

CCNP ISCW

Cisco Router Challenge 1

Outline

This challenge involves the configuration of the E0 port on a router.

Objectives

The objectives of this challenge are to:

- Setup the IP address on E0 port.
- Setup the subnet mask on E0 port.
- Enable the E0 port.
- Set the description for the E0 port.
- Define the speed of the E0 port.
- Define duplex on the E0 port.

Example

```
> enable
# config t
(config)# int e0
(config-if)# ip address 36.109.222.1 255.255.255.128
(config-if)# no shutdown
(config-if)# description testing123
(config-if)# speed 10
(config-if)# duplex half
(config-if)# end
```

Cisco Router Challenge 17

Outline

This challenge involves the configuration of a standard ACL.

Objectives

The objectives of this challenge are to:

- Setup a standard ACL.
- Setup an ACL to permit and deny a single host.
- Setup an ACL to permit and deny a single network.
- Setup an ACL to permit everything else.
- Apply it on the incoming port of E0.

Example

```
> en
# config t
(config)# access-list 2 permit host 130.152.162.10
(config)# access-list 2 deny host 193.68.36.8
(config)# access-list 2 permit 207.182.133.0 0.1.255.255
(config)# access-list 2 deny 153.246.194.0 0.0.127.255
(config)# access-list 2 permit any

(config)# int e0
(config-if)# ip access-group 2 in
```

Cisco Router Challenge 18

Outline

This challenge involves the configuration of a standard ACL.

Objectives

The objectives of this challenge are to:

- Setup a standard ACL.
- Setup an ACL to permit and deny a single host.
- Setup an ACL to permit and deny a single network.
- Setup an ACL to deny everything else.
- Apply it on the incoming port of S0.

Example

```
> en
# config t
(config)# access-list 2 permit host 130.152.162.10
(config)# access-list 2 deny host 193.68.36.8
(config)# access-list 2 permit 207.182.133.0 0.1.255.255
(config)# access-list 2 deny 153.246.194.0 0.0.127.255
(config)# access-list 2 deny any

(config)# int s0
```

```
(config-if)# ip access-group 2 in
```

Cisco Router Challenge 19

Outline

This challenge involves the configuration of an extended ACL.

Objectives

The objectives of this challenge are to:

- Define an extended ACL.
- Define a host to be allowed.
- Define a host to be denied.
- Define a network to be allowed.
- Define a network to be denied.
- Permit everything else.
- Apply ACL onto E0.

Example

```
> en
# config t
(config)# access-list 105 ?
deny      Specify packets to reject
dynamic   Specify a DYNAMIC list of PERMITs or DENYS
permit    Specify packets to forward
remark    Access list entry comment
(config)# access-list 105 permit ?
<0-255>   An IP protocol number
ahp       Authentication Header Protocol
eigrp     Cisco's EIGRP routing protocol
esp       Encapsulation Security Payload
gre       Cisco's GRE tunneling
icmp      Internet Control Message Protocol
igmp      Internet Gateway Message Protocol
igrp      Cisco's IGRP routing protocol
ip        Any Internet Protocol
ipinip    IP in IP tunneling
nos       KA9Q NOS compatible IP over IP tunneling
ospf      OSPF routing protocol
pcp       Payload Compression Protocol
pim       Protocol Independent Multicast
tcp       Transmission Control Protocol
udp       User Datagram Protocol
(config)# access-list 105 permit tcp host 208.89.101.4 host 41.153.91.2 eq ftp

(config)# access-list 105 deny tcp host 197.119.92.8 host 144.98.220.6 eq ftp

(config)# access-list 105 permit tcp 100.120.83.0 255.255.255.0 71.252.23.0
255.255.255.0 eq ftp
```

```

(config)# access-list 105 deny tcp 35.208.170.0 255.255.255.0 184.124.8.0
255.255.255.0 eq ftp

(config)# access-list 105 ?
deny      Specify packets to reject
dynamic   Specify a DYNAMIC list of PERMITs or DENYs
permit    Specify packets to forward
remark    Access list entry comment
(config)# access-list 105 permit tcp
A.B.C.D   Source address
any       Any source host
host      A single source host
(config)# access-list 105 permit tcp any ?
A.B.C.D   Destination address
any       Any destination host
eq        Match only packets on a given port number
gt        Match only packets with a greater port number
host      A single destination host
lt        Match only packets with a lower port number
neq       Match only packets not on a given port number
range     Match only packets in the range of port numbers
(config)# access-list 105 permit tcp any any
(config)# int e0
(config-if)# ip access-group 105 in

```

Cisco Router Challenge 20

Outline

This challenge involves the configuration of named ACLs.

Objectives

The objectives of this challenge are to:

- Define a named standard ACL.
- Define a named extended ACL.

Example

```

> en
# config t
(config)# ip access-list ?
extended   Extended Access List
log-update  Control access list log updates
logging     Control access list logging
standard   Standard Access List
(config)# ip access-list standard
<1-99>     Standard IP access-list number
WORD       Access-list name
(config)# ip access-list standard leeds
(config-std-nacl)# deny ?
Hostname or A.B.C.D  Address to match

```

```

any          Any source host
host         A single host address
(config-std-nacl)# deny host 193.34.245.4
(config-std-nacl)# permit host 16.21.50.10
(config-std-nacl)# deny 18.223.156.0 0.15.255.255
(config-std-nacl)# permit 139.32.80.0 0.15.255.255
(config-std-nacl)# exit
(config)# int s0
(config-if)# ip access-group ?
<1-199>      IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
WORD        Access-list name
(config-if)# ip access-group leads in
(config-if)# exit
(config)# ip access-list extended tennessee
(config-ext-nacl)# deny ?
<0-255>     An IP protocol number
ahp         Authentication Header Protocol
eigrp       Cisco's EIGRP routing protocol
esp         Encapsulation Security Payload
gre         Cisco's GRE tunneling
icmp        Internet Control Message Protocol
igmp        Internet Gateway Message Protocol
igrp        Cisco's IGRP routing protocol
ip          Any Internet Protocol
ipinip      IP in IP tunneling
nos         KA9Q NOS compatible IP over IP tunneling
ospf        OSPF routing protocol
pcp         Payload Compression Protocol
pim         Protocol Independent Multicast
tcp         Transmission Control Protocol
udp         User Datagram Protocol
(config-ext-nacl)# deny tcp host 198.89.74.1 host 208.177.41.6 eq telnet
(config-ext-nacl)# permit tcp host 205.198.245.6 host 202.226.135.3 eq telnet
(config-ext-nacl)# deny tcp 54.83.187.0 255.255.255.0 101.167.107.0 255.255.255.0
eq telnet
(config-ext-nacl)# permit tcp 56.248.48.0 255.255.255.0 138.236.218.0 255.255.255.0
eq telnet
(config-ext-nacl)# exit
(config)# int s1
(config-if)# ip access-group tennessee in

```

Cisco Switch Challenge 33

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 login default local
(config)# username fred password bert
(config)# username fred1 password bert2
```

Cisco Switch Challenge 34

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 35

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)# radius-server host 39.100.234.1  
(config)# radius-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 36

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 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
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)# 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 37

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 38

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 39

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 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 Router Challenge 31

Outline

This challenge involves the configuration of a priority group and route-cache.

Objectives

The objectives of this challenge are to:

- Define an access-list.
- Define an priority-group.
- Define a route-cache.

Example

```

> en
# config t
(config)# access-list ?
  <1-99>                IP standard access list
  <100-199>              IP extended access list
  <1000-1099>            IPX SAP access list
  <1100-1199>            Extended 48-bit MAC address access list
  <1200-1299>            IPX summary address access list
  <1300-1999>            IP standard access list (expanded range)
  <200-299>              Protocol type-code access list
  <2000-2699>            IP extended access list (expanded range)
  <700-799>              48-bit MAC address access list
  <800-899>              IPX standard access list
  <900-999>              IPX extended access list
  dynamic-extended      Extend the dynamic ACL absolute timer
  rate-limit             Simple rate-limit specific access list

(config)# access-list 105 ?
  deny                   Specify packets to reject

```

