect         Security violation protect mode
  restrict        Security violation restrict mode
  shutdown        Security violation shutdown mode
(config-if)# switchport port-security violation shutdown
(config-if)# switchport port-security ?
  aging           Port-security aging commands
  mac-address     Secure mac address
  maximum         Max secure addresses
  violation       Security violation mode
  <cr>

(config-if)# switchport port-security mac-address ?
  H.H.H          48 bit mac address
  sticky         Configure dynamic secure addresses as sticky

(config-if)# switchport port-security mac-address 00e0.4e3d.a1bb

```

# Cisco Switch Challenge 107

## Outline

This challenge involves the configuration of a single host access to SNMP.

## Objectives

The objectives of this challenge are to:

- Define an access-list which permits a single host.
- Apply the access-list onto SNMP restrictions.

## Example

```
# config t
(config)# access-list 6 permit 111.101.136.8
(config)# access-list 6 deny any
(config)# snmp-server community fries ?
<1-99> Std IP accesslist allowing access with this community string
<1300-1999> Expanded IP accesslist allowing access with this community
string
ro Read-only access with this community string
rw Read-write access with this community string
view Restrict this community to a named MIB view
<cr>
(config)# snmp-server community fries rw ?
<1-99> Std IP accesslist allowing access with this community string
<1300-1999> Expanded IP accesslist allowing access with this community
string
<cr>
(config)# snmp-server community fries rw 6
```

# Cisco Switch Challenge 108

## Outline

This challenge involves the configuration of a local server for AAA.

## Objectives

The objectives of this challenge are to:

- Define AAA.
- Define the local server.

## Example

```
> enable
# config t
(config)# aaa new-model
(config)# aaa authentication ?
arap Set authentication lists for arap.
banner Message to use when starting login/authentication.
```

```

dot1x          Set authentication lists for IEEE 802.1x.
enable        Set authentication list for enable.
fail-message   Message to use for failed login/authentication.
login         Set authentication lists for logins.
nasi         Set authentication lists for NASI.
password-prompt Text to use when prompting for a password
ppp          Set authentication lists for ppp.
username-prompt Text to use when prompting for a username
(config)# aaa authentication login ?
WORD         Named authentication list.
default     The default authentication list.
(config)# aaa authentication login default ?
enable      Use enable password for authentication.
group       Use Server-group
line        Use line password for authentication.
local       Use local username authentication.
local-case  Use case-sensitive local username authentication.
none        NO authentication.
(config)# aaa authentication login default local
(config)# username fred password bert
(config)# username fred1 password bert2

```

Or

```

> enable
# config t
(config)# aaa new-model
(config)# aaa authentication login default group ?
WORD      Server-group name
radius    Use list of all Radius hosts.
tacacs+   Use list of all Tacacs+ hosts.

(config)# aaa authentication login default group radius
(config)# username fred password bert
(config)# username fred1 password bert2

```

## Cisco Switch Challenge 109

### Outline

This challenge involves the configuration of a RADIUS server for AAA.

### Objectives

The objectives of this challenge are to:

- Define AAA.
- Define the radius server.

### Example

```

> enable
# config t
(config)# aaa new-model
(config)# radius-server ?
  attribute          Customize selected radius attributes
  authorization      Authorization processing information
  challenge-noecho   Data echoing to screen is disabled during
                    Access-Challenge
  configure-nas      Attempt to upload static routes and IP pools at startup
  deadtime           Time to stop using a server that doesn't respond
  directed-request   Allow user to specify radius server to use with '@server'
  domain-stripping   Strip the domain from the username
  host               Specify a RADIUS server
  key                encryption key shared with the radius servers
  local              Configure local RADIUS server
  optional-passwords The first RADIUS request can be made without requesting a
                    password
  retransmit         Specify the number of retries to active server
  timeout            Time to wait for a RADIUS server to reply
  unique-ident       Higher order bits of Acct-Session-Id
  vsa                Vendor specific attribute configuration
(config)# radius-server host 39.100.234.1
(config)# radius-server key ?
  LINE  Text of shared key
(config)# radius-server key krinkle
(config)# aaa ?
  accounting          Accounting configurations parameters.
  authentication      Authentication configurations parameters.
  authorization       Authorization configurations parameters.
  configuration       Authorization configuration parameters.
  nas                 NAS specific configuration
  new-model           Enable NEW access control commands and functions.(Disables
                    OLD commands.)
  processes           Configure AAA background processes
(config)# aaa authentication ?
  arap                Set authentication lists for arap.
  banner              Message to use when starting login/authentication.
  enable              Set authentication list for enable.
  fail-message        Message to use for failed login/authentication.
  login               Set authentication lists for logins.
  nasi                Set authentication lists for NASI.
  password-prompt    Text to use when prompting for a password
  ppp                 Set authentication lists for ppp.
  username-prompt    Text to use when prompting for a username
(config)# aaa authentication login ?
  WORD                Named authentication list.
  default             The default authentication list.
(config)# aaa authentication login default ?
  enable              Use enable password for authentication.
  group               Use Server-group
  line                Use line password for authentication.
  local               Use local username authentication.
  local-case          Use case-sensitive local username authentication.
  none                NO authentication.
(config)# aaa authentication login default group radius
(config)# aaa authentication ?
  arap                Set authentication lists for arap.

```

