

Remote Access

Cisco Router Challenge 29

Outline

This challenge involves the configuration of a modem connection.

Objectives

The objectives of this challenge are to:

- Setup line port.
- Define transport protocols.
- Define serial parameters.

Example

```
> en
# config t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# line ?
  <0-10>  First Line number
  aux     Auxiliary line
  console Primary terminal line
  tty     Terminal controller
  vty     Virtual terminal
(config)# line 3
(config-line)# transport ?
  input      Define which protocols to use when connecting to the terminal
             server
  output     Define which protocols to use for outgoing connections
  preferred  Specify the preferred protocol to use
(config-line)# transport input ?
  all       All protocols
  none      No protocols
  pad       X.3 PAD
  rlogin    Unix rlogin protocol
  telnet    TCP/IP Telnet protocol
(config-line)# transport input all
(config-line)# modem ?
  CTS-Alarm Alarm device which only uses CTS for call control
  DTR-active Leave DTR low unless line has an active incoming connection
             or EXEC
  Dialin    Configure line for a modern dial-in modem
  Host      Devices that expect an incoming modem call
  InOut     Configure line for incoming AND outgoing use of modem
  Printer   Devices that require DSR/CD active
```

```

    answer-timeout  Set interval between raising DTR and CTS response
    dtr-delay       Set interval during which DTR is held low
(config-line)# modem inout
(config-line)# login ?
    local          Local password checking
    tacacs         Use tacacs server for password checking
    <cr>
(config-line)# login local
(config-line)# speed ?
    <0-4294967295> Transmit and receive speeds
(config-line)# speed 2400

(config-line)# rotary ?
    <0-100>        Rotary group to add line to
(config-line)# rotary 4
(config-line)# flow ?
    NONE          Set no flow control
    hardware      Set hardware flow control
    software      Set software flow control
(config-line)# flow none
(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)# stopbits 1.5
(config-line)# modem dialin

```

Cisco Router Challenge 30

Outline

This challenge involves the configuration of a console server.

Objectives

The objectives of this challenge are to:

- Setup an Async interface.
- Define encapsulation.
- Define authentication.

Example

```

> en
# config t

```

```

(config)# int ?
  Async          Async interface
  BVI            Bridge-Group Virtual Interface
  CTunnel       CTunnel interface
  Dialer        Dialer interface
  FastEthernet  FastEthernet IEEE 802.3
  Group-Async   Async Group interface
  Loopback      Loopback interface
  MFR           Multilink Frame Relay bundle interface
  Multilink     Multilink-group interface
  Null          Null interface
  Serial        Serial
  Tunnel        Tunnel interface
  Vif           PGM Multicast Host interface
  Virtual       Virtual interface
  Virtual-Template Virtual Template interface
  Virtual-TokenRing Virtual TokenRing
  range         interface range command
(config)# int async ?
  <1-65> Async interface number
(config)# int async 5
(config-if)# encapsulation ?
  atm-dxi      ATM-DXI encapsulation
  frame-relay  Frame Relay networks
  hdlc         Serial HDLC synchronous
  lapb         LAPB (X.25 Level 2)
  ppp         Point-to-Point protocol
  smds        Switched Megabit Data Service (SMDS)
  x25         X.25
(config-if)# ppp authentication ?
  chap        Challenge Handshake Authentication Protocol (CHAP)
  ms-chap     Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
  pap         Password Authentication Protocol (PAP)
(config-if)# ppp authentication chap

```

Cisco Router Challenge 32

Outline

This challenge involves the configuration of a NAT.

Objectives

The objectives of this challenge are to:

- Enable Nat on the inside and outside.

Example

```
> en
```

```

# config t
(config)#ip nat ?
    inside      Inside address translation
    outside     Outside address translation
    pool        Define pool of addresses
    service     Special translation for application using non-standard port
    translation NAT translation entry configuration
(config)#ip nat inside
    destination Destination address translation
    source      Source address translation
(config)# ip nat inside ?
    destination Destination address translation
    source      Source address translation
(config)# ip nat inside source ?
    list        Specify access list describing local addresses
    route-map   Specify route-map
    static      Specify static local->global mapping
(config)# ip nat inside source static ?
    A.B.C.D     Inside local IP address
    esp         IPSec-ESP (Tunnel mode) support
    network     Subnet translation
    tcp         Transmission Control Protocol
    udp         User Datagram Protocol
(config)# ip nat inside source static 193.84.250.1 ?
    A.B.C.D     Inside global IP address
(config)# ip nat inside source static 193.84.250.1 195.151.136.5
(config)# int e0
(config-if)# ip nat ?
    inside     Inside interface for address translation
    outside    Outside interface for address translation
(config-if)# ip nat inside
(config-if)# int s0
(config-if)# ip nat outside

```

Cisco Router Challenge 37

Outline

This challenge involves the configuration of ISDN.

Objectives

The objectives of this challenge are to:

- Define an ACL.
- Implement a dialer-list.
- Define ISDN parameters.

Example

```

> en
# config t
(config)# access-list 2
(config)# access-list 2 permit host 168.86.68.8
(config)# access-list 2 deny host 206.207.17.5
(config)# access-list 2 permit 99.22.1.0 0.0.255.255
(config)# dialer-list ?
  <1-10> Dialer group number
(config)# dialer-list 39 ?
  protocol Permit or Deny based on protocols
(config)# dialer-list 39 protocol ?
  appletalk      AppleTalk
  bridge         Bridging
  clns           OSI Connectionless Network Service
  clns_es        CLNS End System
  clns_is        CLNS Intermediate System
  decnet         DECnet
  decnet_node    DECnet node
  decnet_router-L1 DECnet router L1
  decnet_router-L2 DECnet router L2
  hpr           HPR
  ip            IP
  ipx           Novell IPX
  llc2          LLC2
  netbios       NETBIOS
  vines         Banyan Vines
  xns           XNS
(config)# dialer-list 39 protocol ip ?
  deny      Deny specified protocol
  list      Add access list to dialer list
  permit    Permit specified protocol
(config)# dialer-list 39 protocol ip permit
(config)# dialer-list 39 protocol ipx permit
(config)# dialer-list 39
  protocol Permit or Deny based on protocols
(config)# dialer-list 39 protocol ?
  appletalk      AppleTalk
  bridge         Bridging
  clns           OSI Connectionless Network Service
  clns_es        CLNS End System
  clns_is        CLNS Intermediate System
  decnet         DECnet
  decnet_node    DECnet node
  decnet_router-L1 DECnet router L1
  decnet_router-L2 DECnet router L2
  hpr           HPR
  ip            IP
  ipx           Novell IPX
  llc2          LLC2
  netbios       NETBIOS
  vines         Banyan Vines
  xns           XNS
(config)# dialer-list 39 protocol ip
  deny      Deny specified protocol
  list      Add access list to dialer list
  permit    Permit specified protocol
(config)# dialer-list 39 protocol ip list
  <1-199>     IP access list
  <1300-2699> IP expanded access list
(config)# dialer-list 39 protocol ip list 2
(config)# isdn ?
  T310cisco-action Specify what action to take when T310cisco expires

```

```

T310cisco-timeout Specify ISDN VoIP timeout in milliseconds
leased-line       Sets a BRI interface to support leased lines on B & D
                  channels
switch-type       Select the ISDN switch type
tei-negotiation   Set when ISDN TEI negotiation should occur (global)
voice-call-failure Specify what cause code to emit when a voice call fails
                  with no specific cause code
(config)# isdn switch-type ?
  basic-1tr6      1TR6 switch type for Germany
  basic-5ess      Lucent 5ESS switch type for the U.S.
  basic-dms100    Northern Telecom DMS-100 switch type for the U.S.
  basic-net3      NET3 switch type for UK, Europe, Asia and Australia
  basic-ni        National ISDN switch type for the U.S.
  basic-qsig      QSIG switch type
  basic-ts013     TS013 switch type for Australia (obsolete)
  ntt             NTT switch type for Japan
  vn3            VN3 and VN4 switch types for France
  <cr>
(config)# isdn switch-type basic-dms100
(config)# int bri0
(config-if)# isdn ?
  answer1        Specify Called Party number and subaddress
  answer2        Specify Called Party number and subaddress
  autodetect     Enable the automatic spid detection
  caller         Specify incoming telephone number to be verified
  calling-number Specify Calling Number included for outgoing calls
  conference-code Specify a Conference Code
  disconnect-cause Specify cause code to return in call rejection to the
                  switch
  fast-rollover-delay Delay between fastrollover dials
  incoming-voice  Specify options for incoming calls.
  map            Specify E.164 address to numbering plan/type mapping
  not-end-to-end Specify speed when calls received are not isdn end to
                  end
  outgoing-voice Specify information transfer capability for voice calls
  overlap-receiving Specify if the interface will do Overlap Receiving
  send-alerting  Specify if Alerting message to be sent out before
                  Connect message
  sending-complete Specify if Sending Complete included in outgoing SETUP
                  message
  spid1         Specify Service Profile Identifier
  spid2         Specify Service Profile Identifier
  static-tei     Specify a Static TEI for ISDN BRI
(config-if)# isdn spid1 ?
  WORD spid1 string
(config-if)# isdn spid1 512790203500
(config-if)# isdn spid2 532790203500
(config-if)# encapsulation ?
  atm-dxi        ATM-DXI encapsulation
  frame-relay    Frame Relay networks
  hdlc           Serial HDLC synchronous
  lapb           LAPB (X.25 Level 2)
  ppp           Point-to-Point protocol
  smds          Switched Megabit Data Service (SMDS)
  x25           X.25
(config-if)# encapsulation ppp
(config-if)# ppp ?
  authentication Set PPP link authentication method
  bridge         Enable PPP bridge translation
  chap          Set CHAP authentication parameters
  ipcp          Set IPCP negotiation options
  lcp           PPP LCP configuration
  link          Set miscellaneous link parameters