```

dynamic Specify a DYNAMIC list of PERMITs or DENYS
permit Specify packets to forward
remark Access list entry comment
(config)# access-list 105 permit tcp host 144.93.24.10 host 131.33.204.2 eq dns
(config)# access-list 105 deny tcp host 154.31.216.9 host 26.100.164.1 eq dns
(config)# access-list 105 permit tcp 243.76.220.0 255.255.0.0 89.36.160.0
255.255.0.0 eq dns
(config)# access-list 105 deny tcp 102.65.178.0 255.255.0.0 5.101.146.0 255.255.0.0
eq dns
(config)# access-list 105 permit ip ?
A.B.C.D Source address
any Any source host
host A single source host
(config)# access-list 105 permit ip any
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
(config)# access-list 105 permit ip any any
(config)# int e0
(config-if)# ip access-group 105 in
(config)# exit
(config)# priority-list 1 protocol ?
arp IP ARP
bridge Bridging
cdp Cisco Discovery Protocol
compressedtcp Compressed TCP
ip IP
ipx Novell IPX
llc2 llc2
pad PAD links
snapshot Snapshot routing support
(config)# priority-list 1 protocol ip ?
high
medium
normal
low
(config)# priority-list 1 protocol ip high ?
fragments Prioritize fragmented IP packets
gt Prioritize packets greater than a specified size
list To specify an access list
lt Prioritize 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
<cr>
(config)# priority-list 1 protocol ip high list ?
<1-199> IP access list
<1300-2699> IP expanded access list
(config)# priority-list 1 protocol ip high list 105
(config)# int e0
(config-if)#priority-group ?
<1-16> Priority group
(config-if)#priority-group 1
(config-if)# ip route-cache ?
cef Enable Cisco Express Forwarding
flow Enable Flow fast-switching cache
policy Enable fast-switching policy cache for outgoing packets
same-interface Enable fast-switching on the same interface
<cr>

```

```
(config-if)# ip route-cache
(config-if)# int e1
(config-if)# ip route-cache
```

Cisco Router Challenge 33

Outline

This challenge involves the configuration of services on the router.

Objectives

The objectives of this challenge are to:

- Define encrypted passwords.
- Define timestamps.
- Disable TCP small services.
- Disable UDP small services.

Example

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

```

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

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

```

Cisco Router Challenge 38

Outline

This challenge involves the configuration of AAA.

Objectives

The objectives of this challenge are to:

- Define AAA details.

Example

```

> en
# config t

```

```
(config)# aaa new-model
(config)# aaa authn logging def radius
(config)# aaa authn ppp def radius
(config)# aaa authn banner new york
(config)# aaa authn fail personal device
(config)# aaa author network default radius
(config)# aaa author exec default radius
```

Cisco Router Challenge 39

Outline

This challenge involves the configuration of Tacacs+.

Objectives

The objectives of this challenge are to:

- Setup of Tacacs+.

Example

```
> en
# config t
(config)# aaa new-model
(config)# aaa authn logging def tacacs+
(config)# aaa authn ppp def tacacs+
(config)# aaa authn banner new york
(config)# aaa authn fail personal device
(config)# aaa author network default tacacs+
(config)# aaa author exec default tacacs+
```

Cisco Router Challenge 40

Outline

This challenge involves the configuration of restrictions on the local HTTP server.

Objectives

The objectives of this challenge are to:

- Setup an ACL to permit a single host.
- Apply ACL to restrict access to the HTTP server to only one host.

Example

```
> en
# config t
(config)# access-list 7 permit host 23.17.220.3
(config)# access-list 7 deny any
(config)# ip http server
(config)# ip http ?
  access-class    Restrict access by access-class
  authentication  Set http authentication method
  path            Set base path for HTML
  port            HTTP port
  server          Enable HTTP server
(config)# ip http access-class ?
  <1-99> Access list number
(config)# ip http access-class 7
```

Cisco Router Challenge 41

Outline

This challenge involves the configuration of the HTTP server which denies a single host.

Objectives

The objectives of this challenge are to:

- Setup an ACL which denies a single host.
- Apply the ACL to deny the host access to the HTTP server.

Example

```
> en
# config t
(config)# access-list 7 deny host 23.17.220.3
(config)# access-list 7 permit any
(config)# ip http server
(config)# ip http access-class 7
```

Cisco Router Challenge 42

Outline

This challenge involves the configuration of permitting a single host access to the Telnet server.

Objectives

The objectives of this challenge are to:

- Setup an ACL to allow a single host access.
- Apply the ACL to the Telnet server so that only a single host can get access.

Example

```
> en
# config t
(config)# access-list 1 permit host 202.179.77.6
(config)# access-list 1 deny any
(config)# line vty 0 15
(config-line)# login
(config-line)# access-class ?
  <1-199>      IP access list
  <1300-2699>  IP expanded access list
  WORD        Access-list name
(config-line)# access-class 1 ?
  in  Filter incoming connections
  out Filter outgoing connections
(config-line)# access-class 1 in
```

Cisco Router Challenge 43

Outline

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

Objectives

The objectives of this challenge are to:

- Setup an ACL to deny a single host access.
- Apply the ACL to the Telnet server so that only a single host cannot get access.

Example

```
> en
# config t
(config)# access-list 1 deny host 202.179.77.6
(config)# access-list 1 permit any
(config)# line vty 0 15
(config-line)# login
(config-line)# access-class ?
(config-line)# access-class 1 in
```

Cisco Router Challenge 44

Outline

This challenge involves the configuration of IP Inspect.

Objectives

The objectives of this challenge are to:

- Setup limits for the number of connections over one-minute.
- Setup limits for the number of open connections.
- Define SYN waits.

Example

```
> en
# config t
(config)# ip inspect ?
  alert-off          Disable alert
  audit-trail        Enable the logging of session information (addresses and
                    bytes)
  dns-timeout        Specify timeout for DNS
  max-incomplete     Specify maximum number of incomplete connections before
                    clamping
  name               Specify an inspection rule
  one-minute         Specify one-minute-sample watermarks for clamping
  tcp                Config timeout values for tcp connections
  udp                Config timeout values for udp flows
  <cr>
(config)# ip inspect one-minute ?
  high               Specify high-watermark for clamping
  low                Specify low-watermark for clamping
(config)# ip inspect one-minute low 360
(config)# ip inspect one-minute high 410
(config)# ip inspect max-incomplete low 720
(config)# ip inspect max-incomplete high 770
(config)# ip inspect dns-timeout 1
(config)# ip inspect tcp ?
  finwait-time       Specify timeout for TCP connections after a FIN
  idle-time          Specify idle timeout for tcp connections
  max-incomplete     Specify max half-open connection per host
  synwait-time       Specify timeout for TCP connections after a SYN and no
                    further data
(config)# ip inspect tcp synwait-time ?
  <1-2147483>        Timeout in seconds
(config)# ip inspect tcp synwait-time 35
(config)# ip inspect tcp finwait-time 5

(config)# ip inspect tcp max-incomplete ?
  host               Specify max half-open connection per host
(config)# ip inspect tcp max-incomplete host 800
(config)# ip inspect tcp ?
  finwait-time       Specify timeout for TCP connections after a FIN
  idle-time          Specify idle timeout for tcp connections
  max-incomplete     Specify max half-open connection per host
  synwait-time       Specify timeout for TCP connections after a SYN and no
                    further data
(config)# ip inspect tcp idle-time 70
```

```
(config)# ip inspect udp idle-time 57
```

Cisco Router Challenge 45

Outline

This challenge involves the configuration of a context based access-list (CBAC).

Objectives

The objectives of this challenge are to:

- Setup a CBAC.
- Define the protocols which the CBAC applies to.

Example

```
> en
# config t
(config)# access-list 105 permit ip any any
(config)# int fa0/0
(config-if)# ip access-group 105 in
(config-if)# exit
(config)# ip inspect name cisco ?
  cuseeme      CUSeeMe Protocol
  fragment     IP fragment inspection
  ftp          File Transfer Protocol
  h323         H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
  http        HTTP Protocol
  netshow     Microsoft NetShow Protocol
  rcmd        R commands (r-exec, r-login, r-sh)
  realaudio   Real Audio Protocol
  rpc         Remote Procedure Call Protocol
  rtsp        Real Time Streaming Protocol
  smtp        Simple Mail Transfer Protocol
  sqlnet      SQL Net Protocol
  streamworks StreamWorks Protocol
  tcp         Transmission Control Protocol
  tftp        TFTP Protocol
  udp         User Datagram Protocol
  vdolive     VDOLive Protocol
(config)# ip inspect name cisco tcp
(config)# ip inspect name cisco udp
(config)# ip inspect name cisco ftp
(config)# ip inspect name cisco sqlnet
(config)# int e0
(config-if)#ip inspect ?
  WORD Name of inspection defined
(config-if)#ip inspect cisco
(config-if)#ip inspect cisco in
(config-if)# exit
(config)# access-list 106 deny ip any any
(config)# int s0
(config-if)# ip access-group 106 in
```

Explanation

ACLs are fairly static in their operation, and they do not take into account the context of a data packet. Thus they cannot detect the actual state of a connection. A typical type of attack in a system is DoS (Denial-of-Service), which is caused when multiple remote clients make access to the same server. Knowing the context of a data packet, or its associated connection thus allows finer control of the security of the system. For example in a DoS the firewall could detect that the number of connections in a given time limit had exceeded a given number, and block any other ones, within a given time. Context-based Access Control (CBAC) are thus stateful, and dynamic, and can look further into packets than normal ACLs. In client-server communications the key states in most connections are:

- Client sends a **SYN** flag to the server.
- The server responds with a **SYN, ACK** to the client.
- The client responds with an **ACK**, and the connection is made.
- The client and server then communicate.
- The client sends a **FIN, ACK** flag.
- The server sends an **ACK** flag, and the connection is finished.

Context-based Access Control is used to implement firewall options, such as limiting the number of open connections. A typical attack is the DoS (Denial of Service) attack, where the external party opens up multiple connections. To overcome this, the router can be setup to detect a minimum threshold for half-open sessions. The half-open session is where either the client or server quits the session without the other side knowing about it. In a DoS, the client opens a connection, and does not complete it. The server does not know that the client has disconnected, thus the connection still takes some resources on the server, which can become overburdened if there are many open sessions. On the Napier pods, use Pod C (Router 1) for an example of router which implements these CBACs.

Global timeouts and thresholds

The main limits that are defined are:

- **ip inspect tcp synwait-time**. This defines the time to wait before a connection drops. Default: 30 seconds.
- **ip inspect tcp finwait-time**. This defined the time after a FIN flag for a connection to be dropped. Default: 5 seconds.
- **ip inspect tcp idle-time**. This defines the length of time that a connection can be idle. Default: 1 hour.
- **ip inspect dns-time**. This defines the amount of time of a time-out for a DNS query. Default: 5 seconds.
- **ip inspect max-incomplete high**. This defines the maximum number of half-open connections, before it starts to delete them one-by-one. Default: 500.

- **ip inspect max-incomplete low.** This defines the lower limit for the half-open connections. Default: 400.
- **ip inspect one-minute high.** This defines the maximum number of half-open connections in a minute, before it starts to delete them one-by-one. Default: 500 per minute.
- **ip inspect one-minute low.** This defines the lower limit for the half-open connections over a minute. Default: 400.

For example to limit the maximum open sessions at any time to between 900 and 1100:

```
(config)# ip inspect ?
  alert-off          Disable alert
  audit-trail        Enable the logging of session information (addresses and
                    bytes)
  dns-timeout        Specify timeout for DNS
  max-incomplete     Specify maximum number of incomplete connections before
                    clamping
  name               Specify an inspection rule
  one-minute         Specify one-minute-sample watermarks for clamping
  tcp                Config timeout values for tcp connections
  udp                Config timeout values for udp flows
  <cr>
(config)# ip inspect tcp ?
  finwait-time       Specify timeout for TCP connections after a FIN
  idle-time          Specify idle timeout for tcp connections
  max-incomplete     Specify max half-open connection per host
  synwait-time       Specify timeout for TCP connections after a SYN and no
                    further data
(config)# ip inspect max-incomplete low 900
(config)# ip inspect max-incomplete high 1100
```

and for the maximum open sessions for one-minute:

```
(config)# ip inspect one-minute low 900
(config)# ip inspect one-minute high 1100
```

get rid of IP inspect, use:

```
(config)# no ip inspect one-minute low
```

To limit the DNS-timeout to 10 seconds:

```
(config)# ip inspect dns-timeout 10
```

Cisco Router Challenge 46

Outline

This challenge involves the configuration of a port map.

Objectives

The objectives of this challenge are to:

- Define the port-mapping for various protocols.

Example

```
> en
# config t
(config)# ip port-map http port 1126
(config)# ip port-map ftp port 1188
(config)# ip port-map smtp port 1897
(config)# ip port-map telnet port 1189
(config)# exit
# show ip port-map
Default mapping: vdolive          port 7000      system defined
Default mapping: sunrpc           port 111       system defined
Default mapping: netshow         port 1755     system defined
Default mapping: cuseeme         port 7648     system defined
Default mapping: tftp            port 69       system defined
Default mapping: rtsp            port 8554     system defined
Default mapping: realmedia       port 7070     system defined
Default mapping: streamworks     port 1558     system defined
Default mapping: ftp             port 21       system defined
Default mapping: telnet          port 23       system defined
Default mapping: rtsp            port 554      system defined
Default mapping: h323            port 1720     system defined
Default mapping: sip             port 5060     system defined
Default mapping: smtp            port 25       system defined
Default mapping: http            port 80       system defined
Default mapping: msrpc           port 135      system defined
Default mapping: exec            port 512      system defined
Default mapping: login           port 513      system defined
Default mapping: sql-net         port 1521     system defined
Default mapping: shell           port 514      system defined
Default mapping: mgcp            port 2427     system defined
Default mapping: http            port 1126     user defined
Default mapping: ftp             port 1188     user defined
Default mapping: smtp            port 1897     user defined
Default mapping: telnet          port 1189     user defined
```

Explanation

Many ports are well-known on the Internet, such as port 23 for Telnet and port 80 for HTTP. In many situations the port mapping to the protocol is not always standard, such as HTTP using port 8080. The **ip port-map** command can be used to remap ports to their application. An example of the command is:

```
(config) # ip port-map ?
cuseeme      CUSeeMe Protocol
dns          Domain Name Server
exec         Remote Process Execution
finger       Finger
ftp          File Transfer Protocol
gopher       Gopher
h323         H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
http         Hypertext Transfer Protocol
imap         Internet Message Access Protocol
kerberos     Kerberos
```

```

ldap      Lightweight Directory Access Protocol
login     Remote login
lotusnote Lotus Note
mgcp      Media Gateway Control Protocol
ms-sql    Microsoft SQL
msrpc     Microsoft Remote Procedure Call
netshow   Microsoft NetShow
nfs       Network File System
nntp      Network News Transfer Protocol
pop2      Post Office Protocol - Version 2
pop3      Post Office Protocol - Version 3
realmedia RealNetwork's Realmedia Protocol
rtsp      Real Time Streaming Protocol
sap       SAP
shell     Remote command
sip       Session Initiation Protocol
smtp      Simple Mail Transfer Protocol
snmp      Simple Network Management Protocol
sql-net   SQL-NET
streamworks StreamWorks Protocol
sunrpc    SUN Remote Procedure Call
sybase-sql Sybase SQL
tacacs    Login Host Protocol (TACACS)
telnet    Telnet
tftp      Trivial File Transfer Protocol
vdolive   VDOLive Protocol

```

So, for example, to map HTTP to port 8080:

```
(config) # ip port-map http port 8080
```

Then to show the port mapping:

```

# show ip port-map
Default mapping: vdolive      port 7000      system defined
Default mapping: sunrpc      port 111      system defined
Default mapping: netshow     port 1755     system defined
Default mapping: cuseeme     port 7648     system defined
Default mapping: tftp        port 69       system defined
Default mapping: rtsp        port 8554     system defined
Default mapping: realmedia   port 7070     system defined
Default mapping: streamworks port 1558     system defined
Default mapping: ftp         port 21       system defined
Default mapping: telnet      port 23       system defined
Default mapping: http        port 8080     user defined
Default mapping: rtsp        port 554     system defined
Default mapping: h323        port 1720     system defined
Default mapping: sip         port 5060     system defined
Default mapping: smtp        port 25       system defined
Default mapping: http        port 80       system defined
Default mapping: msrpc       port 135     system defined
Default mapping: exec        port 512     system defined
Default mapping: login       port 513     system defined
Default mapping: sql-net     port 1521     system defined
Default mapping: shell       port 514     system defined
Default mapping: mgcp        port 2427     system defined

# show ip port-map http
Default mapping: http        port 8080     user defined
Default mapping: http        port 80       system defined

```

Cisco Router Challenge 47

Outline

This challenge involves the configuration of an audit trail.

Objectives

The objectives of this challenge are to:

- Setup logging.
- Define an audit-trail.

Example

```
> en
# config t
(config)# logging on
(config)# logging 150.74.40.1
(config)# logging ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  cns-events          Set CNS Event logging level
  console             Set console logging level
  count              Count every log message and timestamp last occurrence
  exception          Limit size of exception flush output
  facility            Facility parameter for syslog messages
  history            Configure syslog history table
  host               Set syslog server host name or IP address
  monitor            Set terminal line (monitor) logging level
  on                 Enable logging to all supported destinations
  rate-limit         Set messages per second limit
  source-interface   Specify interface for source address in logging
                    transactions
  trap              Set syslog server logging level
(config)# logging host 18.46.203.4
(config)# logging trap ?
 <0-7>              Logging severity level
 alerts            Immediate action needed          (severity=1)
 critical          Critical conditions            (severity=2)
 debugging         Debugging messages          (severity=7)
 emergencies      System is unusable            (severity=0)
 errors            Error conditions             (severity=3)
 informational     Informational messages        (severity=6)
 notifications     Normal but significant conditions (severity=5)
 warnings         Warning conditions            (severity=4)
 <cr>
(config)# logging trap warning

(config)# logging monitor warning

(config)# logging console warning

(config)# logging buffer ?
 <0-7>              Logging severity level
 <4096-2147483647> Logging buffer size
 alerts            Immediate action needed          (severity=1)
 critical          Critical conditions            (severity=2)
 debugging         Debugging messages          (severity=7)
```