```

banner          Message to use when starting login/authentication.
enable          Set authentication list for enable.
fail-message    Message to use for failed login/authentication.
login           Set authentication lists for logins.
nasi           Set authentication lists for NASI.
password-prompt Text to use when prompting for a password
ppp            Set authentication lists for ppp.
username-prompt Text to use when prompting for a username
(config)# aaa authentication ppp ?
WORD           Named authentication list.
default        The default authentication list.
(config)# aaa authentication ppp default radius
(config)# aaa authorization ?
commands       For exec (shell) commands.
config-commands For configuration mode commands.
exec           For starting an exec (shell).
network        For network services. (PPP, SLIP, ARAP)
reverse-access For reverse access connections
(config)# aaa authorization network ?
WORD           Named authorization list.
default        The default authorization list.
(config)# aaa authorization network default ?
enable         Use enable password for authentication.
group          Use Server-group
line           Use line password for authentication.
local          Use local username authentication.
local-case     Use case-sensitive local username authentication.
(config)# aaa authorization network default group radius
(config)# aaa authorization exec default group radius

```

# Cisco Switch Challenge 110

## Outline

This challenge involves the configuration of a Tacacs+ server for AAA.

## Objectives

The objectives of this challenge are to:

- Define AAA.
- Define the Tacacs+ server.

## Example

```

> enable
# config t
(config)# aaa new-model
(config)# tacacs-server ?
administration Start tacacs+ daemon handling administrative messages
attempts        Number of login attempts via TACACS
directed-request Allow user to specify tacacs server to use with '@server'

```

```

dns-alias-lookup    Enable IP Domain Name System Alias lookup for TACACS
                   servers
extended           Enable extended TACACS
host               Specify a TACACS server
key               Set TACACS+ encryption key.
last-resort        Define TACACS action if no server responds
optional-passwords The first TACACS request can be made without password
                   verification
packet            Modify TACACS+ packet options
retransmit         Search iterations of the TACACS server list
timeout           Time to wait for a TACACS server to reply
(config)# tacacs-server h ?
  Hostname or A.B.C.D  IP address of TACACS server
  <cr>
(config)# tacacs-server host 39.100.234.1
(config)# tacacs-server key ?
  LINE  Encryption key string
(config)# tacacs-server key krinkle
(config)# aaa authentication login default group tacacs
(config)# aaa authentication ppp default group tacacs
(config)# aaa authorization network default group tacacs
(config)# aaa authorization exec default group tacacs

```

# Cisco Switch Challenge 111

## Outline

This challenge involves the configuration of a Tacacs+ server for commands.

## Objectives

The objectives of this challenge are to:

- Define AAA.
- Define privileges.
- Define command authorization for a Tacacs+ server.

## Example

```

> enable
# config t
(config)# aaa new-model
(config)# privilege ?
  cns_connect_intf_config  CNS Connect Intf Info Mode
  config-rtr-http          RTR HTTP raw request Configuration
  configure                Global configuration mode
  exec                     Exec mode
  interface                Interface configuration mode
  interface                Interface range configuration mode
  ipenacl                  IP named extended access-list configuration mode
  ipsnacl                  IP named simple access-list configuration mode

```

line	Line configuration mode
mac-naacl	MAC named extended ACL configuration mode
map-class	Map class configuration mode
map-list	Map list configuration mode
mstp_cfg	MSTP configuration mode
null-interface	Null interface configuration mode
preauth	AAA Preauth definitions
rtr	RTR Entry Configuration
sg-radius	Radius Server-group Definition
sg-tacacs+	Tacacs+ Server-group Definition
template	Template configuration mode
vc-class	VC class configuration mode

```

(config)# privilege configure level 7 snmp-server host
(config)# privilege configure level 7 snmp-server enable
(config)# privilege configure level 7 snmp-server
(config)# privilege exec level 7 ping
(config)# privilege exec level 7 configure terminal
(config)# privilege exec level 7 configure
(config)# radius-server host 39.100.234.1
(config)# radius-server key krinkle
(config)# aaa authorization commands 0 default group tacacs+
(config)# aaa authorization commands 15 default group tacacs+
(config)# aaa authorization commands 7 default group tacacs+

```

## Explanation

The privilege levels go from level 0 to level 15, such as:

- **Level 0.** This only includes five commands: disable, enable, exit, help and logout.
- **Level 1.** This is the non-privileged mode with a prompt of **router>**.
- **Level 15.** This is the highest level of privilege, and has a prompt of **router#**.

Typical 1 commands are:

access-enable	Create a temporary Access-List entry
clear	Reset functions
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
lock	Lock the terminal
login	Log in as a particular user
logout	Exit from the EXEC
name-connection	Name an existing network connection
<b>ping</b>	<b>Send echo messages</b>
rcommand	Run command on remote switch
resume	Resume an active network connection
show	Show running system information
systat	Display information about terminal lines
telnet	Open a telnet connection
terminal	Set terminal line parameters

```
traceroute      Trace route to destination
tunnel          Open a tunnel connection
where           List active connections
```

Thus:

```
(config)# privilege configure level 7 snmp-server host
(config)# privilege configure level 7 snmp-server enable
(config)# privilege configure level 7 snmp-server
(config)# privilege exec level 7 ping
(config)# privilege exec level 7 configure terminal
(config)# privilege exec level 7 configure
```

moves these commands to Level 7. For example ping is a Level 1 command and is now a Level 7, while the rest have moved from Level 15 to Level 7.

## Cisco Switch Challenge 112

### Outline

This challenge involves enabling 802.1x authentication.

### Objectives

The objectives of this challenge are to:

- Define AAA
- Enable 802.1x.
- Define re-authentication.

### Example