```

```

max-bad-auth      Allow multiple authentication failures
multilink         Make interface multilink capable
pap              Set PAP authentication parameters
quality          Set minimum Link Quality before link is down
reliable-link    Use LAPB with PPP to provide a reliable link
timeout          Set PPP timeout parameters
use-tacacs       Use TACACS to verify PPP authentications
(config-if)# ppp authentication chap
(config-if)# dialer ?
callback-secure  Enable callback security
enable-timeout  Set length of time an interface stays down before it
                is available for dialing
fast-idle      Set idle time before disconnecting line with an
                unusually high level of contention
hold-queue       Configure output hold queue
idle-timeout     Specify idle timeout before disconnecting line
load-threshold  Specify threshold for placing additional calls
map             Define multiple dial-on-demand numbers
pool-member     Specify dialer pool membership
priority        Specify priority for use in dialer group
redial          Configure redial for this interface
rotary-group    Add to a dialer rotary group
snapshot        Enable snapshot address for dialer profile
string          Specify telephone number to be passed to DCE device
vpdn            Enable vpdn dial
wait-for-carrier-time How long the router will wait for carrier
watch-disable   Time to wait before bringing down watched route link
watch-group     Assign interface to dialer-watch-list
(config-if)# dialer fast-idle 30
(config-if)# dialer-group 39

```

Cisco Router Challenge 21

Outline

This challenge involves the configuration of AAA on the device.

Objectives

The objectives of this challenge are to:

- Define E0 settings.
- Enable AAA.
- Define AAA authentication.

Example

```

> en
# config t
(config)# aaa new-model
(config)# aaa authen logging def local

```

```
(config)# aaa authen ppp def none
(config)# aaa authen banner new york
(config)# aaa authen fail personal device
(config)# aaa author network default none
(config)# aaa author exec default none
```

Cisco Router Challenge 49

Outline

This challenge involves the configuration of a local AAA.

Objectives

The objectives of this challenge are to:

- Setup AAA parameters for local users.

Example

```
> en
# config t
(config)# aaa new-model
(config)# aaa authorization command 1 test local
(config)# aaa authorization network 1 test local
(config)# aaa authentication login default local-case
(config)# line con 0
(config-line)# login authentication default
(config-line)# line aux 0
(config-line)# login authentication default
(config-line)# line vty 0 15
(config-line)# login authentication default
(config-line)# exit
(config)# username ben password fries
(config)# username ben password yellow
```

Cisco Router Challenge 50

Outline

This challenge involves the configuration of AAA applied to an ISDN connection.

Objectives

The objectives of this challenge are to:

- Setup local AAA.
- Apply AAA onto an ISDN connection.

Example

```
> en
# config t
(config)# aaa new-model
(config)# aaa authorization command 1 test local
(config)# aaa authorization network 1 test local
(config)# aaa authentication login munich local
(config)# username ann password doghouse
(config)# username daniel password bravo
(config)# int bri0
(config-if)# encapsulation ppp
(config-if)# ppp authentication chap munich
```

Cisco Router Challenge 56

Outline

This challenge involves setting up a VPN.

Objectives

The objectives of this challenge are to:

- Enable IPsec.
- Define an IKE policy.
- Define the encryption for IKE.
- Define the authentication protocol for IKE.
- Define the authentication type.
- Define the Diffie-Hellman method.
- For pre-share, define the identity.
- For pre-share, define the key and the address.
- For pre-share, 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)# lifetime 10500
(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
```

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.

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)# encryption des
```

```
(config-isakmp)# hash sha
(config-isakmp)# authentication pre-share
(config-isakmp)# lifetime 10500
(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)# match address 109
(config-crypto-map)# set peer 192.168.1.1
(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
```

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 59

Outline

This challenge involves setting of CA.

Objectives

The objectives of this challenge are to:

- Generate a public and private key.
- Define CA.

Example

```
> en
# config t
(config)# hostname london
(config)# ip domain-name test.com
london (config)# crypto key generate rsa
london (config)# crypto ca identity idaho
  (ca-identity)# ?
Syntax: enrollment url [url]
Syntax: enrollment mode ra
Syntax: crl option
Syntax: query [url]

london (ca-identity)# enrollment url http://helpcert
london (ca-identity)# crl optional
london (ca-identity)# exit
(config)# crypto ca authenticate idaho
```

```
(config)# crypto ca enroll idaho
```

Cisco Router Challenge 36

Outline

This challenge involves the configuration of frame relay.

Objectives

The objectives of this challenge are to:

- Define frame-relay encapsulation.

Example

```
> en
# config t
(config)# int s0
(config-if)# ip address 196.85.163.9 255.255.192.0
(config-if)# no shutdown
(config-if)# encapsulation ?
  atm-dxi      ATM-DXI encapsulation
  frame-relay  Frame Relay networks
  hdlc         Serial HDLC synchronous
  lapb        LAPB (X.25 Level 2)
  ppp         Point-to-Point protocol
  smds        Switched Megabit Data Service (SMDS)
  x25         X.25
(config-if)# encapsulation frame-relay
(config-if)# frame-relay ?
  broadcast-queue  Define a broadcast queue and transmit rate
  class            Define a map class on the interface
  de-group         Associate a DE group with a DLCI
  interface-dlci   Define a DLCI on an interface/subinterface
  intf-type        Configure a FR DTE/DCE/NNI interface
  inverse-arp      Enable/disable inverse ARP on a DLCI
  ip               Frame Relay Internet Protocol config commands
  lapf            set LAPF parameter
  lmi-n391dte      set full status polling counter
  lmi-n392dce      LMI error threshold
  lmi-n392dte      LMI error threshold
  lmi-n393dce      set LMI monitored event count
  lmi-n393dte      set LMI monitored event count
  lmi-t392dce      set DCE polling verification timer
```

```

lmi-type          Use CISCO-ANSI-CCITT type LMI
local-dlci       Set source DLCI when LMI is not supported
map              Map a protocol address to a DLCI address
multicast-dlci   Set DLCI of a multicast group
priority-dlci-group Define a priority group of DLCIs
qos-autosense    enable QoS autosense
route            frame relay route for pvc switching
svc             Enable frame relay SVCs
traffic-shaping  Enable Frame Relay Traffic Shaping
traps-maximum   set max traps FR generates at link up or when getting
                LMI Full Status message
(config-if)# frame-relay map ?
  bridge Bridging
  ip      IP
  ipx     Novell IPX
  llc2    llc2
(config-if)# frame-relay map ip ?
  A.B.C.D Protocol specific address
(config-if)# frame-relay map ip 196.85.163.14 ?
  <16-1007> DLCI
(config-if)# frame-relay map ip 196.85.163.14 102 ?
  broadcast Broadcasts should be forwarded to this address
  cisco      Use CISCO Encapsulation
  compress   Enable TCP/IP and RTP/IP header compression
  ietf       Use RFC1490/RFC2427 Encapsulation
  nocompress Do not compress TCP/IP headers
  payload-compression Use payload compression
  rtp        RTP header compression parameters
  tcp        TCP header compression parameters
  <cr>
(config-if)# frame-relay map ip 196.85.163.14 102 broadcast
(config-if)# frame-relay map ip 196.85.163.17 103 broadcast
(config-if)# ip ospf ?
  authentication Enable authentication
  authentication-key Authentication password (key)
  cost            Interface cost
  database-filter Filter OSPF LSA during synchronization and flooding
  dead-interval  Interval after which a neighbor is declared dead
  demand-circuit OSPF demand circuit
  hello-interval Time between HELLO packets
  message-digest-key Message digest authentication password (key)
  mtu-ignore     Ignores the MTU in DBD packets
  network        Network type
  priority        Router priority
  retransmit-interval Time between retransmitting lost link state
                  advertisements
  transmit-delay Link state transmit delay
(config-if)# ip ospf network ?
  broadcast Specify OSPF broadcast multi-access network
  non-broadcast Specify OSPF NBMA network
  point-to-multipoint Specify OSPF point-to-multipoint network
  point-to-point Specify OSPF point-to-point network
(config-if)# ip ospf network point-to-multipoint

```

Cisco Router Challenge 63

Outline

This challenge involves the configuration of frame relay.

Objectives

The objectives of this challenge are to:

- Define frame relay.
- Define encapsulation for frame-relay.
- Define a mapping.
- Define an LMI type.