```

emergencies      System is unusable          (severity=0)
errors           Error conditions            (severity=3)
informational    Informational messages      (severity=6)
notifications    Normal but significant conditions (severity=5)
warnings        Warning conditions          (severity=4)
<cr>
(config)# logging buffer warnings
(config)# logging buffer 981997
(config)# ip inspect audit-trail
(config)# no ip inspect alert-off

```

Cisco Router Challenge 48

Outline

This challenge involves the configuration to deny an incoming SYN packet.

Objectives

The objectives of this challenge are to:

- Apply an extended ACL which detects the SYN packet.

Example

```

> en
#config t
(config)# access-list 107 deny tcp any any ?
  ack          Match on the ACK bit
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established Match established connections
  fin          Match on the FIN bit
  fragments    Check non-initial fragments
  gt           Match only packets with a greater port number
  log          Log matches against this entry
  log-input    Log matches against this entry, including input interface
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  psh          Match on the PSH bit
  range        Match only packets in the range of port numbers
  rst          Match on the RST bit
  syn          Match on the SYN bit
  time-range   Specify a time-range
  tos          Match packets with given TOS value
  urg          Match on the URG bit
  <cr>
(config)# access-list 107 deny tcp any any established
(config)# access-list 107 permit tcp any any
(config)# int s0
(config-if)# ip access-group ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name

```

```
(config-if)# ip access-group 107 ?
  in    inbound packets
  out   outbound packets
(config-if)# ip access-group 107 in
```

Cisco Router Challenge 54

Outline

This challenge involves the configuration of an authentication proxy.

Objectives

The objectives of this challenge are to:

- Define AAA.
- Setup an authentication proxy.

Example

```
> en
# config t
(config)# aaa new-model

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

(config)# ip auth-proxy ?
  auth-cache-time  Authorization Cache Timeout in min
  auth-proxy-audit Authentication Proxy Auditing
  auth-proxy-banner Authentication Proxy Banner
  name             Specify an Authentication Proxy Rule
<cr>
(config)# ip auth-proxy auth-cache-time ?
  <1-35791> Timeout in minutes
(config)# ip auth-proxy auth-cache-time 45

(config)# ip auth-proxy name yellow http

(config)# int fa0

(config-if)# ip auth-proxy ?
  WORD Name of authenticaion proxy rule
(config-if)# ip auth-proxy yellow
```

```

(config-if)# exit
# show ip auth-proxy configuration
# sh ip auth-proxy config
Authentication global cache time is 40 minutes
Authentication Proxy Rule Configuration
  Auth-proxy name testing
    http list not specified auth-cache-time 40 minutes
Authentication Proxy Rule Configuration
  Auth-proxy name testing

```

Cisco Router Challenge 55

Outline

This challenge involves the configuration of IDS rules.

Objectives

The objectives of this challenge are to:

- Setup IDS rules.
- Define a SPAM filter.

Example

```

> en
# config t
(config)# ip audit ?
  attack      Specify default action for attack signatures
  info        Specify default action for informational signatures
  name        Specify an IDS audit rule
  notify      Specify the notification mechanisms (nr-director or log) for the
              alarms
  po          Specify nr-director's PostOffice information (for sending events
              to the nr-directors)
  signature   Add a policy to a signature
  smtp        Specify SMTP Mail spam threshold
(config)# ip audit notify ?
  log         Send events as syslog messages
  nr-director Send events to the nr-director
(config)# ip audit notify log
(config)# logging 132.191.125.3

(config)# ip audit ?
  attack      Specify default action for attack signatures
  info        Specify default action for informational signatures
  name        Specify an IDS audit rule
  notify      Specify the notification mechanisms (nr-director or log) for the
              alarms
  po          Specify nr-director's PostOffice information (for sending events
              to the nr-directors)
  signature   Add a policy to a signature
  smtp        Specify SMTP Mail spam threshold
(config)# ip audit info ?

```

```

    action Specify the actions
(config)# ip audit info action ?
    alarm Generate events for matching signatures
    drop Drop packets matching signatures
    reset Reset the connection (if applicable)
(config)# ip audit info action drop
(config)# ip audit attack action reset
(config)# ip audit signature ?
    <1-65535> Signature to be configured
(config)# ip audit signature 1005 disable
(config)# ip audit smtp ?
    spam Specify the threshold for spam signature
    <cr>
(config)# ip audit smtp spam ?
    <1-65535> Threshold of correspondents to trigger alarm
(config)# ip audit smtp spam 4

```

Cisco Router Challenge 56

Outline

This challenge involves setting up IKE for a VPN connection.

Objectives

The objectives of this challenge are to:

- Define the IKE policy.
- Define encryption.
- Define hash function.
- Define authentication type.
- Define identity type.
- Define authentication key and address (for pre-share authentication).
- Define the transform set.

Example

```

> en
# config t
(config)# crypto isakmp enable
(config)# crypto isakmp policy 111
(config-isakmp)# encryption des
(config-isakmp)# hash sha
(config-isakmp)# authentication pre-share
(config-isakmp)# group 1
(config-isakmp)# exit
(config)# crypto isakmp identity hostname
(config)# crypto isakmp key test address 192.168.1.1
(config)# crypto ipsec transform-set test esp-des

```

Cisco Router Challenge 57

Outline

This challenge involves setting up a crypto map and applying it to an interface.

Objectives

The objectives of this challenge are to:

- Define a Crypto access-list, to identify the traffic to encrypt.
- Define IKE.
- Define a crypto map.
- Bind the ACL with the crypto map.
- Apply crypto map to E0.
- Show the tunnel details.

Example

```
> en
# config t
(config)# hostname newhampshire
(config)# access-list 109 permit ip 50.93.142.0 0.0.255.255
        136.163.130.0 0.0.255.255
(config)# crypto isakmp enable
(config)# crypto isakmp policy 111
(config-isakmp)# ?
ISAKMP commands:
 authentication  Set authentication method for protection suite
 default        Set a command to its defaults
 encryption     Set encryption algorithm for protection suite
 exit          Exit from ISAKMP protection suite configuration mode
 group         Set the Diffie-Hellman group
 hash          Set hash algorithm for protection suite
 lifetime      Set lifetime for ISAKMP security association
 no           Negate a command or set its defaults
(config-isakmp)# en ?
 3des  Three key triple DES
 aes   AES - Advanced Encryption Standard.
 des   DES - Data Encryption Standard (56 bit keys).
(config-isakmp)# encryption des
(config-isakmp)# hash ?
 md5  Message Digest 5
 sha  Secure Hash Standard
(config-isakmp)# hash sha
```

```

(config-isakmp)# authentication ?
  pre-share  Pre-Shared Key
  rsa-encr   Rivest-Shamir-Adleman Encryption
  rsa-sig    Rivest-Shamir-Adleman Signature
(config-isakmp)# authentication pre-share
(config-isakmp)# g ?
  1  Diffie-Hellman group 1
  2  Diffie-Hellman group 2
  5  Diffie-Hellman group 5
(config-isakmp)# group 1
(config-isakmp)# exit
(config)# crypto isakmp identity hostname
(config)# crypto isakmp key test address 192.168.1.1
(config)# crypto ipsec transform-set finland esp-des
(config)# crypto map manchester 10 ipsec-isakmp
(config-crypto-map)# ?
Crypto Map configuration commands:
  default      Set a command to its defaults
  description  Description of the crypto map statement policy
  dialer       Dialer related commands
  exit         Exit from crypto map configuration mode
  match        Match values.
  no           Negate a command or set its defaults
  qos          Quality of Service related commands
  reverse-route Reverse Route Injection.
  set          Set values for encryption/decryption
Router(config-crypto-map)# match ?
  address      Match address of packets to encrypt.