```
> en
# config t
(config)# int fa0/1
(config-if)# no switchport
(config-if)# dot1x ?
  default          Configure Dot1x with default values for this port
  host-mode        Set the Host mode for 802.1x on this interface
  max-req          Max No.of Retries
  port-control     set the port-control value
  reauthentication Enable or Disable Reauthentication for this port
  timeout          Various Timeouts

(config-if)# dot1x port-control ?
  auto             PortState will be set to AUTO
  force-authorized PortState set to Authorized
  force-unauthorized PortState will be set to Unauthorized
(config-if)# dot1x port-control auto
(config-if)# dot1x reauthentication ?
<cr>
```

```

(config-if)# dot1x re-authentication

(config-if)# dot1x timeout ?
  quiet-period      QuietPeriod in Seconds
  reauth-period     Time after which an automatic re-authentication should be
                   initiated
  server-timeout    Timeout for Radius Retries
  supp-timeout      Timeout for Supplicant retries
  tx-period         Timeout for Supplicant Re-transmissions

(config-if)# dot1x timeout reauth-period ?
  <1-65535> Enter a value between 1 and 65535

(config-if)# dot1x timeout reauth-period 180

```

# Cisco Switch Challenge 113

## Outline

This challenge involves enabling 802.1x authentication with authentication from an AAA server.

## Objectives

The objectives of this challenge are to:

- Enable AAA.
- Define the Radius server.
- radius server.
- Enable 802.1x.
- Define re-authentication.
- Define Dot1x timeouts.

The commands used are:

```

(config)# aaa new-model
(config)# aaa accounting connection default start-stop group radius
(config)# aaa accounting network default start-stop group radius
(config)# aaa authentication dot1x default group radius local
(config)# dot1x system-auth-control
(config)# radius-server host 10.0.0.1 auth-port 1812 key test
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# dot1x port-control auto
(config-if)# dot1x re-authentication
(config-if)# dot1x timeout reauth-period 180
(config-if)# dot1x timeout tx-period 40
(config-if)# dot1x timeout quiet-period 10
(config-if)# dot1x max-req 3

```

## Example

```

> en
# config t
(config)# aaa new-model
(config)# aaa authn dot1x ?
    WORD      Named authentication list.
    default   The default authentication list.

(config)# aaa authentication dot1x default ?
    enable    Use enable password for authentication.
    group     Use Server-group
    line      Use line password for authentication.
    local     Use local username authentication.
    local-case Use case-sensitive local username authentication.
    none      NO authentication.

(config)# aaa authentication dot1x default ?
    enable    Use enable password for authentication.
    group     Use Server-group
    line      Use line password for authentication.
    local     Use local username authentication.
    local-case Use case-sensitive local username authentication.
    none      NO authentication.

(config)# aaa authentication dot1x default group ?
    WORD      Server-group name
    radius    Use list of all Radius hosts.
    tacacs+   Use list of all Tacacs+ hosts.
(config)# aaa authentication dot1x default group radius local
(config)# aaa accounting network ?
    WORD      Named Accounting list.
    default   The default accounting list.

(config)# aaa accounting network default ?
    none      No accounting.
    start-stop Record start and stop without waiting
    stop-only  Record stop when service terminates.
    wait-start Same as start-stop but wait for start-record commit.

(config)# aaa accounting network d star ?
    group     Use Server-group

(config)# aaa accounting net d star g ?
    WORD      Server-group name
    radius    Use list of all Radius hosts.
    tacacs+   Use list of all Tacacs+ hosts.
(config)# aaa accounting network default start-stop group radius
(config)# aaa accounting connection ?
    WORD      Named Accounting list.
    default   The default accounting list.

(config)# aaa accounting connection default ?
    none      No accounting.
    start-stop Record start and stop without waiting
    stop-only  Record stop when service terminates.
    wait-start Same as start-stop but wait for start-record commit.

(config)# aaa accounting connection default start-stop ?
    group     Use Server-group

(config)# aaa accounting connection default start-stop group ?
    WORD      Server-group name
    radius    Use list of all Radius hosts.
    tacacs+   Use list of all Tacacs+ hosts.

```

```

(config)# aaa accounting connection default start-stop group radius ?
  group Use Server-group
  <cr>
(config)# aaa accounting connection default start-stop group radius
(config)# dot1x ?
  system-auth-control Enable or Disable SysAuthControl
(config)# dot1x system-auth-control

(config)# radius-server host ?
  Hostname or A.B.C.D IP address of RADIUS server

(config)# radius-server host 10.0.0.1 ?
  acct-port UDP port for RADIUS accounting server (default is 1646)
  alias 1-8 aliases for this server (max. 8)
  auth-port UDP port for RADIUS authentication server (default is 1645)
  backoff Retry backoff pattern (Default is retransmits with constant
  delay)
  key per-server encryption key (overrides default)
  non-standard Parse attributes that violate the RADIUS standard
  retransmit Specify the number of retries to active server (overrides
  default)
  timeout Time to wait for this RADIUS server to reply (overrides
  default)
  <cr>