Example

```
> en
# config t
(config)# int s0
(config-if)# ip address 62.250.1.7 255.0.0.0
(config-if)# no shut
(config-if)# encapsulation ?
  atm-dxi      ATM-DXI encapsulation
  frame-relay  Frame Relay networks
  hdlc         Serial HDLC synchronous
  lapb        LAPB (X.25 Level 2)
  ppp         Point-to-Point protocol
  smds        Switched Megabit Data Service (SMDS)
  x25         X.25
(config-if)# encapsulation frame-relay
(config-if)# frame-relay map ip 62.250.1.12 ?
  <16-1007>   DLCI
(config-if)# frame-relay map ip 62.250.1.12 102
  broadcast   Broadcasts should be forwarded to this address
  cisco       Use CISCO Encapsulation
  compress    Enable TCP/IP and RTP/IP header compression
  ietf        Use RFC1490/RFC2427 Encapsulation
  nocompress  Do not compress TCP/IP headers
  payload-compression Use payload compression
  rtp         RTP header compression parameters
  tcp         TCP header compression parameters
  <cr>
(config-if)# frame-relay map ip 62.250.1.12 102 broadcast
(config-if)# frame-relay map ip 62.250.1.15. 103 broadcast
(config-if)# frame-relay ?
  broadcast-queue Define a broadcast queue and transmit rate
  class           Define a map class on the interface
  de-group        Associate a DE group with a DLCI
  interface-dlci  Define a DLCI on an interface/subinterface
  intf-type       Configure a FR DTE/DCE/NNI interface
  inverse-arp     Enable/disable inverse ARP on a DLCI
  ip              Frame Relay Internet Protocol config commands
  lapf           set LAPF parameter
```

```

lmi-n391dte      set full status polling counter
lmi-n392dce      LMI error threshold
lmi-n392dte      LMI error threshold
lmi-n393dce      set LMI monitored event count
lmi-n393dte      set LMI monitored event count
lmi-t392dce      set DCE polling verification timer
lmi-type         Use CISCO-ANSI-CCITT type LMI
local-dlci       Set source DLCI when LMI is not supported
map              Map a protocol address to a DLCI address
multicast-dlci   Set DLCI of a multicast group
priority-dlci-group Define a priority group of DLCIs
qos-autosense    enable QOS autosense
route            frame relay route for pvc switching
svc              Enable frame relay SVCs
traffic-shaping  Enable Frame Relay Traffic Shaping
traps-maximum    set max traps FR generates at link up or when getting
                  LMI Full Status message
(config-if)# frame-relay lmi-type ?
    cisco
    ansi
    q933a
(config-if)# frame-relay lmi-type ansi

```

Ref

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/wan_c/wcdfrely.htm

Cisco Router Challenge 64

Outline

This challenge involves the configuration of frame relay for traffic shaping.

Objectives

The objectives of this challenge are to:

- Define a map class.
- Define traffic rates.
- Define adaptive –shaping.
- Define a priority-group.
- Apply map class to an interface.

Example

```
> en
# config t
(config)# map-class frame kirkcaldy
(config-map-class)# frame-relay traffic ?
    <600-45000000> Committed Information Rate (CIR)
(config-map-class)# frame-relay traffic 9600 ?
    <0-45000000> Peak rate (CIR + EIR)
    <cr>
(config-map-class)# frame-relay traffic 9600 18000
(config-map-class)# frame-relay adaptive-shaping ?
    becn          Enable rate adjustment in response to BECN
    foresight     Enable rate adjustment in response to ForeSight messages and BECN
(config-map-class)# frame-relay adaptive-shaping becn
(config-map-class)# frame-relay priority-group 3
(config-map-class)# exit
(config)# int s0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# encapsulation frame-relay
(config-if)# frame-relay traffic-shaping
(config-if)# frame-relay class kirkcaldy
```

Explanation

Traffic shaping controls the traffic going out of an interface, and should match the flow of traffic to the required rate at which the remote device wishes to receive the data. The commands used include:

```
frame-relay adaptive-shaping [becn | foresight]1
```

Select either BECN or ForeSight as the congestion backward-notification mechanism to which traffic shaping will adapt.

```
frame-relay traffic-shaping
```

Enable Frame Relay traffic shaping and per-VC queueing.

```
frame-relay traffic-rate average [peak]
```

Define the traffic rate for the map class.

```
frame-relay priority-group list-number
```

Specify a priority queue list.

```
map-class frame-relay map-class-name
```

Specify a map class to define.

Ref:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart4/qcfrts.htm

Cisco Router Challenge 65

Outline

This challenge involves the configuration of frame relay for traffic shaping for queuing.

Objectives

The objectives of this challenge are to:

- Define a map class.
- Define traffic rates.
- Define adaptive-shaping.
- Define a priority-group.
- Apply map class to an interface.

Example

```
# config t
(config)# map-class frame-relay ion
(config-map-class)# frame-relay priority-group 37
(config-map-class)# exit
(config)# priority-list 37 protocol ip normal
(config)# priority-list 37 default ?
    high
    medium
    normal
    low
(config)# priority-list 37 default medium
(config)# int s0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# encapsulation frame-relay
(config-if)# frame-relay traffic-shaping
(config-if)# frame-relay class kirkcaldy
```

Explanation

With **priority queuing** the traffic is prioritized using a priority-list, and the priority-group command within the class-map defines which priority-list to use. These queues are: high, medium, normal, or low priority. Thus, the router searches in the high queue first, and

transmit these packets before the other queues, and so on. Thus the high priority traffic is defined as traffic which must go, no matter what, while other traffic can be dropped.

To configure priority the following protocol is used:

```
priority-list list-number protocol protocol-name {high | medium | normal | low} queue-keyword keyword-value
```

where

- Protocol classifies the traffic. It is typically IP, but can be IPX, AppleTalk, and so on.
- List-number defines that all statements use the same policy, and can range from 1 to 16.
- Queue-keyword can be one of: fragments, gt, lt, list, tcp, and udp.
- Keyword-value specifies the port for TCP or UDP.

The default queue for all other traffic can then be specified with:

```
priority-list list-number default {high | medium | normal | low}
```

Ref

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b75b0.html

Cisco Router Challenge 66

Outline

This challenge involves the configuration of frame relay for priority queuing.

Objectives

The objectives of this challenge are to:

- Define an access-list to define the traffic for queuing.
- Define a map class.
- Define a queue list.

Example

```

# config t
> en
# config t
(config)# access-list 100 permit tcp 215.78.24.0 255.255.0.0 97.49.56.0
                               255.255.0.0 eq smtp

(config)# map-class frame-relay ion
(config-map-class)# frame-relay priority-group 37
(config-map-class)# exit
(config)# queue-list ?
  <1-16> Queue list number
(config)# queue-list 13 ?
  default          Set custom queue for unspecified datagrams
  interface        Establish priorities for packets from a named interface
  lowest-custom    Set lowest number of queue to be treated as custom
  protocol         priority queueing by protocol
  queue           Configure parameters for a particular queue
  stun            Establish priorities for stun packets
(config)# queue-list 13 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)# queue-list 13 protocol ip ?
  <0-16> queue number
(config)# queue-list 13 protocol ip 1 ?
  fragments  Prioritize fragmented IP packets
  gt        Classify packets greater than a specified size
  list     To specify an access list
  lt        Classify packets less than a specified size
  tcp      Prioritize TCP packets 'to' or 'from' the specified port
  udp      Prioritize UDP packets 'to' or 'from' the specified port
  <cr>
(config)# queue-list 13 protocol ip 1 list ?
  <1-199>      IP access list
  <1300-2699> IP expanded access list
(config)# queue-list 13 protocol ip 1 list 100

(config)# queue-list 13 queue 1 byte-count 1000 limit 2
(config)# queue-list 13 queue 2 byte-count 700 limit 20
(config)# queue-list 13 default 2

(config)# int s0
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# encapsulation frame-relay
(config-if)# frame-relay traffic-shaping
(config-if)# frame-relay class kirkcaldy

```

Explanation

This example uses two queues, which are identified by an ACL (in this case they are the same, but normally they would have different ACLs). For example the first queue is matched to the ACL with a number of 100:

```
queue-list 13 protocol ip 1 list 100
```

The following command defines that queue 1 has a byte-count limit of 1000 bytes and that there is a maximum of two packets in the queue:

```
queue-list 13 queue 1 byte-count 1000 limit 2
```

Ref:

http://www.cisco.com/en/US/products/hw/switches/ps1893/products_command_reference_chapter09186a008007dec9.html

Cisco Router Challenge 67

Outline

This challenge involves the configuration of backup routes.

Objectives

The objectives of this challenge are to:

- Define a backup interface.
- Define the backup timings.