Router(config-crypto-map)# match address ?
  <100-199>    IP access-list number
  <2000-2699>  IP access-list number (expanded range)
  WORD         Access-list name
(config-crypto-map)# match address 109
(config-crypto-map)# set ?
  identity      Identity restriction.
  isakmp-profile Specify isakmp Profile
  peer          Allowed Encryption/Decryption peer.
  pfs           Specify pfs settings
  security-association Security association parameters
  transform-set Specify list of transform sets in priority order
(config-crypto-map)# set peer 144.55.62.1
(config-crypto-map)# set transform-set ?
  WORD         Proposal tag
(config-crypto-map)# set transform-set finland
(config-crypto-map)# set pfs group1
(config-crypto-map)# exit
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shut
(config-if)# crypto map Manchester
(config-if)# exit
(config)# exit
# show crypto ipsec sa

interface: E0
  Crypto map tag: Manchester, local addr 192.168.1.1

```

```

protected vrf: (none)
local ident (addr/mask/prot/port): (50.93.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (136.163.0.0/255.255.0.0/0/0)
current_peer 192.168.1.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 43, #pkts encrypt: 43, #pkts digest: 43
  #pkts decaps: 43, #pkts decrypt: 43, #pkts verify: 43
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 4, #recv errors 0

local crypto endpt.: 192.168.1.1, remote crypto endpt.: 144.55.62.1
path mtu 1500, ip mtu 1500, ip mtu idb E0
current outbound spi: 0x267BC43(40352835)

inbound esp sas:
  spi: 0xD9F4BC76(3656694902)
  transform: esp-des
  in use settings = {Tunnel, }
  conn id: 2001, flow_id: SW:1, crypto map: Manchester
  sa timing: remaining key lifetime (k/sec): (4558868/3550)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x267BC43(40352835)
  transform: esp-des
  in use settings = {Tunnel, }
  conn id: 2002, flow_id: SW:2, crypto map: Manchester
  sa timing: remaining key lifetime (k/sec): (4558868/3548)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

# show crypto isakmp sa
dst          src          state          conn-id slot          status
144.55.62.1 192.168.1.1  QM_IDLE       1      0      ACTIVE

```

Cisco Router Challenge 58

Outline

This challenge involves setting an access-list to allow IPSec.

Objectives

The objectives of this challenge are to:

- Create an access-list which allows AHP, ESP and ISAKMP.
- Applies the access-list.

Example

```
> en
# config t
(config)# hostname london

london (config)# access-list 101 permit ahp host 117.84.81.2 host
61.222.47.2

london (config)# access-list 101 permit esp host 117.84.81.2 host
61.222.47.2

london (config)# access-list 101 permit udp host 117.84.81.2 host
61.222.47.2 eq isakmp

london (config)# int e0
london (config-if)# ip address 136.22.25.1 255.252.0.0
london (config-if)# no shut
london (config-if)# ip access-group 101 in
```

Cisco Router Challenge 60

Outline

This challenge involves blocking SNMP.

Objectives

The objectives of this challenge are to:

- Define an access-list to block SNMP.
- Applies the access-list.
- Disable SNMP-server commands.

Example

```
> en
# config t
(config)# access-list 110 deny udp any any eq snmp
(config)# int e0
(config-if)# ip access-group 110 in
(config-if)# exit
(config)# service timestamps log datetime
(config)# service sequence-numbers
(config)# service dhcp
(config)# service finger
(config)# no service tcp-small-servers
(config)# no service udp-small-servers
(config)# service password-encryption
(config)# no snmp-server community annt RO
(config)# no snmp-server contact steven
(config)# no snmp-server location uk
(config)# no snmp-server host 78.113.70.11
(config)# no snmp-server enable traps
(config)# no snmp-server chassis-ID paris
```

Cisco Router Challenge 61

Outline

This challenge involves manually configuring RSA keys for peers.

Objectives

The objectives of this challenge are to:

- Define the public key for a given host.
- Specify the key.

Example

```
> en
# config t
(config)# crypto key pubkey-chain rsa
(config-pubkey-chain)# addressed-key 142.217.4.10
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
```

```
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 0123
(config-pubkey-key)# exit
(config-pubkey-chain)# exit
(config)# exit
# show crypto key pubkey rsa
```

Cisco Router Challenge 62

Outline

This challenge involves the setup of authenticated routing protocols.

Objectives

The objectives of this challenge are to:

- Define EIGRP.
- Apply MD5 authentication on an interface.
- Define the authentication key chain.

Example

```
# config t
(config)# router eigrp 142
(config-router)# network 205.104.0.0
(config-router)# int s0
(config-if)# ip address 205.118.116.6 255.255.255.224
(config-if)# ip authentication mode eigrp 142 md5
(config-if)# ip authentication key-chain eigrp 142 ann
(config-if)# exit
(config)# key chain ann
(config-keychain)# key 1
(config-keychain-key)# key-string hotel
(config-keychain-key)# exit
```

Router Challenge 124: SSH Explained

Outline: This challenge involves an analysis of SSH.

Objectives: The objectives of this challenge are to explain SSH.

Explanation

The TELNET protocol is insecure as the text is passed as plain text. An improved method is to use SSH, which encrypts data. It requires that the domain-name and an RSA key pair:

```
ap# config t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)# ip domain-name test.com
ap(config)# crypto key generate rsa
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
```

To view the public key:

```
ap#show crypto key mypubkey rsa
% Key pair was generated at: 00:42:19 UTC Mar 1 2002
Key name: ap.test.com
Usage: General Purpose Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DDD8C6 4B744520
 F1499B01 49C485A2 20C9FB37 8CD11053 039D344B 3C5BD55E E84E17C8 FD62DA08
 32020F80 910AFBCC 6D402F90 96E8A59B 40467A3E 8FEED18B B1020301 0001
% Key pair was generated at: 00:42:21 UTC Mar 1 2002
Key name: ap.test.com.server
Usage: Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B435A4 C007251B
 312319CA 0E919F76 72D2D5A9 36B4710C CC4DE0C4 080D2B47 55970CA5 39F21170
 D07C0000 832F6A1C 81411423 BE52CBF4 ECBE417E 1C3C09D1 2BBC90DF 8DA398DB
 AE8EFA46 282AEC54 F0909F82 466A19DD EBEFAEDE 7B4B992F 5F020301 0001
```

An SSH client such as putty can then be used to connect to the access point:

... graphic missed out on version see help file.

after which the client shows the message:

... graphic missed out on version see help file.

and the SSH connection is made, such as:

... graphic missed out on version see help file.

To get rid of keys:

```
ap(config)# crypto key zero
```

and to set the timeout and authentication retries:

```
ap(config)# ip ssh time-out 60
ap(config)# ip ssh authentication-retries 2
```

which sets the timeout to 60 seconds, and a maximum of two retries. Finally, to prevent Telnet sessions:

```
ap(config)#line vty 0 4
ap(config-line)# transport input ssh
```

Router Challenge 127: HSRP

Outline: This challenge involves an analysis of HSRP.

Objectives: The objectives of this challenge are to explain HSRP.

Explanation

Cisco's Hot Standby Routing Protocol (HSRP) allows a router to provide a backup for another. In HSRP, the backup router only monitors the other router. If it determines that the active (monitored) router is not responding, it will take over.

```
ap# config t
ap (config)# int e0
ap (config-if)# ip address 10.0.0.1 255.0.0.0
(config-if)# standby ?
  <0-255>      group number
authentication Authentication
delay         HSRP initialisation delay
ip            Enable HSRP and set the virtual IP address
mac-address   Virtual MAC address
name          Redundancy name string
preempt       Overthrow lower priority Active routers
priority      Priority level
redirect      Configure sending of ICMP Redirect messages with an HSRP
              virtual IP address as the gateway IP address
timers        Hello and hold timers
track         Priority tracking
use-bia       HSRP uses interface's burned in address
version       HSRP version
ap (config-if)# standby 1 ip 10.0.0.2
ap (config-if)# standby 1 preempt
ap (config-if)# standby 1 priority 100
ap (config-if)# standby 1 authentication edinburgh
ap (config-if)# standby 1 timers 5 15
```

```

ap (config-if)# st ANY ?
authentication Authentication
ip Enable HSRP and set the virtual IP address
mac-address Virtual MAC address
name Redundancy name string
preempt Overthrow lower priority Active routers
priority Priority level
timers Hello and hold timers
track Priority tracking

ap (config-if)# st 1 au ?
WORD Plain text authentication string
md5 Use MD5 authentication
text Plain text authentication

ap (config-if)# st 1 i ?
A.B.C.D Virtual IP address
<cr>

ap (config-if)# st 1 m ?
H.H.H MAC address

ap (config-if)# st 1 n ?
WORD name string

ap (config-if)# st 1 pre ?
delay Wait before preempting
<cr>

ap (config-if)# st 1 pri ?
<0-255> Priority value

ap (config-if)# st 1 ti ?
<1-254> Hello interval in seconds
msec Specify hello interval in milliseconds

ap (config-if)# st 1 ti 1 ?
<2-255> Hold time in seconds

ap (config-if)# st 1 tr ?
<1-500> Tracked object number
Async Async interface
BVI Bridge-Group Virtual Interface
CDMA-Ix CDMA Ix interface
CTunnel CTunnel interface
Dialer Dialer interface
FastEthernet FastEthernet IEEE 802.3
Lex Lex interface
Loopback Loopback interface
MFR Multilink Frame Relay bundle interface
Multilink Multilink-group interface
Port-channel Ethernet Channel of interfaces
Tunnel Tunnel interface
Vif PGM Multicast Host interface
Virtual-PPP Virtual PPP interface
Virtual-TokenRing Virtual TokenRing

```

HSRP uses a priority scheme to determine the default active router. The **active router** is assigned a **higher priority** than all the other HSRP-configured routers (the default priority is 100). It uses multicast messages to advertise priority among HSRP-configured routers. Thus,

if the active router fails to send these messages within a certain time (defined in the **timers** option), the standby router with the highest priority takes over.

Cisco Router Challenge 22

Outline

This challenge involves the configuration of a DHCP server on the router.

Objectives

The objectives of this challenge are to:

- Setup a DHCP server.
- Setup a DHCP Pool.
- Define DHCP networks and subnets.
- Define DHCP parameters, such as DNS, NetBios, Timeout and domain.

Example