(config)# radius-server host 10.0.0.1 au ?
  <0-65536> Port number

(config)# radius-server host 10.0.0.1 au 1812 ?
  acct-port UDP port for RADIUS accounting server (default is 1813)
  auth-port UDP port for RADIUS authentication server (default is 1812)
  key per-server encryption key (overrides default)
  non-standard Parse attributes that violate the RADIUS standard
  retransmit Specify the number of retries to active server (overrides
  default)
  timeout Time to wait for this RADIUS server to reply (overrides
  default)
  <cr>

(config)# radius-server host 10.0.0.1 auth-port 1812 key ?
  LINE Text for this server's key

(config)# radius-server host 10.0.0.1 auth-port 1812 key test

(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# dot1x ?
  default Configure Dot1x with default values for this port
  host-mode Set the Host mode for 802.1x on this interface
  max-req Max No.of Retries
  port-control set the port-control value
  reauthentication Enable or Disable Reauthentication for this port
  timeout Various Timeouts
(config-if)# dot1x port-control auto
(config-if)# dot1x re-authentication
(config-if)# dot1x timeout ?
  quiet-period QuietPeriod in Seconds
  reauth-period Time after which an automatic re-authentication should be
  initiated
  server-timeout Timeout for Radius Retries
  supp-timeout Timeout for Supplicant retries

```

```
tx-period          Timeout for Supplicant Re-transmissions
(config-if)# dot1x timeout reauth-period 180
(config-if)# dot1x timeout tx-period 40
(config-if)# dot1x timeout quiet-period 10
(config-if)# dot1x max-req ?
<1-10> Enter a value between 1 and 10
(config-if)# dot1x max-req 3
```

# Cisco Switch Challenge 114

## Outline

This challenge involves the configuration of security of a switch.

## Objectives

The objectives of this challenge are to:

- Define usernames and passwords.
- Define privilege levels.
- Restrict access of users to a single host.

## Example

```
> enable
# config t
(config)# username fred password bert
(config)# username test nopassword
(config)# username fred privilege 15
(config)# username test privilege 1
(config)# username test user-maxlinks 2
(config)# access-list 9 permit host 192.168.0.1
(config)# username fred access-class 9
```

## Explanation

The privilege levels go from level 0 to level 15, such as:

- **Level 0.** This only includes five commands: disable, enable, exit, help and logout.
- **Level 1.** This is the non-privileged mode with a prompt of **router>**.
- **Level 15.** This is the highest level of privilege, and has a prompt of **router#**.

Typical 1 commands are:

access-enable	Create a temporary Access-List entry
clear	Reset functions
connect	Open a terminal connection
disable	Turn off privileged commands

disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
lock	Lock the terminal
login	Log in as a particular user
logout	Exit from the EXEC
name-connection	Name an existing network connection
ping	Send echo messages
rcommand	Run command on remote switch
resume	Resume an active network connection
show	Show running system information
systat	Display information about terminal lines
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
tunnel	Open a tunnel connection
where	List active connections

Thus:

```
(config)# username fred privilege 15
(config)# username test privilege 1
```

sets the maximum privilege level for **fred** at 15, while **test** will only be able to enter the non-privileged mode. Also:

```
(config)# access-list 9 permit host 192.168.0.1
(config)# username fred access-class 9
```

restricts the access for fred to a single host (192.168.0.1), so that the user will not be able to log-in from any other host. The following:

```
(config)# username test user-maxlinks 2
```

restricts the number of connections for **test** to two.

## Cisco Switch Challenge 115

### Outline

This challenge involves the configuration of security of a switch.

### Objectives

The objectives of this challenge are to:

- Define Tacacs+.
- Define accounting for start and stop events.

## Example

```
> enable
# config t
(config)# aaa new-model
(config)# aaa account network default start-stop group tacacs+
(config)# aaa account reverse-access default group tacacs+
```

# Cisco Switch Challenge 116

## Outline

This challenge involves the configuration of security of a switch based on 802.1x.

## Objectives

The objectives of this challenge are to:

- Define AAA.
- Define port authentication.

## Example

```
> enable
# config t
(config)# aaa new-model
(config)# aaa authentication dot1x default group radius
(config)# int fa0/1
(config-if)# dot1x ?
  default          Configure Dot1x with default values for this port
  guest-vlan       Configure Guest-vlan on this interface
  host-mode        Set the Host mode for 802.1x on this interface
  max-req          Max No.of Retries
  port-control     set the port-control value
  reauthentication Enable or Disable Reauthentication for this port
  timeout         Various Timeouts
(config-if)# dot1 port-control ?
  auto             PortState will be set to AUTO
  force-authorized PortState set to Authorized
  force-unauthorized PortState will be set to Unauthorized
(config-if)# dot1x port-control auto
(config-if)# int fa0/2
(config-if)# dot1x port-control auto
(config-if)# int fa0/4
(config-if)# dot1x port-control auto
(config-if)# exit
(config)# exit
# sh dot1x all
Sysauthcontrol          = Disabled
```

```

Dot1x Protocol Version          = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
# sh dot1x all
Dot1x Info for interface FastEthernet0/1
-----
Supplicant MAC <Not Applicable>
  AuthSM State      = N/A
  BendSM State      = N/A
PortStatus          = N/A
MaxReq              = 2
HostMode            = Single
Port Control        = Auto
QuietPeriod         = 60 Seconds
Re-authentication   = Disabled
ReAuthPeriod        = 3600 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
TxPeriod            = 30 Seconds
Guest-Vlan          = 0
# sh dot1x stat interface fa0/1
PortStatistics Parameters for Dot1x
-----
TxReqId = 0      TxReq = 0      TxTotal = 0
RxStart = 0      RxLogoff = 0    RxRespId = 0    RxResp = 0
RxInvalid = 0   RxLenErr = 0    RxTotal= 0
RxVersion = 0   LastRxSrcMac 0000.0000.0000

```

# Cisco Switch Challenge 117

## Outline

This challenge involves enabling 802.1x authentication.

## Objectives

The objectives of this challenge are to:

- Enable 802.1x.
- Define re-authentication.

## Example

```

> en
# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# dot1x ?
  default          Configure Dot1x with default values for this port
  host-mode        Set the Host mode for 802.1x on this interface
  max-req          Max No.of Retries

```

```
port-control      set the port-control value
reauthentication  Enable or Disable Reauthentication for this port
timeout          Various Timeouts
```

```
(config-if)# dot1x port-control ?
```

```
auto             PortState will be set to AUTO
force-authorized PortState set to Authorized
force-unauthorized PortState will be set to Unauthorized
```

```
(config-if)# dot1x port-control auto
```

```
(config-if)# dot1x reauthentication ?
```

```
<cr>
```

```
(config-if)# dot1x re-authentication
```

```
(config-if)# dot1x t ?
```

```
quiet-period      QuietPeriod in Seconds
reauth-period     Time after which an automatic re-authentication should be
                  initiated
server-timeout    Timeout for Radius Retries
supp-timeout      Timeout for Supplicant retries
tx-period         Timeout for Supplicant Re-transmissions
```

```
(config-if)# dot1x t r ?
```

```
<1-65535> Enter a value between 1 and 65535
```

```
(config-if)# dot1x timeout reauth-period 180
```

# Cisco Switch Challenge 118

## Outline

This challenge involves defending against an attacker depleting the DHCP pool using DHCP snooping.

## Objectives

The objectives of this challenge are to:

- Enable DHCP snooping.
- Apply DHCP snooping on an interface.

## Example

```
> en
```

```
# config t
```

```
Switch(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
snoothing          DHCP Snooping
Switch(config)# ip dhcp snooping ?
  information      DHCP Snooping information
  vlan            DHCP Snooping vlan
  <cr>
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan ?
  <1-4094>        DHCP Snooping vlan first number
Switch(config)# ip dhcp snooping vlan 4
Switch(config)# int fa0/1
Switch(config-if)# ip dhcp ?
  snooping        DHCP Snooping
Switch(config-if)# ip dhcp snooping ?
  limit           DHCP Snooping limit
  trust           DHCP Snooping trust config
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit ?
  rate           DHCP Snooping limit

Switch(config-if)# ip dhcp snooping limte rate ?
  <1-4294967294> DHCP snooping rate limit
Switch(config-if)# ip dhcp snooping limte rate 30

```

# Cisco Switch Challenge 119

## Outline

This challenge involves the setting up storm control

## Objectives

The objectives of this challenge are to:

- Enable storm control

## Example

```

> enable

Switch# config t
Switch(config)# int vlan 1
Switch(config-vlan)# ip address 1.2.3.4 255.0.0.0
Switch(config-vlan)# exit

Switch(config)# int fa0/1
Switch(config-if)# storm-control ?
  broadcast       Broadcast address storm control
  multicast       Multicast address storm control
  unicast         Unicast address storm control

```

```
Switch(config-if)# storm-control multicast ?
level Set storm suppression level on this interface
```

```
Switch(config-if)# storm-control multicast level ?
<0 - 100> Enter Integer part of level as percentage of bandwidth
```

```
Switch(config-if)# storm-control multicast level 50
Switch(config-if)# exit
Switch(config)# exit
```

```
Switch# sh storm
Interface  Filter State  Level  Current
-----
Fa0/1     inactive      100.00% N/A
Fa0/2     inactive      100.00% N/A
Fa0/3     inactive      100.00% N/A
Fa0/4     inactive      100.00% N/A
Fa0/5     inactive      100.00% N/A
Fa0/6     inactive      100.00% N/A
Fa0/7     inactive      100.00% N/A
Fa0/8     inactive      100.00% N/A
Fa0/9     inactive      100.00% N/A
Fa0/10    inactive      100.00% N/A
Fa0/11    inactive      100.00% N/A
Fa0/12    inactive      100.00% N/A
Fa0/13    inactive      100.00% N/A
Fa0/14    inactive      100.00% N/A
Fa0/15    inactive      100.00% N/A
Fa0/16    inactive      100.00% N/A
Fa0/17    inactive      100.00% N/A
Fa0/18    inactive      100.00% N/A
Fa0/19    inactive      100.00% N/A
Fa0/20    inactive      100.00% N/A
Fa0/21    inactive      100.00% N/A
Fa0/22    inactive      100.00% N/A
Fa0/23    inactive      100.00% N/A
Fa0/24    inactive      100.00% N/A
Gi0/1     inactive      100.00% N/A
Gi0/2     inactive      100.00% N/A
```