```
> en
# config t
(config)# ip dhcpd pool wyoming
(config-dhcp)# network 249.189.108.0 255.255.255.254
(config-dhcp)# dns-server 249.189.108.58
(config-dhcp)# netbios-name-server 249.189.108.61
(config-dhcp)# lease 3
(config-dhcp)# default-router 249.189.108.87
(config-dhcp)# exit
(config)# ip dhcp ?
  conflict                DHCP address conflict parameters
  database                 Configure DHCP database agents
  excluded-address        Prevent DHCP from assigning certain addresses
  limited-broadcast-address Use all 1's broadcast address
  ping                     Specify ping parameters used by DHCP
  pool                     Configure DHCP address pools
  relay                     DHCP relay agent parameters
  smart-relay              Enable Smart Relay feature
(config)#ip dhcp excluded-address 249.189.108.26
(config)# ip dhcp ping ?
  packets Specify number of ping packets
  timeout Specify ping timeout
(config)# ip dhcp ping timeout 350
```

Cisco Router 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 login default local
(config)# username fred password bert
(config)# username fred1 password bert2
```

Cisco Router 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 Router 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 host 39.100.234.1
(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 Router Challenge 111

Outline

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

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 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
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)# 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 Router Challenge 112

Outline

This challenge involves the configuration of security of a router.

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 Router Challenge 113

Outline

This challenge involves the configuration Tacacs+ for accounting.

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 Router Challenge 114

Outline

This challenge involves the configuration of ATM.

Objectives

The objectives of this challenge are to:

- Define E0.
- Define ATM.
- Define bridge protocol.

Example

```
> enable
# config t
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shut
(config-if)# bridge-group 1
(config-if)# exit
(config)# int atm0
(config-if)# ?
Interface configuration commands:
  access-expression      Build a bridge boolean access expression
  apollo                 Apollo interface subcommands
  appletalk              Appletalk interface subcommands
  arp                    Set arp type (arpa, probe, snap) or timeout
```

atm	Modify ATM parameters
backup	Modify backup parameters
bandwidth	Set bandwidth informational parameter
bridge-group	Transparent bridging interface parameters
carrier-delay	Specify delay for interface transitions
cdp	CDP interface subcommands
class-int	Configure default vc-class name
clns	CLNS interface subcommands
crypto	Encryption/Decryption commands
custom-queue-list	Assign a custom queue list to an interface
decnet	Interface DECnet config commands
default	Set a command to its defaults
delay	Specify interface throughput delay
description	Interface specific description
dspu	Down Stream PU
exit	Exit from interface configuration mode
fair-queue	Enable Fair Queuing on an Interface
frs	DLC Switch Interface Command
help	Description of the interactive help system
hold-queue	Set hold queue depth
ip	Interface Internet Protocol config commands
ipv6	IPv6 interface subcommands
ipx	Novell/IPX interface subcommands
isis	IS-IS commands
iso-igrp	ISO-IGRP interface subcommands
lan-name	LAN Name command
lane	Modify LANE parameters
lat	LAT commands
llc2	LLC2 Interface Subcommands
load-interval	Specify interval for load calculation for an interface
locaddr-priority	Assign a priority group
logging	Configure logging for interface
loopback	Configure internal loopback on an interface
mac-address	Manually set interface MAC address
map-group	Configure static map group
max-reserved-bandwidth	Maximum Reservable Bandwidth on an Interface
mls	mls sub/interface commands
mpls	Configure MPLS interface parameters
mpoa	MPOA interface configuration commands
mtu	Set the interface Maximum Transmission Unit (MTU)
multilink-group	Put interface in a multilink bundle
multiring	Enable RIF usage for a routable protocol
netbios	Use a defined NETBIOS access list or enable name-caching
no	Negate a command or set its defaults
ntp	Configure NTP
priority-group	Assign a priority group to an interface
pvc	Configure ATM PVC parameters
random-detect	Enable Weighted Random Early Detection (WRED) on an Interface
rate-limit	Rate Limit
sap-priority	Assign a priority group
service-policy	Configure QoS Service Policy
shutdown	Shutdown the selected interface
smrp	Simple Multicast Routing Protocol interface subcommands
sna	SNA pu configuration
snapshot	Configure snapshot support on the interface
snmp	Modify SNMP interface parameters
source-bridge	Configure interface for source-route bridging
snmp	10BaseT 100 meter limit enforcement
sscop	SSCOP Interface Subcommands

```

standby                Interface HSRP configuration commands
svc                    Configure ATM SVC parameters
tag-switching          Tag Switching interface configuration commands
tarp                   TARP interface subcommands
timeout               Define timeout values for this interface
traffic-shape          Enable Traffic Shaping on an Interface or
                      Sub-Interface
transmit-interface     Assign a transmit interface to a receive-only
                      interface
vines                 VINES interface subcommands
xns                   XNS interface subcommands
(config-if)# mac-address 1111.2222.3333
(config-if)# dsl operating-mode auto
(config-if)# bridge-group 1
(config-if)# pvc ?
  <0-7>                Enter VPI/VCI value (slash required)
  <1-1023>             Enter VCI value
  WORD                 Optional handle to refer to this connection
(config-if)# pvc 8/35
(config-if-atm-vc)# ?
ATM virtual circuit configuration commands:
atm                   atm pvc commands
broadcast             Pseudo-broadcast
class-vc              Configure default vc-class name
default               Set a command to its defaults
dialer                set dialer pool this pvc belongs to
encapsulation         Select ATM Encapsulation for VC
exit-vc               Exit from ATM VC configuration mode
ilmi                  Configure ILMI management
inarp                 Change the inverse arp timer on the PVC
no                    Negate a command or set its defaults
oam                   Configure oam parameters
oam-pvc               Send oam cells on this pvc
pppoe-client          pppoe client
protocol              Map an upper layer protocol to this connection.
ubr                   Enter Unspecified Peak Cell Rate (pcr) in Kbps.
ubr+                  Enter Peak Cell Rate (pcr) Minimum Cell Rate (mcr) in Kbps.
vbr-nrt               Enter Variable Bit Rate (pcr) (scr) (bcs)
vcci                  VCC Identifier
(config-if-atm-vc)# encapsulation ?
  aal5ciscoppp         Cisco PPP over AAL5 Encapsulation
  aal5mux              AAL5+MUX Encapsulation
  aal5nlpid            AAL5+NLPID Encapsulation
  aal5snap             AAL5+LLC/SNAP Encapsulation
(config-if-atm-vc)# encapsulation aal5snap
(config-if-atm-vc)# exit
(config-if)# exit
(config)# bridge 1 protocol ieee

```

Explanation

In this case a bridge is created between the E0 and the ATM0 port. The encapsulation is aal5snap (AAL5 Link Control/Subnet Access Protocol) which supports multiple protocols over the same PVC.

Cisco Router Challenge 115

Outline

This challenge involves the configuration of ATM with a dialer interface and to encapsulate PPP within an Ethernet environment.

Objectives

The objectives of this challenge are to:

- Define a dialer
- Define ATM.

Example

```
> enable
# config t
(config)# int atm0
(config-if)# dsl operating-mode auto
(config-if)# pvc ?
  <0-7>      Enter VPI/VCI value(slash required)
  <1-1023>   Enter VCI value
  WORD      Optional handle to refer to this connection
(config-if)# pvc 8/35
(config-if-atm-vc)# ?
ATM virtual circuit configuration commands:
  atm          atm pvc commands
  broadcast    Pseudo-broadcast
  class-vc     Configure default vc-class name
  default      Set a command to its defaults
  dialer       set dialer pool this pvc belongs to
  encapsulation Select ATM Encapsulation for VC
  exit-vc      Exit from ATM VC configuration mode
  ilmi         Configure ILMI management
  inarp        Change the inverse arp timer on the PVC
  no           Negate a command or set its defaults
  oam          Configure oam parameters
  oam-pvc      Send oam cells on this pvc
  pppoe-client pppoe client
  protocol     Map an upper layer protocol to this connection.
  ubr          Enter Unspecified Peak Cell Rate (pcr) in Kbps.
  ubr+         Enter Peak Cell Rate(pcr)Minimum Cell Rate(mcr) in Kbps.
  vbr-nrt      Enter Variable Bit Rate (pcr) (scr) (bcs)
  vcci         VCC Identifier
(config-if-atm-vc)# pppoe-client dial-pool-number 1
(config-if-atm-vc)# exit
(config-if)# exit
(config)# int dialer0
(config-if)# ip address negotiated
(config-if)# encapsulation ppp
(config-if)# dialer pool 1
(config-if)# ip mtu 1492
(config-if)# ppp chap hostname newyork
(config-if)# ppp chap password default1
```

Explanation

PPPoE encapsulates PPP within an Ethernet frame.