```
Switch# sh storm multi
Interface  Filter State  Level  Current
-----
Fa0/1     Forwarding    50.00%  0.00%
Fa0/2     inactive      100.00% N/A
Fa0/3     inactive      100.00% N/A
Fa0/4     inactive      100.00% N/A
Fa0/5     inactive      100.00% N/A
Fa0/6     inactive      100.00% N/A
Fa0/7     inactive      100.00% N/A
Fa0/8     inactive      100.00% N/A
Fa0/9     inactive      100.00% N/A
Fa0/10    inactive      100.00% N/A
Fa0/11    inactive      100.00% N/A
Fa0/12    inactive      100.00% N/A
Fa0/13    inactive      100.00% N/A
Fa0/14    inactive      100.00% N/A
Fa0/15    inactive      100.00% N/A
Fa0/16    inactive      100.00% N/A
Fa0/17    inactive      100.00% N/A
Fa0/18    inactive      100.00% N/A
Fa0/19    inactive      100.00% N/A
```

```

Fa0/20    inactive    100.00%  N/A
Fa0/21    inactive    100.00%  N/A
Fa0/22    inactive    100.00%  N/A
Fa0/23    inactive    100.00%  N/A
Fa0/24    inactive    100.00%  N/A
Gi0/1     inactive    100.00%  N/A
Gi0/2     inactive    100.00%  N/A

```

```

Switch# sh stor fa0/1 m
Interface  Filter State   Level   Current
-----
Fa0/1     Forwarding    50.00%  0.00%

```

# Cisco Switch Challenge 120

## Outline

This challenge involves the configuration of a MAC ACL.

## Objectives

The objectives of this challenge are to:

- Define a MAC ACL.
- Define a host to bar from FA0/1.
- Apply the MAC ACL on an interface (FA0/1).

## Example

```

> en
# config t
(config)# mac ?
  access-list    Named access-list
  address-table  Configure the MAC address table
(config)# mac acc ?
  extended      Extended Access List
(config)# mac acc ex ?
  WORD          access-list name
(config)# mac acc ex Edinburgh
(config-ext-macl)# ?
Extended MAC Access List configuration commands:
  default      Set a command to its defaults
  deny         Specify packets to reject
  exit         Exit from MAC Named ACL configuration mode
  no           Negate a command or set its defaults
  permit       Specify packets to forward
(config-ext-macl)# deny ?
  H.H.H        48-bit source MAC address
  any          any source MAC address
  host         A single source host
(config-ext-macl)# deny host 1.1.1 ?
  H.H.H        48-bit destination MAC address
  any          any destination MAC address

```

```

host    A single destination host
(config-ext-macl)# deny host 1.1.1 any
(config-ext-macl)# permit any any
(config-ext-macl)# exit
(config)# int fa0/1
(config-if)# mac ?
    access-group  MAC access-group configuration commands
(config-if)# mac access-group ?
    WORD          ACL name

(config-if)# mac access-group Edinburgh ?
    in            Apply to Ingress
(config-if)# mac acc Edinburgh in
(config-if)# exit
(config)# exit
# show access-list
Extended MAC access list Edinburgh
    deny host 1.1.1 any
    permit any any

```

# Cisco Switch Challenge 121

## Outline

This challenge involves the configuration of monitors for port spanning.

## Objectives

The objectives of this challenge are to:

- Define monitors for source and destination.

## Example

```

> en
# config t
(config)# monitor ?
    session      Configure a SPAN session

(config)# monitor session
    <1-2>        SPAN session number

(config)# monitor session 1 ?
    destination  SPAN destination interface, VLAN
    source       SPAN source interface, VLAN

(config)# monitor session 1 destination ?
    interface    SPAN destination interface
    remote       SPAN destination Remote

(config)# monitor session 1 source interface ?
    FastEthernet  FastEthernet IEEE 802.3
    GigabitEthernet  GigabitEthernet IEEE 802.3z

```

```

(config)# monitor session 1 des interface fa0
,       Specify another range of interfaces
-       Specify a range of interfaces
both   Monitor received and transmitted traffic
rx     Monitor received traffic only
tx     Monitor transmitted traffic only
<cr>
(config)# monitor session 1 source interface fa0/3
(config)# monitor session 1 destination interface fa0/7
(config)# exit
# sh monitor
  Session 1
-----
Source Ports:
  RX Only:      None
  TX Only:      None
  Both:         FA0/3
Destination Ports: FA0/7
# config t
(config)# int vlan 1
(config-if)# ip address 148.183.229.5 255.255.248.0
(config-if)# exit
(config)# ip domain-name perthshire.cc
(config)# ip default-gateway 148.183.229.6

```

## Cisco Switch Challenge 122

**Area:** Switches – MAC address notification traps

### Outline

MAC address notification allows the tracking of MAC address activity through SNMP using a trap which sends information to an SNMP server when there is activity. The trap interval defines the time that the updates will be send to the SNMP server which can reduce network traffic when there are a great deal of MAC address activity.

### Objectives

The objectives of this challenge are to:

- Define MAC address notification traps.
- Define notification details.

The commands used are:

```

# config t
(config)# snmp-server host 1.2.3.4
(config)# snmp-server enable traps mac-notification
(config)# mac address-table notification
(config)# mac address-table notification interval 60
(config)# mac address-table notification history-size 160

```

```
(config)# int fa0/6
(config-if)# int fa0/6
(config-if)# snmp trap mac-notification added
```

## Example

```
# config t
(config)# snmp-server host 1.2.3.4
(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 Informs options
  ip              IP ToS configuration for SNMP traffic
  location        Text for mib object sysLocation
  manager         Modify SNMP manager parameters
  packetize       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 enable ?
  informs  Enable SNMP Informs
  traps    Enable SNMP Traps

(config)# snmp-server 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 mac-notification

(config)# mac ?
  access-list   Named access-list
  address-table Configure the MAC address table

(config)# mac address-table ?
  aging-time    Set MAC address table entry maximum age
```

```

notification Enable/Disable MAC Notification on the switch
static static keyword

(config)# mac address-table notification ?
  history-size Number of MAC notifications to be stored
  interval Interval between the MAC notifications
  <cr>

(config)# mac address-table notification
(config)# mac address-table notification interval 60
(config)# mac address-table notification history-size 160

(config)# int fa0/6
(config-if)# snmp ?
  ifindex Persist ifindex for the interface
  trap Allow a specific SNMP trap

(config-if)# snmp trap ?
  link-status Allow SNMP LINKUP and LINKDOWN traps
  mac-notification MAC Address notification for the interface

(config-if)# snmp trap mac-notification ?
  added Enable Mac Address added notification for this port
  removed Enable Mac Address removed notification for this port

(config-if)# snmp trap mac-notification added
(config-if)# end

# show mac address-table notification
MAC Notification Feature is Disabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 0
Number of MAC Addresses Removed : 0
Number of Notifications sent to NMS : 0
Maximum Number of entries configured in History Table : 120
Current History Table Length : 0
MAC Notification Traps are Disabled
History Table contents
-----

# sh mac address-table notification interface
MAC Notification Feature is Enabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
-----
Interface MAC Added Trap MAC Removed Trap
-----
FastEthernet0/1 Disabled Disabled
FastEthernet0/2 Disabled Disabled
FastEthernet0/3 Disabled Disabled
FastEthernet0/4 Disabled Disabled
FastEthernet0/5 Disabled Disabled
FastEthernet0/6 Enabled Disabled
FastEthernet0/7 Disabled Disabled
FastEthernet0/8 Disabled Disabled
FastEthernet0/9 Disabled Disabled
FastEthernet0/10 Disabled Disabled
FastEthernet0/11 Disabled Disabled
FastEthernet0/12 Disabled Disabled
FastEthernet0/13 Disabled Disabled
FastEthernet0/14 Disabled Disabled
FastEthernet0/15 Disabled Disabled
FastEthernet0/16 Disabled Disabled
FastEthernet0/17 Disabled Disabled

```

FastEthernet0/18	Disabled	Disabled
FastEthernet0/19	Disabled	Disabled
FastEthernet0/20	Disabled	Disabled
FastEthernet0/21	Disabled	Disabled
FastEthernet0/22	Disabled	Disabled
FastEthernet0/23	Disabled	Disabled
FastEthernet0/24	Disabled	Disabled
GigabitEthernet0/1	Disabled	Disabled
GigabitEthernet0/2	Disabled	Disabled

# Cisco Switch Challenge 123

**Area:** Switches – Secure Addresses

## Outline

Secure addresses allow the administrator to define the MAC address of the host which connects to a certain VLAN and interface to be pre-defined. If it does not match, it will not be able to connect.

## Objectives

The objectives of this challenge are to:

- Define secure MAC addresses.

The commands used are:

```
# config t
(config)# int fa0/1
(config-if)# switchport mode access
(config-if)# switchport port-security mac-address 1.2.3
(config-if)# int fa0/2
(config-if)# switchport mode access
(config-if)# switchport port-security mac-address 1.2.4
(config-if)# int fa0/3
(config-if)# switchport mode access
(config-if)# switchport port-security mac-address 1.2.5
(config-if)# end
```

## 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
```



```
(config-if)# switchport mode dynamic desirable
```

and thus must be changed to:

```
(config-if)# switchport mode access
```

As, with this, it gives:

```
(config-if)# switchport port mac 1.2.3
FastEthernet0/x is dynamic port. port-security parameters cannot be set.
```

If another address is added to an already defined interface gives:

```
(config-if)# sw port- mac- 1.2.5
Total secure mac-addresses on interface FastEthernet0/x has reached maximum limit.
```

The number of secure addresses can be changed with the:

```
switchport port-security maximum x
```

command

## Cisco Switch Challenge 124

### Outline

This challenge involves setting up a static MAC address table.

### Objectives

The objectives of this challenge are to:

- Enable static MAC address table.
- Show the MAC address table.

### Example

```
> en
# config t
(config)# mac ?
  access-list      Named access-list
  address-table    Configure the MAC address table

(config)# mac address-table ?
  ageing-time      Set MAC address table entry maximum age
  notification     Enable/Disable MAC Notification on the switch
  static           static keyword

(config)# mac address-table ageing-time ?
```

```

<0-0>          Enter 0 to disable aging
<10-1000000>  Aging time in seconds

(config)# mac address-table static ?
H.H.H  48 bit mac address

(config)# mac address-table static 1.1.1 ?
vlan  VLAN keyword

(config)# mac address-table static 1.1.1 vlan ?
<1-4094>  VLAN id of mac address table

(config)# mac address-table static 1.1.1 vlan 1 ?
drop      drop frames
interface interface

(config)# mac address-table static 1.1.1 vlan 1 int ?
FastEthernet      FastEthernet IEEE 802.3
GigabitEthernet  GigabitEthernet IEEE 802.3z
Port-channel      Ethernet Channel of interfaces

(config)# mac address-table static 1.1.1 vlan 1 int fa0/1
(config)# exit
# sh mac-address-table
      Mac Address Table
-----