Cisco Router Challenge 116

Outline

This challenge involves the configuration of PPPoA with NAT

Objectives

The objectives of this challenge are to:

- Define a dialer.
- Define ATM.

Example

```
> enable
# config t
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shut
(config-if)# exit
(config)# int atm0
(config-if)# dsl operating-mode auto
(config-if)# pvc 8/35
(config-if-atm-vc)# ?
ATM virtual circuit configuration commands:
 atm                atm pvc commands
 broadcast          Pseudo-broadcast
 class-vc           Configure default vc-class name
 default            Set a command to its defaults
 dialer             set dialer pool this pvc belongs to
 encapsulation      Select ATM Encapsulation for VC
 exit-vc            Exit from ATM VC configuration mode
 ilmi               Configure ILMI management
 inarp              Change the inverse arp timer on the PVC
 no                 Negate a command or set its defaults
 oam                Configure oam parameters
 oam-pvc            Send oam cells on this pvc
 pppoe-client       pppoe client
 protocol           Map an upper layer protocol to this connection.
 ubr                Enter Unspecified Peak Cell Rate (pcr) in Kbps.
 ubr+               Enter Peak Cell Rate (pcr) Minimum Cell Rate (mcr) in Kbps.
 vbr-nrt            Enter Variable Bit Rate (pcr) (scr) (bcs)
 vcci               VCC Identifier
(config-atm-vc)# encapsulation aal5mux ppp dialer
```

```

(config-atm-vc)# dialer pool member 1
(config-atm-vc)# exit
(config-if)# exit
(config)# int dialer0
(config-if)# ip address negotiated
(config-if)# encapsulation ppp
(config-if)# dialer pool 1
(config-if)# ppp chap hostname newyork
(config-if)# ppp chap password default1
(config-if)# exit
(config)# ip nat inside source list 10 interface dialer0 overload
(config)# access-list 10 permit 10.0.0.0 0.0.0.255
(config)# ip route 0.0.0.0 0.0.0.0 dialer0

```

Explanation

PPPoA encapsulates PPP within ATM cells.

Cisco Router Challenge 117

Outline

This challenge involves the configuration of ATM for VPDN.

Objectives

The objectives of this challenge are to:

- Define a dialer
- Define ATM.

Example

```

> enable
# config t
(config)# vpdn enable

(config)# vpdn-group ?
WORD VPDN Group name
(config)# vpdn-group test
(config-vpdn)# ?
VPDN group configuration commands:
accept-dialin VPDN accept-dialin group configuration
accept-dialout VPDN accept-dialout group configuration
default Set a command to its defaults
description Description for this VPDN group
exit Exit from VPDN group configuration mode
ip IP settings for tunnel
no Negate a command or set its defaults
redirect Call redirection options
request-dialin VPDN request-dialin group configuration

```

```

request-dialout  VPDN request-dialout group configuration
source          Configuration source for this vpdn-group
source-ip       Set source IP address for this vpdn-group
vpn            VPN ID/VRF name
(config-vpdn)# request-dialin ?
<cr>
(config-vpdn)# request-dialin

(config-vpdn-req-in)# ?
VPDN group request-dialin configuration commands:
default        Set a command to its defaults
dnis          Initiate a tunnel based on DNIS
domain        Initiate a tunnel based on domain name
exit          Exit from VPDN group request dialin sub-configuration mode
multihop      Initiate a multihop tunnel based on peer hostname or tunnel ID
no           Negate a command or set its defaults
protocol      Tunneling protocol to be used

(config-vpdn-req-in)# protocol ?
l2f          Use L2F
l2tp        Use L2TP
pptp        Use PPTP
pppoe       Use PPPoE
(config-vpdn-req-in)# protocol pppoe
(config-vpdn-req-in)# exit
(config-vpdn)# exit
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shut
(config-if)# exit
(config)# int atm0
(config-if)# ?
Interface configuration commands:
access-expression  Build a bridge boolean access expression
apollo            Apollo interface subcommands
appletalk         Appletalk interface subcommands
arp              Set arp type (arpa, probe, snap) or timeout
atm              Modify ATM parameters
backup           Modify backup parameters
bandwidth        Set bandwidth informational parameter
bridge-group     Transparent bridging interface parameters
carrier-delay    Specify delay for interface transitions
cdp             CDP interface subcommands
class-int       Configure default vc-class name
clns            CLNS interface subcommands
crypto          Encryption/Decryption commands
custom-queue-list Assign a custom queue list to an interface
decnet          Interface DECnet config commands
default         Set a command to its defaults
delay           Specify interface throughput delay
description      Interface specific description
dspu            Down Stream PU
exit            Exit from interface configuration mode
fair-queue      Enable Fair Queuing on an Interface
fras           DLC Switch Interface Command
help           Description of the interactive help system
hold-queue     Set hold queue depth
ip             Interface Internet Protocol config commands
ipv6          IPv6 interface subcommands
ipx           Novell/IPX interface subcommands
isis          IS-IS commands
iso-igrp      ISO-IGRP interface subcommands
lan-name      LAN Name command

```

lane	Modify LANE parameters
lat	LAT commands
llc2	LLC2 Interface Subcommands
load-interval	Specify interval for load calculation for an interface
locaddr-priority	Assign a priority group
logging	Configure logging for interface
loopback	Configure internal loopback on an interface
mac-address	Manually set interface MAC address
map-group	Configure static map group
max-reserved-bandwidth	Maximum Reservable Bandwidth on an Interface
mls	mls sub/interface commands
mpls	Configure MPLS interface parameters
mpoa	MPOA interface configuration commands
mtu	Set the interface Maximum Transmission Unit (MTU)
multilink-group	Put interface in a multilink bundle
multiring	Enable RIF usage for a routable protocol
netbios	Use a defined NETBIOS access list or enable name-caching
no	Negate a command or set its defaults
ntp	Configure NTP
priority-group	Assign a priority group to an interface
pvc	Configure ATM PVC parameters
random-detect	Enable Weighted Random Early Detection (WRED) on an Interface
rate-limit	Rate Limit
sap-priority	Assign a priority group
service-policy	Configure QoS Service Policy
shutdown	Shutdown the selected interface
smrp	Simple Multicast Routing Protocol interface subcommands
sna	SNA pu configuration
snapshot	Configure snapshot support on the interface
snmp	Modify SNMP interface parameters
source-bridge	Configure interface for source-route bridging
sqelch	10BaseT 100 meter limit enforcement
sscop	SSCOP Interface Subcommands
standby	Interface HSRP configuration commands
svc	Configure ATM SVC parameters
tag-switching	Tag Switching interface configuration commands
tarp	TARP interface subcommands
timeout	Define timeout values for this interface
traffic-shape	Enable Traffic Shaping on an Interface or Sub-Interface
transmit-interface	Assign a transmit interface to a receive-only interface
vines	VINES interface subcommands
xns	XNS interface subcommands

(config-if)# dsl operating-mode auto

(config-if)# pvc 8/35

(config-if-atm-vc)# ?

ATM virtual circuit configuration commands:

atm	atm pvc commands
broadcast	Pseudo-broadcast
class-vc	Configure default vc-class name
default	Set a command to its defaults
dialer	set dialer pool this pvc belongs to
encapsulation	Select ATM Encapsulation for VC
exit-vc	Exit from ATM VC configuration mode
ilmi	Configure ILMI management
inarp	Change the inverse arp timer on the PVC
no	Negate a command or set its defaults
oam	Configure oam parameters

```

oam-pvc          Send oam cells on this pvc
pppoe-client     pppoe client
protocol        Map an upper layer protocol to this connection.
ubr             Enter Unspecified Peak Cell Rate (pcr) in Kbps.
ubr+           Enter Peak Cell Rate(pcr)Minimum Cell Rate(mcr) in Kbps.
vbr-nrt        Enter Variable Bit Rate (pcr) (scr) (bcs)
vcci           VCC Identifier
(config-if-atm-vc)# pppoe-client dial-pool-number 1
(config-if-atm-vc)# exit
(config-if)# exit
(config)# int dialer0
(config-if)# ip address negotiated
(config-if)# encapsulation ppp
(config-if)# dialer pool 1
(config-if)# ip mtu 1492
(config-if)# ppp chap hostname newyork
(config-if)# ppp chap password default1

```

Cisco Router Challenge 118

Outline

This challenge involves the configuration of interactive PPP sessions.

Objectives

The objectives of this challenge are to:

- Define async parameters.
- Define line parameters.

Example

```

> enable
# config t
(config)# int async 6
(config-if)# encapsulation ppp
(config-if)# async ?
    default Specify default parameters
    dynamic Specify parameters which user may change
    mode Specify line mode (interactive or dedicated interface use)
(config-if)# async mode ?
    dedicated Line is dedicated as an async interface
    interactive Line may be switched between interactive use and async interface
(config-if)# async mode interactive
(config-if)# exit

```

```
(config)# line 1
(config-line)# autoselect ?
  arap          Set line to allow ARAP autoselection
  during-login  Do autoselect at the Username/Password prompt
  ppp           Set line to allow PPP autoselection
  slip          Set line to allow SLIP autoselection
  timeout       Set wait timeout for initial autoselect byte
  <cr>
(config-line)# autoselect ppp
(config-line)# autoselect during-login
```

Cisco Router Challenge 119

Outline

This challenge involves the configuration of interface addressing method for local devices.