```

Vlan	Mac Address	Type	Ports
All	0012.00b0.2780	STATIC	CPU
All	0012.00b0.2781	STATIC	CPU
All	0012.00b0.2782	STATIC	CPU
All	0012.00b0.2783	STATIC	CPU
All	0012.00b0.2784	STATIC	CPU
All	0012.00b0.2785	STATIC	CPU
All	0012.00b0.2786	STATIC	CPU
All	0012.00b0.2787	STATIC	CPU
All	0012.00b0.2788	STATIC	CPU
All	0012.00b0.2789	STATIC	CPU
All	0012.00b0.278a	STATIC	CPU
All	0012.00b0.278b	STATIC	CPU
All	0012.00b0.278c	STATIC	CPU
All	0012.00b0.278d	STATIC	CPU
All	0012.00b0.278e	STATIC	CPU
All	0012.00b0.278f	STATIC	CPU
All	0012.00b0.2790	STATIC	CPU
All	0012.00b0.2791	STATIC	CPU
All	0012.00b0.2792	STATIC	CPU
All	0012.00b0.2793	STATIC	CPU
All	0012.00b0.2794	STATIC	CPU
All	0012.00b0.2795	STATIC	CPU
All	0012.00b0.2796	STATIC	CPU
All	0012.00b0.2797	STATIC	CPU
All	0012.00b0.2798	STATIC	CPU
All	0012.00b0.2799	STATIC	CPU
All	0012.00b0.279a	STATIC	CPU
All	0100.0c00.0000	STATIC	CPU

```

All      0100.0ccc.cccc      STATIC      CPU
All      0100.0ccc.cccd      STATIC      CPU
All      0100.0ccd.cdce      STATIC      CPU
All      0180.c200.0000      STATIC      CPU
All      0180.c200.0001      STATIC      CPU
All      0180.c200.0002      STATIC      CPU
All      0180.c200.0003      STATIC      CPU
All      0180.c200.0004      STATIC      CPU
All      0180.c200.0005      STATIC      CPU
All      0180.c200.0006      STATIC      CPU
All      0180.c200.0007      STATIC      CPU
All      0180.c200.0008      STATIC      CPU
All      0180.c200.0009      STATIC      CPU
All      0180.c200.000a      STATIC      CPU
All      0180.c200.000b      STATIC      CPU
All      0180.c200.000c      STATIC      CPU
All      0180.c200.000d      STATIC      CPU
All      0180.c200.000e      STATIC      CPU
All      0180.c200.000f      STATIC      CPU
All      0180.c200.0010      STATIC      CPU
    1      0001.0001.0001      STATIC      Fa0/1
    1      000d.28fb.ebda      DYNAMIC     Gi0/2
    1      000d.298e.f359      DYNAMIC     Gi0/1
Total Mac Addresses for this criterion: 51

```

On a switch, the secure address table holds secure MAC addresses and their associated ports and VLANs. The command allows a secure address that is forwarded to only one port per VLAN. Thus:

```
(config)# mac-address-table static 1.1.1 vlan 1 int fa0/1
```

Will forward anything for the MAC address of 1.1.1 on VLAN 1 to FA0/1.

An alternative is:

```

> en
# config t
(config)# mac-address-table ?
(config)# mac-address-table ageing-time ?
(config)# mac-address-table static ?
(config)# mac-address-table static 1.1.1 ?
(config)# mac-address-table static 1.1.1 vlan ?
(config)# mac-address-table static 1.1.1 vlan 1 ?
(config)# mac-address-table static 1.1.1 vlan 1 int ?
(config)# mac-address-table static 1.1.1 vlan 1 int fa0/1

```

## Cisco Switch Challenge 125

### Outline

This challenge involves setting up SNMP MAC notification traps.

## Objectives

The objectives of this challenge are to:

- Enable a MAC SNMP trap.
- Define an interval time.
- Apply the trap on an interface.

## Example

```
> en
# config t
Switch(config)# snmp-server host 192.168.0.1
Switch(config)# snmp-server enable traps mac-notification
Switch(config)# mac-address-table notification interval ?
<0-2147483647> Notification interval in seconds
Switch(config)# mac-address-table notification interval 60
Switch(config)# mac-address-table notification history-size ?
<0-500> Number of entries in history table
Switch(config)# mac-address-table notification history-size 100
Switch(config)# interface fastethernet0/1
Switch(config-if)# snmp ?
  ifindex  Persist ifindex for the interface
  trap     Allow a specific SNMP trap
Switch(config-if)# snmp trap ?
  link-status      Allow SNMP LINKUP and LINKDOWN traps
  mac-notification MAC Address notification for the interface
Switch(config-if)# snmp trap mac-notification ?
  added    Enable Mac Address added notification for this port
  removed  Enable Mac Address removed notification for this port
Switch(config-if)# snmp trap mac-notification added
```

MAC address notification is used to track whenever a machine connects to the network. In this case whenever a new MAC address is learned, or one is removed, generates an SNMP trap. If there are many machines connecting, the traps can be grouped together, and sent at regular intervals (such as 60 second in the example).

# Cisco Switch Test

## MLS Optimization and Security

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

<http://networksims.com/s9.html>

# Cisco Switch Test

**Final test**

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

**<http://networksims.com/>**