Objectives

The objectives of this challenge are to:

- Define async parameters.
- Define loopback parameters.

Example

```
> enable
# config t
(config)# int loopback1
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# exit
(config)# int async 6
(config-if)# ip unnumbered loopback1
```

Cisco Router Challenge 120

Outline

This challenge involves the configuration of a specific address for the dial-in host.

Objectives

The objectives of this challenge are to:

- Define async parameters.
- Define the peer address.

Example

```
> enable
# config t
(config)# int async 6
(config-if)# peer default ip address 192.168.1.1
```

Explanation

In this example the access-server uses the Async 6 port for an asynchronous connection. Once it has connected it assigns the connected host with the IP address of 192.168.1.1 (Figure 1).

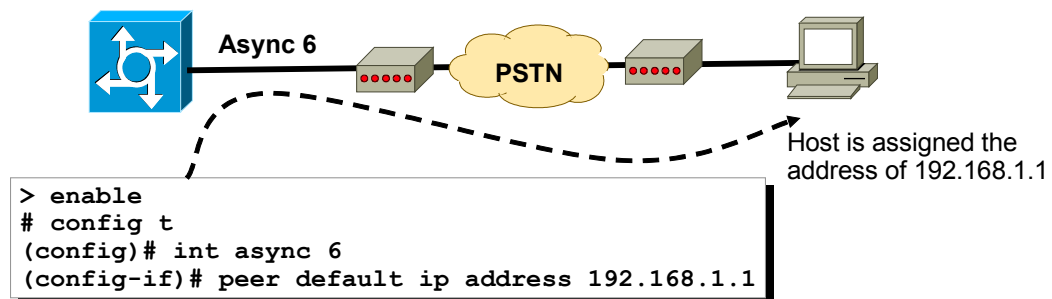


Figure 1: Host assigned a fixed IP address

Cisco Router Challenge 121

Outline

This challenge involves the configuration of the allocation of the address for the dial-in host using a local pool.

Objectives

The objectives of this challenge are to:

- Define async parameters.
- Define local pool of address for remote host.

Example

```
> enable
# config t
(config)# int async 6
(config-if)# peer default ip address pool testing
(config)# ip local pool testing 10.0.0.1 10.0.0.10
```

Explanation

In this example the access-server uses the Async 6 port for an asynchronous connection. Once it has connected it assigns the connected host with an IP address from the pool of addresses from 10.0.0.1 to 10.0.0.10 (see Figure 1).

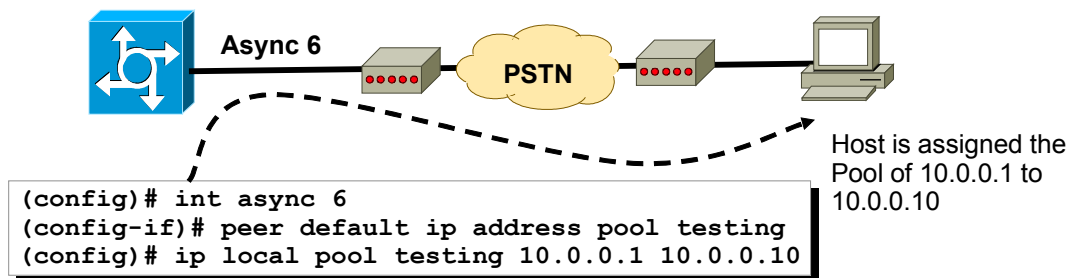


Figure 1: Host assigned an address from the local pool

Cisco Router Challenge 122

Outline

This challenge involves the configuration of DHCP allocation address for the dial-in host using a DHCP pool.

Objectives

The objectives of this challenge are to:

- Define async parameters.
- Define the peer address.
- Define a DHCP pool.

Example

```
> enable
# config t
(config)# int async 6
(config-if)# peer default ip address dhcp-pool wyoming
(config)# ip dhcpd pool wyoming
(config-dhcp)# network 249.189.108.0 255.255.255.254
(config-dhcp)# dns-server 249.189.108.58
(config-dhcp)# netbios-name-server 249.189.108.61
(config-dhcp)# lease 3
(config-dhcp)# default-router 249.189.108.87
(config-dhcp)# exit
(config)# ip dhcp ?
  conflict           DHCP address conflict parameters
  database           Configure DHCP database agents
  excluded-address   Prevent DHCP from assigning certain addresses
  limited-broadcast-address Use all 1's broadcast address
  ping               Specify ping parameters used by DHCP
  pool               Configure DHCP address pools
  relay              DHCP relay agent parameters
  smart-relay        Enable Smart Relay feature
(config)#ip dhcp excluded-address 249.189.108.26
(config)# ip dhcp ping ?
  packets  Specify number of ping packets
  timeout  Specify ping timeout
(config)# ip dhcp ping timeout 350
```

Explanation

In this example the access-server uses the Async 6 port for an asynchronous connection. Once it has connected it assigns the connected host with the IP address of taking from the dhcp pool (Figure 1).

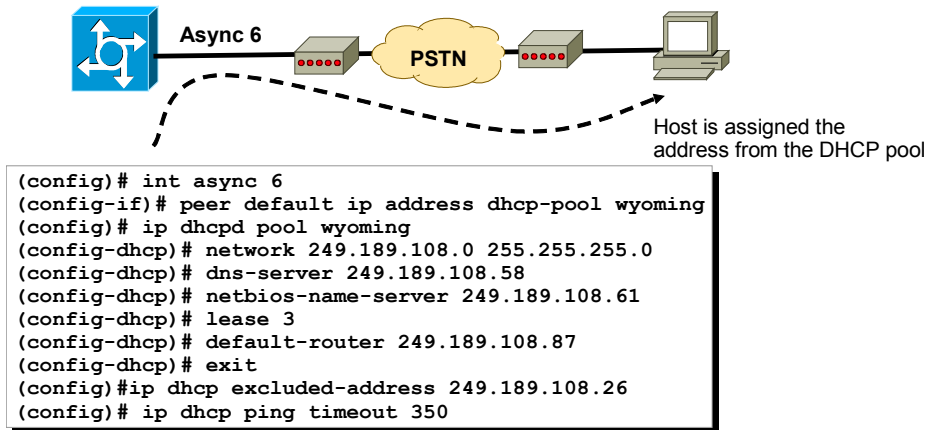


Figure 1: Host assigned an address from the DHCP server pool

Cisco Router Challenge 123

Outline

This challenge involves the configuration for PAP.

Objectives

The objectives of this challenge are to:

- Define async parameters.
- Define local address.
- Define PAP details.

Example

```

> enable
# config t
(config)# hostname edinburgh
(config)# username newyork password test
(config)# int async 6
(config-if)# encapsulation ppp
(config-if)# ppp authentication pap
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# dialer map ip 192.168.1.2 name newyork
(config-if)# ppp pap sent-username edinburgh password ttt

```

Explanation

In this example the username is set as the hostname of the remote device. Figure 1 shows an example configuration for two devices, on which either can connect to the other.

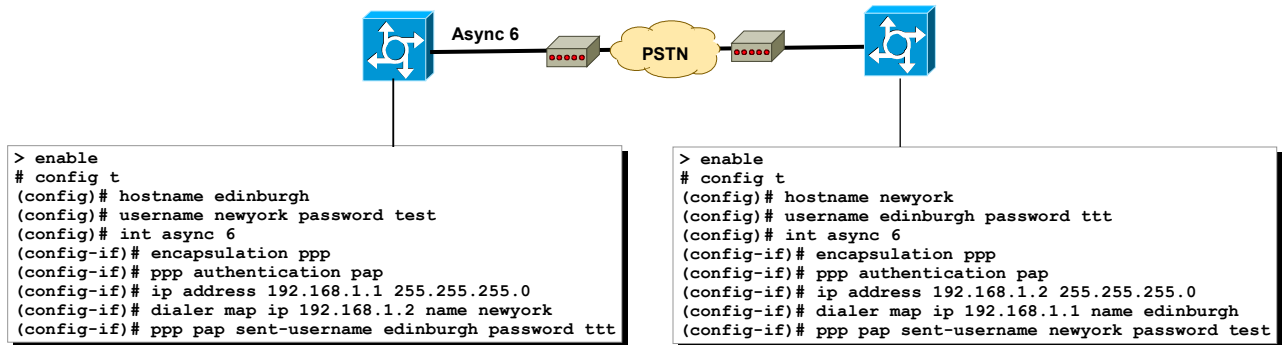


Figure 1: Host assigned an address from the DHCP server pool