Example

```
> en
# config t
(config)# int s0
(config-if)# ip address 139.202.25.3 255.255.255.240
(config-if)# no shut
(config-if)# backup ?
  delay      Delays before backup line up or down transitions
  interface  Configure an interface as a backup
  load       Load thresholds for line up or down transitions
(config-if)# backup interface ?
  Async      Async interface
  BRI        ISDN Basic Rate Interface
  BVI        Bridge-Group Virtual Interface
```

```

Dialer          Dialer interface
FastEthernet    FastEthernet IEEE 802.3
Group-Async     Async Group interface
Lex             Lex interface
Loopback        Loopback interface
Multilink       Multilink-group interface
Null            Null interface
Serial          Serial
Tunnel          Tunnel interface
Virtual-Template Virtual Template interface
Virtual-TokenRing Virtual TokenRing
Vlan            Catalyst Vlans
(config-if)# backup interface bri0
(config-if)# backup delay ?
<0-4294967294> Seconds
never          Never activate the backup line
(config-if)# backup delay 52 ?
<0-4294967294> Seconds
never          Never deactivate the backup line
(config-if)# backup delay 52 83
(config-if)# backup load 86 68

```

Remember to check that the BRI0 interface is now a backup, such as:

```

# sh interface bri0
BRI0 is standby mode, line protocol is down
Hardware is PQUICC BRI with U interface
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/0/16 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions

```

Explanation

A backup route is important to provide resilience. The following defines that the BRI0 interface will be the backup route:

```

backup interface bri0

```

Then to activate the backup after 52 seconds of the primary line being in active, and for the secondary to backup after 83 seconds of the primary line being re-activated, the following command is used:

```
backup delay 52 83
```

When loading is used, the following defines that the backup route becomes active when at 86% of the full load, and deactivates at 68% of full load:

```
backup load 86 68
```

Ref:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_reference_chapter09186a00800ca527.html

Cisco Router Challenge 68

Outline

This challenge involves the configuration of Weighted Fair Queues.

Objectives

The objectives of this challenge are to:

- Define a frame-relay encapsulation
- Define congestion discard threshold.
- Define bandwidth on interface.

Example

```
> en
# config t
(config)# int s0
(config-if)# encapsulation frame-relay
(config-if)# fair-queue 128
(config-if)# bandwidth 100
(config-if)# exit
(config)# exit
```

Remember to check that queuing is applied:

```
# sh int s0
```

```
Serial0 is down, line protocol is down
Hardware is PowerQUICC Serial
Internet address is /0
MTU 1500 bytes, BW 100 Kbit, DLY 20000 usec,
  reliability 128/255, txload 1/255, rxload 1/255
Encapsulation frame-relay, loopback not set
Keepalive set (10 sec)
Last input 03:56:59, output 00:00:06, output hang never
Last clearing of "show interface" counters 6d07h
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/2/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  63247 packets input, 3952974 bytes, 0 no buffer
  Received 61877 broadcasts, 0 runts, 535 giants, 0 throttles
  2571 input errors, 138 CRC, 1456 frame, 0 overrun, 0 ignored, 743
abort
  64668 packets output, 4136835 bytes, 0 underruns
  0 output errors, 0 collisions, 474 interface resets
  0 output buffer failures, 0 output buffers swapped out
  952 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```

Ref:

<http://www.opalsoft.net/qos/WhyQos-2424.htm>

Cisco Router Challenge 69

Outline

This challenge involves the configuration of CBWFQ.

Objectives

The objectives of this challenge are to:

- Define CBWFQ.

Example

```
> en
# config t
(config)# access-list 108 permit ip 162.78.102.0 0.0.255.255 247.226.90.0
0.0.255.255
(config)# class-map tayside
```

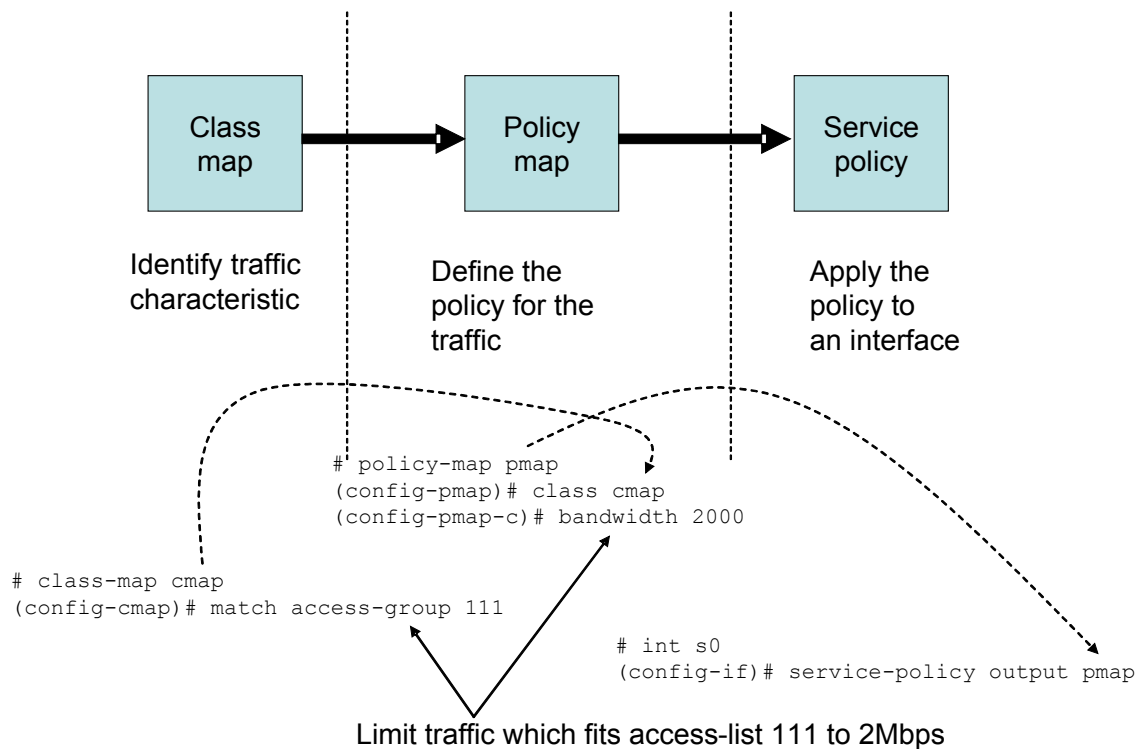
```

(config-cmap)# match access-group 108
(config-cmap)# exit
(config)# policy-map ankle
(config-pmap)# class tayside
(config-pmap-c)# bandwidth 128
(config-pmap-c)# queue-limit 21
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output ankle

```

Explanation

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



Ref:

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

Cisco Router Challenge 70

Outline

This challenge involves the configuration of dynamic NAT.

Objectives

The objectives of this challenge are to:

- Define a dynamic NAT pool.
- Define an access-list to identify the traffic to be translated.
- Apply NAT on E0 and S0 interfaces.

Example

```
> en
# config t
(config)# access-list 7 permit 195.11.220.0 31.255.255.255
(config)# ip nat pool mynatpool 150.122.41.150 150.122.41.99 netmask
255.255.255.0
  (config)# ip nat inside source list 7 pool mynatpool
(config)# int e0
(config-if)# ip nat inside
(config-if)# int s0
(config-if)# ip nat outside
```

Cisco Router Challenge 71

Outline

This challenge involves the configuration of dynamic NAT.

Objectives

The objectives of this challenge are to:

- Define three static NAT mappings.
- Apply NAT on E0 and S0 interfaces.

Example

```
> en
# config t
(config)# ip nat inside source static 160.94.210.50 93.123.33.13
(config)# ip nat inside source static 160.94.210.53 93.123.33.15
(config)# ip nat inside source static 160.94.210.55 93.123.33.18
(config)# int e0
(config-if)# ip nat inside
```

```
(config-if)# int s0
(config-if)# ip nat outside
```

Explanation

In this case the lines:

```
(config)# ip nat inside source static 160.94.210.50 93.123.33.13
(config)# ip nat inside source static 160.94.210.53 93.123.33.15
(config)# ip nat inside source static 160.94.210.55 93.123.33.18
```

defines that a host with the address of 160.94.210.50 will be viewed from the outside of the network as 93.123.33.13. Thus, for example, if the host at 160.94.210.50 is a Web server, users from outside the network will access it using the address of 93.123.33.13. Normally servers which have public access have a static mappings as this allows them to be accessed through the static mapping.

Theory

Network address translation (NAT) is defined in RFC1631, and swaps one network address with another. This allows private networks (RFC1918) to be created, which are then translated to public address when they access the Internet. A router can operate at the border of a domain and translate addresses from private to public, and vice-versa. For example, a node could be given a private address of 192.168.10.12. The NAT could then translate this to a public address of 168.10.34.31. The NAT table would then have the mapping of:

Private	Public
192.168.10.12	168.10.34.21

If a host from outside the domain sends a data packet back to the domain, the NAT will translate the public address back into the private address. These translations can be statically assigned, such as where it is setup with a permanent mapping, or dynamically, where the tables can change as the network requires. Figure 1 gives an example, where the destination address is 11.22.33.44. The address in this case is changed from 192.168.10.12 to 168.10.34.21, as the data packet goes out of the domain, and is changed back when it comes back into the domain.

PAT (Port address translation)

NAT routers can use port address translation (PAT), which allows many internal address to be mapped to the same global address. This is also named as a *many-to-one* NAT, or address overloading. With PAT, the NAT router keeps a track of the connections, and the TCP/UDP ports that are being used. The NAT router then changes the global address back into a private address based on these. In Figure 2 there is a single external address (168.10.34.21),

but multiple **source** ports are used to identify the connection. It can be seen in the example in Figure 3 that a host has four different connections with a WWW server, and each of the connections have been mapped to a unique source port (5555, 5556, 5557 and 5558).

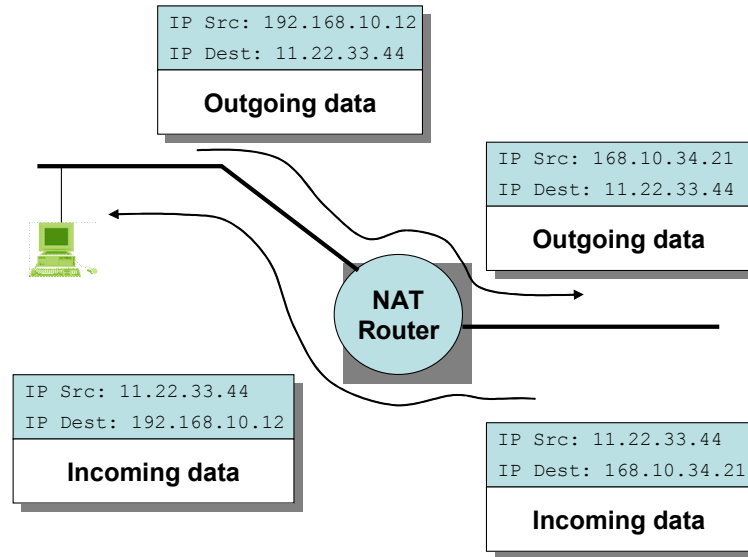
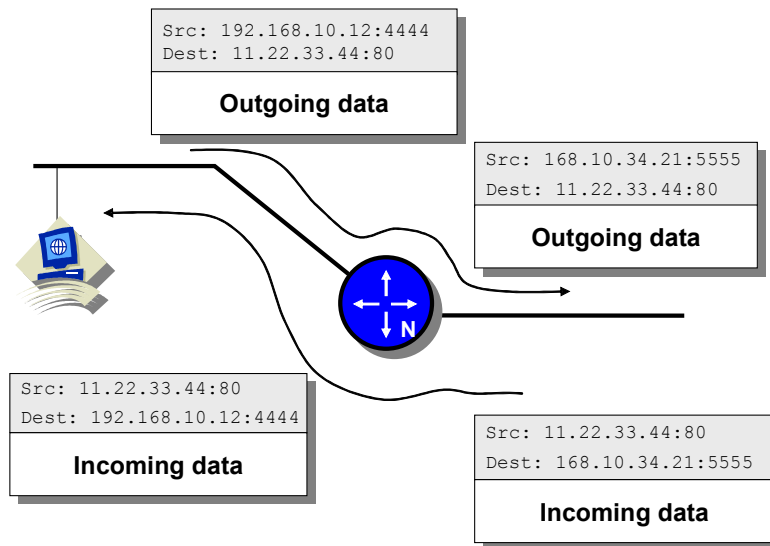


Figure 1 Example of NAT

In summary the advantages of NAT are:

- Hides the network addresses of the network.
- Bars direct contact with a host.
- Increased range of address.
- Allow easy creation of subnetworks.



PAT (Port address translation) – Maps many addresses to one global address.

Figure 2 Example of port address translation (PAT)

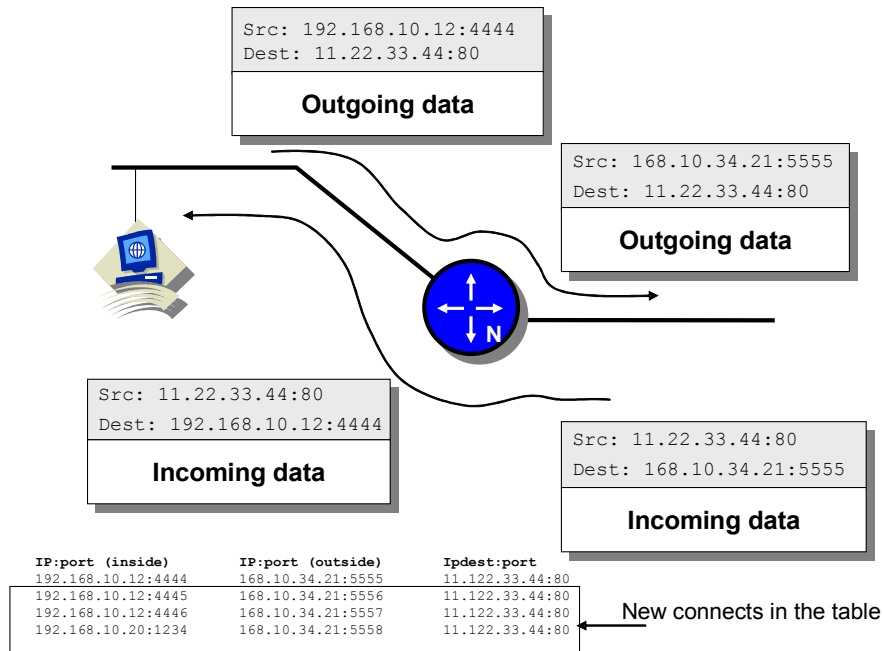
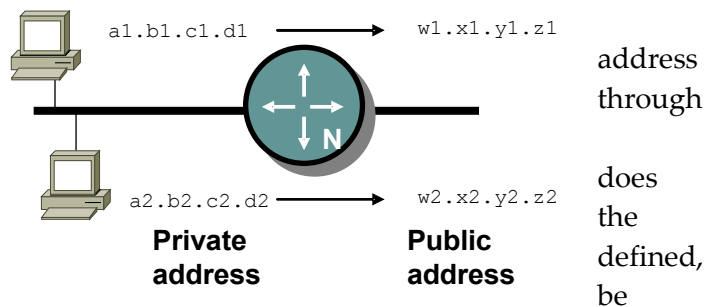


Figure 3 Example of port address translation (PAT)

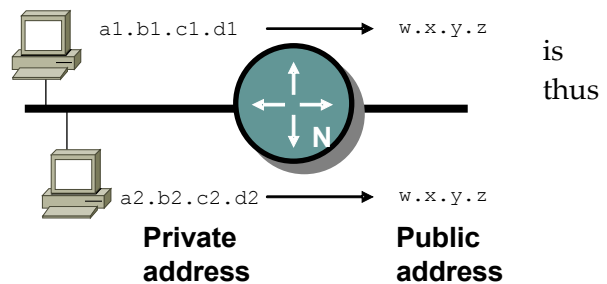
NAT types

The three main types of NAT are:

- **Static translation.** Each public IP translates to a private one a static table. It is good for security/ logging/ traceability, but not hide the internal network. As network addresses are statically the nodes inside the network can be contacted directly from outside. Static translation also does not save in network addresses, although an organisation may limit access by limiting the number of private addresses which are available.



- **IP Masquerading (Dynamic Translation).** A single public IP address is used for the whole network. The table is dynamic, and uses TCP ports to identify connections. It has the advantage that a complete network requires only a single public address, but, of course, the network which is allocated with private addresses is dependent upon the NAT device for its connection to external networks.



- **Load Balancing Translation.** With this, a request is made to a resource, such as to a WWW server, the NAT device then looks at the current loading of the systems, and forwards the request to the one which is most lightly used (Figure 4).

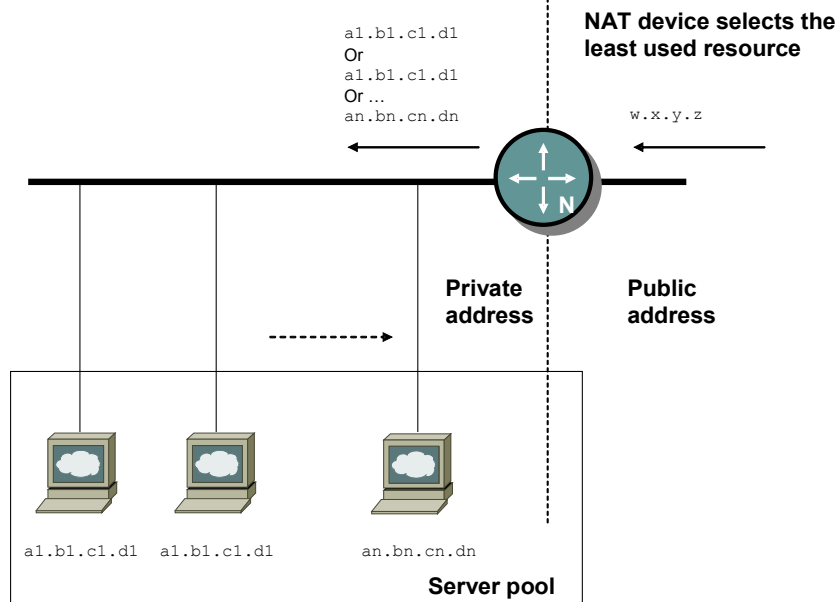


Figure 4 Load balancing translation

NAT backtracking

Dynamic NAT is good at isolating the external network from a public *untrusted* network, as it allows the NAT device to create a table of connections which have been initiated from inside. Thus external devices cannot contact hosts as they cannot be mapped into in the NAT device. Unfortunately some applications, such as FTP and IRC, require a server connection to be setup on the host. Thus the NAT device must be able to implement backtracking of connections, as illustrated in Figure 5.

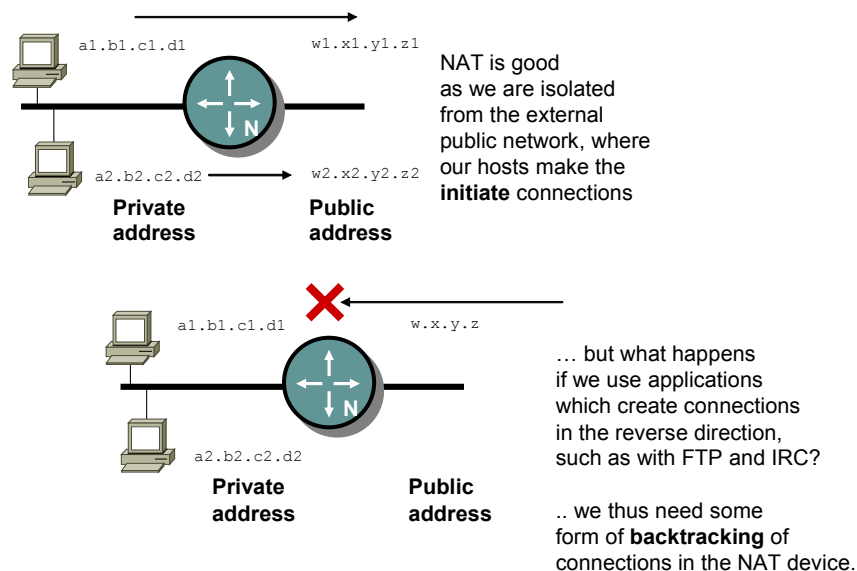


Figure 5 NAT backtracking

NAT weaknesses

Static NAT is poor for security, as it does not hide the network. This is because there is a one-to-one mapping, and external nodes can thus connect to internal devices. It also does not hide the host from the external network, so that it can be traced, if the mapping table is known. **Dynamic NAT** is much better for security, as it hides the network. Unfortunately it has two major weaknesses:

- *Backtracking* allows external parties to trace back a connection.
- If the NAT device becomes compromised the external party can redirect traffic.

These weaknesses are illustrated in Figure 5.

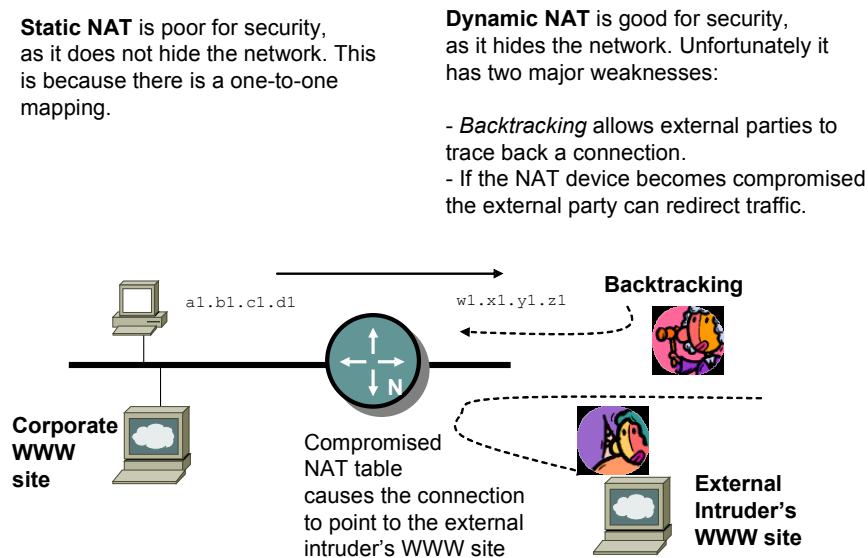


Figure 5 NAT weaknesses

Programming dynamic NAT

Network address translation allows private IP address to be translated to public address. This can either be achieved statically, where the translation is fixed by a translation table, or can be dynamic, where the translation table is set-up as required by the network. Typically, a global address pool is used from which the public addresses are taken. The command for this has the format of:

```
RouterA# config t
RouterA(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length
prefix-length}
```

where the submask length is defined by the optional `netmask` argument (such as 255.255.255.0), or by a length using `prefix-length` (or 24 for the 255.255.255.0 subnet mask).

After this, the types of packets which will be translated will be defined. This is achieved with the access-list command, and has the form:

```
RouterA# config t
RouterA(config)#access-list access-list-number permit source [source-wildcard]
```

A dynamic translation uses the `ip nat inside source list` command, such as:

```
Router(config)#ip nat inside source list access-list-number pool name
```

where the access list number is defined. This is then applied to one of the interfaces using the command (for s0):

```
RouterA# config t
RouterA (config) # int s0
RouterA(config-if)#ip nat inside
```

This will translate data packets which are coming into the port. To translate outgoing one, the `ip nat outside` command is used.

For example, to define a pool of addresses from 180.10.11.1 to 180.10.11.254:

```
RouterA(config)#ip nat pool org_pool 180.10.11.1 180.10.11.254 netmask 255.255.255.0
```

which defines the global addresses as `org_pool`. This will be used to send translated data packets out in the Internet. An `access-list` command is then used to match the translation addresses:

```
RouterA(config)#access-list 2 permit 192.168.10.0 0.0.0.255
RouterA(config)#ip nat inside source list 2 pool org_pool
```

which applies the access-list number 2 to the IP NAT pool of `org_pool`. This can then be applied to the interfaces with:

```
RouterA(config)#interface e0
RouterA(config-if)#ip nat inside
RouterA(config-if)#interface s0
RouterA(config-if)#ip nat outside
```

Thus if a host with an address of 192.168.10.10 sends a data packet out of the network, it will have one of the addresses from the pool, such as 180.10.11.1. All the hosts outside the network will use the address from the pool to communicate with the node. By default, these entries remain in the table for up to 24 hours (in order to allow communications to return). The time-out can be changed using the command:

```
RouterA(config)#ip nat translation timeout seconds
```

This is an important factor, especially when there is a large number of hosts which can only use a limited pool of addresses. A lower time-out will allow an address to be released, so that another node can use it.

NAT also enhances security as it limits external users in their connection to local network, as the translations of addresses will not be permanent (unless a static translation is implemented). NAT thus hides the topology of the network.

Static translation uses a fixed lookup table to translate the addresses, where each address which requires an Internet address has a corresponding public IP address. If it is used on its own, it cannot thus preserve IP address. Thus, typically the two methods are used, where important nodes, such as servers, will have a static entry, as this guarantees them an address, while other nodes, which are less important, will be granted a dynamic translation. This also aids security as the important devices can run enhanced security and monitoring software, which might not be possible on lower-level devices, which are typically administered on a daily basis by non-IT personnel.

Static addresses are also useful in translating network topologies from one network address structure to another, or even when individual nodes are moved from one subnet to another.

An example of configuring for static addresses of a node of 192.168.10.10 to the address of 180.10.11.1:

```
RouterA(config)#ip nat inside source static 192.168.10.10 180.10.11.1
```

This can this be applied to the inside and outside interfaces with:

```
RouterA(config)#interface e0
RouterA(config-if)#ip nat inside
RouterA(config-if)#interface s0
RouterA(config-if)#ip nat outside
```

NAT allows organisations to quickly remap their addresses, as conditions require, such as changing Internet access provider, or to respond to a network breach.

One of the advanced features of NAT routers is their ability to use Port Address Translation (PAT), which allows multiple inside addresses to map to the same global address. This is sometimes called a *many-to-one* NAT, or *address overloading*. With address overloading, many private addressed nodes can access the Internet using a single global address. The NAT router keeps track of the different conversations by mapping TCP and UDP port numbers in the translation table. A translation entry is one which maps one IP address and port pair to another, and is called an extended *table entry*. This table will match internal private IP addresses and ports, to the global address.

The NAT command is used to configure PAT with:

```
RouterA(config)#ip nat inside source list access-list-number pool name overload
```

For example, if a network has 20 IP global addresses from 180.10.11.1 to 180.10.11.20, then the router could be configured with:

```
RouterA(config)#ip nat pool org_pat_pool 180.10.11.1 180.10.11.20 netmask
255.255.255.0
RouterA(config)#access-list 2 permit 10.1.1.0 0.0.0.255
RouterA(config)#ip nat inside source list 2 pool org_pat_pool overload
RouterA(config)#interface e 0
RouterA(config-if)#ip nat inside
RouterA(config-if)#interface s 0
RouterA(config-if)#ip nat outside
```

This creates an access-list with a label of 2, which is applied using the overload method, to provide PAT. This method is obviously important in a home network, where users are granted an IP address for their router. The home network can then be setup with private addresses.

Cisco Router Challenge 72

Outline

This challenge involves the configuration of NAT overload.

Objectives

The objectives of this challenge are to:

- Define an overloaded NAT.
- Define an access-list to identify the traffic to be translated.
- Apply NAT on E0 and S0 interfaces.

Example

```
> en
# config t
(config)# access-list 7 permit 195.11.220.0 31.255.255.255
(config)# ip nat pool mynatpool 150.122.41.99 150.122.41.150 netmask
255.255.255.0
(config)# ip nat inside source list 7 pool mynatpool overload
(config)# int e0
(config-if)# ip nat inside
(config-if)# int s0
(config-if)# ip nat outside
```

Explanation

NAT overload is used when more addresses are required than are in the pool. In this case:

```
(config)# access-list 7 permit 195.11.220.0 31.255.255.255
```

identifies the traffic that will be translated for NAT, while:

```
(config)# ip nat pool mynatpool 150.122.41.99 150.122.41.150 netmask  
255.255.255.0
```

defines the pool of addresses what will be used. As NAT overload is used there can be many more addresses which can be mapped to this pool. Finally NAT overload is defined with:

```
(config)# ip nat inside source list 7 pool mynatpool overload
```

With NAT overload, the device overloads the first address. Once it reaches its limit of overloading the device moves onto the second address, and so on.

Cisco Router Challenge 73

Outline

This challenge involves the configuration of NAT overload without an address pool.

Objectives

The objectives of this challenge are to:

- Define an overloaded NAT, and define the port for the external address.
- Define an access-list to identify the traffic to be translated.
- Apply NAT on E0 and S0 interfaces.

Example

```
> en  
# config t  
(config)# access-list 8 permit 195.11.220.0 31.255.255.255  
(config)# ip nat inside source list 8 interface s0 ?  
  overload Overload an address translation  
  <cr>  
(config)# ip nat inside source list 8 interface s0 overload  
(config)# int e0  
(config-if)# ip nat inside  
(config-if)# int s0  
(config-if)# ip nat outside
```

Explanation

NAT overload without a pool is used where there is only a single address to be used, which is borrowed from the external interface. In this case:

```
(config)# access-list 8 permit 195.11.220.0 31.255.255.255
```

Finally NAT overload is defined with:

```
(config)# ip nat inside source list 8 interface s0 overload
```

where the address on the S0 interface is used as the external address. Thus all of the internal addresses will be translated to the single external address when it passes from inside the network to the outside. This is often the case of a home network, which typically has only a single address for the network connection.

Cisco Router Challenge 74

Outline

This challenge involves the configuration of TCP load distribution for NAT.

Objectives

The objectives of this challenge are to:

- Define an TCP load distribution.
- Define an access-list to identify the traffic to be translated.
- Apply NAT on E0 and S0 interfaces.

Example

```
> en
# config t
(config)# access-list 7 permit host 195.11.220.2
(config)# ip nat pool globalnat 208.132.69.7 208.132.69.57 netmask
255.255.192.0 ?
    type Specify the pool type
    <cr>
(config)# ip nat pool globalnat 208.132.69.7 208.132.69.57 netmask
255.255.192.0 type ?
    match-host Keep host numbers the same after translation
    rotary Rotary address pool
(config)# ip nat pool globalnat 208.132.69.7 208.132.69.57 netmask
255.255.192.0 type rotary
```

```
(config)# ip nat inside destination list 7 pool mynatpool
(config)# int e0
(config-if)# ip nat inside
(config-if)# int s0
(config-if)# ip nat outside
```

Explanation

TCP Load Distribution is used where there is a pool of servers, and the NAT translation assigns the mapping to one of these, in order to even the load. The command:

```
(config)# ip nat pool globalnat 208.132.69.7 208.132.69.57 netmask
255.255.192.0 type rotary
```

defines that the addresses should be assigned to the pool. For example the translations would be:

	Inside Local	Inside Global
1st:	208.132.69.7 <-	195.11.220.2
2nd:	208.132.69.8 <-	195.11.220.2
3rd:	208.132.69.9 <-	195.11.220.2

and so on. Thus when the first connection comes in for the address of 195.11.220.2, it will be translated to 208.132.69.7, the second for 208.132.69.8. Thus each of the servers will have a more equal loading. The following command defines a dynamic destination translation (where normally NAT would translate from a source node in the inside network):

```
(config)# ip nat inside destination list 7 pool mynatpool
```

Cisco Router Challenge 75

Outline

This challenge involves the configuration of NAT for overlapping networks.

Objectives

The objectives of this challenge are to:

- Define an overloaded NAT.
- Define an access-list to identify the traffic to be translated.
- Apply NAT on E0 and S0 interfaces.

Example

```
> en
# config t
(config)# access-list 7 permit 195.11.220.0 31.255.255.255
(config)# ip nat pool mynatpool 150.122.41.99 150.122.41.150 netmask
255.255.255.0
(config)# ip nat pool yournatpool 140.12.41.99 140.22.41.150 netmask
255.255.255.0

(config)# ip nat inside source list 7 pool mynatpool
(config)# ip nat outside source list 7 pool yournatpool

(config)# int e0
(config-if)# ip nat inside
(config-if)# int s0
(config-if)# ip nat outside
```

Cisco Router Challenge 76

Outline

This challenge involves the configuration of a dialer profile.

Objectives

The objectives of this challenge are to:

- Define the interface for Dialer0.
- Define encapsulation and authentication.
- Define dialer details.

Example

```
> en
# config t
(config)# int dialer0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# description test link
(config-if)# encapsulation ppp
(config-if)# ppp authentication chap
(config-if)# dialer remote-name temp
(config-if)# dialer idle-timeout 100
(config-if)# dialer fast-idle 80
(config-if)# dialer string 2221111
(config-if)# dialer pool 1
(config-if)# dialer-group 1
(config-if)# int bri0
(config-if)# dialer pool-member 1
```

Cisco Router Challenge 77

Outline

This challenge involves the configuration of a dialer profile with a map-class.

Objectives

The objectives of this challenge are to:

- Define a dialer map-class.
- Define the interface for Dialer0.
- Define encapsulation and authentication.
- Define dialer details.

Example

```
> en
# config t
(config)# map-class dialer kirkcaldy
(config-map-class)# dialer fast-idle 15
(config-map-class)# dialer idle-timeout 60
(config-map-class)# exit
(config)# int dialer0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# description test link
(config-if)# encapsulation ppp
(config-if)# ppp authentication chap
(config-if)# dialer remote-name temp
(config-if)# dialer string 2221111 class kirkcaldy
(config-if)# dialer pool 1
(config-if)# dialer-group 1
(config-if)# int bri0
(config-if)# dialer pool-member 1
```

Explanation

In the previous example (Challenge 75), the following was used:

```
(config)# int dialer0
```

```
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# description test link
(config-if)# encapsulation ppp
(config-if)# ppp authentication chap
(config-if)# dialer remote-name temp
(config-if)# dialer idle-timeout 100
(config-if)# dialer fast-idle 80
(config-if)# dialer string 2221111
(config-if)# dialer pool 1
(config-if)# dialer-group 1
(config-if)# int bri0
(config-if)# dialer pool-member 1
```

In order to allow reuse a class-map can be created for the characteristics of the dialup string, such as:

```
(config)# map-class dialer kirkcaldy
(config-map-class)# dialer fast-idle 15
(config-map-class)# dialer idle-timeout 60
(config-map-class)# exit
```

and can be applied onto the dialer string with:

```
(config-if)# dialer string 2221111 class kirkcaldy
```

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 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 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
tracert	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 of security of a router.

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)# mac-address 1111.2222.3333
(config-if)# dsl operating-mode auto
(config-if)# bridge-group 1
(config-if)# pvc 8/35
(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 8/35
(config-atm-vc)# pppoe-client dial-pool-number 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)# 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-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 test
(config-vpdn)# request-dialin
(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)# dsl operating-mode auto
(config-if)# pvc 8/35
(config-atm-vc)# pppoe-client dial-pool-number 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)# 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).

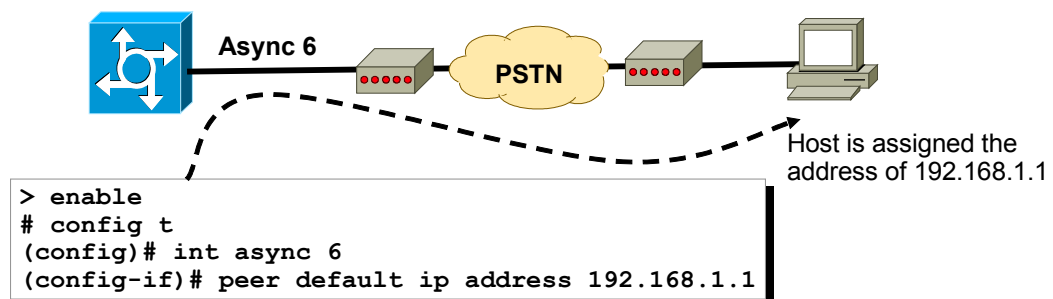


Figure 1: Host assigned a fixed IP address

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).

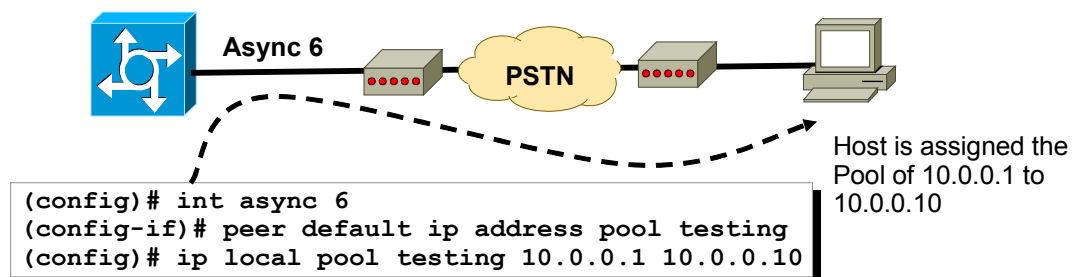


Figure 1: Host assigned an address from the local pool

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).

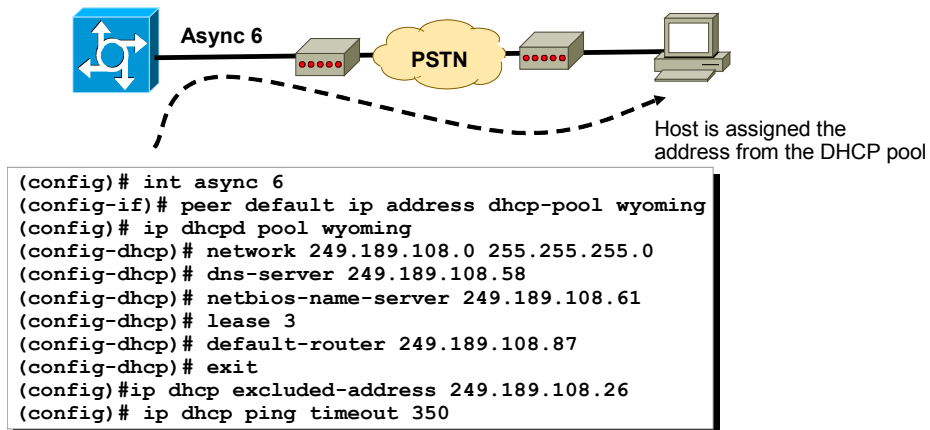


Figure 1: Host assigned an address from the DHCP server pool

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.

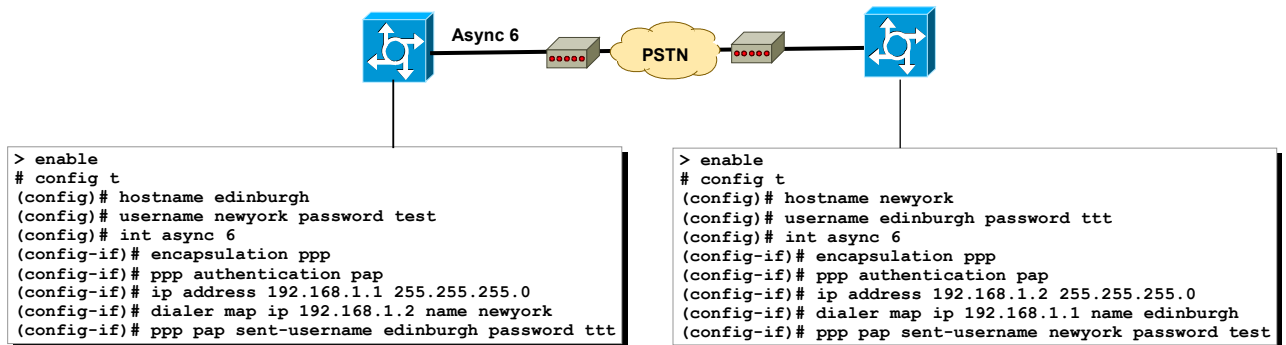


Figure 1: Host assigned an address from the DHCP server pool

Cisco Router Challenge 193

Outline

This challenge involves the configuration of a 2501 Console Server, which has multiple TTY connections which connect to the console ports of devices. This allows for remote connections. For example the first TTY connection can be connected to by:

telnet IP 2001

the second by:

telnet IP 2002

Objectives

The objectives of this challenge are to:

- Define the hostname.
- Show connections.

Example

```

> enable
# config t
(config)# int loopback0
(config-if)# ip address 10.0.0.1 255.255.255.255
(config-if)# exit
  
```

```

(config)# int e0
(config-if)# ip address 192.168.1.100 255.255.255.0
(config-if)# no shutdown
(config-if)# exit
(config)# line 1 16
(config-line)# tran input ?
    all      All protocols
    none     No protocols
    pad      X.3 PAD
    rlogin   Unix rlogin protocol
    telnet   TCP/IP Telnet protocol
    v120     Async over ISDN

(config-line)# transport input all
(config-line)# no ?
absolute-timeout      Set absolute timeout for line disconnection
access-class          Filter connections based on an IP access list
activation-character   Define the activation character
autobaud              Set line to normal autobaud
autocommand           Automatically execute an EXEC command
autocommand-options   Autocommand options
autohangup            Automatically hangup when last connection closes
autoselect            Set line to autoselect
buffer-length         Set DMA buffer length
data-character-bits   Size of characters being handled
databits              Set number of data bits per character
disconnect-character  Define the disconnect character
dispatch-character    Define the dispatch character
dispatch-machine      Reference a TCP dispatch state machine
dispatch-timeout      Set the dispatch timer
domain-lookup         Enable domain lookups in show commands
editing               Enable command line editing
escape-character      Change the current line's escape character
exec                  Configure EXEC
exec-banner           Enable the display of the EXEC banner
exec-character-bits   Size of characters to the command exec
exec-timeout          Set the EXEC timeout
flowcontrol           Set the flow control
flush-at-activation   Clear input stream at activation
full-help             Provide help to unprivileged user
history              Enable and control the command history function
hold-character        Define the hold character
insecure             Mark line as 'insecure' for LAT
international         Enable international 8-bit character support
ip                    IP options
length               Set number of lines on a screen
location             Enter terminal location description
lockable             Allow users to lock a line
logging              Modify message logging facilities
login                Enable password checking
logout-warning        Set Warning countdown for absolute timeout of
                    line
modem                Configure the Modem Control Lines
monitor              Copy debug output to the current terminal line
motd-banner          Enable the display of the MOTD banner
notify               Inform users of output from concurrent sessions
ntp                  Configure NTP
padding              Set padding for a specified output character
parity               Set terminal parity
password             Set a password
private              Configuration options that user can set will
                    remain in effect between terminal sessions
privilege            Change privilege level for line

```

```

refuse-message          Define a refuse banner
rotary                  Add line to a rotary group
rxspeed                 Set the receive speed
script                  specify event related chat scripts to run on the
                        line
session-disconnect-warning Set warning countdown for session-timeout
session-limit           Set maximum number of sessions
session-timeout         Set interval for closing connection when there is
                        no input traffic
special-character-bits  Size of the escape (and other special) characters
speed                   Set the transmit and receive speeds
start-character         Define the start character
stop-character          Define the stop character
stopbits                Set async line stop bits
telnet                  Telnet protocol-specific configuration
terminal-type           Set the terminal type
timeout                 Timeouts for the line
transport                Define transport protocols for line
txspeed                 Set the transmit speeds
vacant-message          Define a vacant banner
width                   Set width of the display terminal
x25                     X25 protocol-specific configuration
(config-line)# no exec
(config-line)# exit
(config)# exit

# sh version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-I-L), Version 12.0(2a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 01-Jan-99 14:38 by phanguye
Image text-base: 0x0302E1C0, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c)XB1, PLATFORM SPECIFIC RELEASE SOFTWARE (fc1)
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c)XB1, PLATFORM SPECIFIC
RELEASE SOFTWARE (fc1)

cons uptime is 32 minutes
System restarted by power-on
System image file is "flash:c2500-i-1.120-2a"

cisco AS2511-RJ (68030) processor (revision I) with 6144K/2048K bytes of memory.
Processor board ID 12933183, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
16 terminal line(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

# show running
Using 1157 out of 32762 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname cons
!
```

```

enable secret 5 $1$JoVG$/lz4ezMej5nRUstTCFmvv1
enable password 7 110A15040401
!
ip subnet-zero
no ip routing
no ip domain-lookup
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0
 ip address 192.168.1.100 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
ip default-gateway 192.168.1.254
ip classless
!
!
line con 0
 password 7 14141C0A1C55
 login
 transport input none
line 1 16
 no exec
 exec-timeout 0 0
 password 7 030752180500
 login
 transport input all
 transport output telnet
line aux 0
line vty 0 4
 password 7 045805071F70
 login
!
end

```

sh line

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
0	CTY		-	-	-	-	-	0	0	0/0	-
1	TTY	9600/9600	-	-	-	-	-	0	22	0/0	-
2	TTY	9600/9600	-	-	-	-	-	0	62	0/0	-
* 3	TTY	9600/9600	-	-	-	-	-	0	20	0/0	-
4	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
5	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
6	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
7	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
8	TTY	9600/9600	-	-	-	-	-	0	2	0/0	-
9	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
10	TTY	9600/9600	-	-	-	-	-	0	2	0/0	-
11	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
12	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
13	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
14	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
15	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-

16	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
17	AUX	9600/9600	-	-	-	-	-	0	0	0/0	-
* 18	VTY		-	-	-	-	-	1	0	0/0	-
19	VTY		-	-	-	-	-	0	0	0/0	-
20	VTY		-	-	-	-	-	0	0	0/0	-
21	VTY		-	-	-	-	-	0	0	0/0	-
22	VTY		-	-	-	-	-	0	0	0/0	-

In this case there is a connection on TTY 3 and TTY 18.

clear line 3

sh line

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
0	CTY		-	-	-	-	-	0	0	0/0	-
1	TTY	9600/9600	-	-	-	-	-	0	22	0/0	-
2	TTY	9600/9600	-	-	-	-	-	0	62	0/0	-
3	TTY	9600/9600	-	-	-	-	-	0	20	0/0	-
4	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
5	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
6	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
7	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
8	TTY	9600/9600	-	-	-	-	-	0	2	0/0	-
9	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
10	TTY	9600/9600	-	-	-	-	-	0	2	0/0	-
11	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
12	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
13	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
14	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
15	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
16	TTY	9600/9600	-	-	-	-	-	0	0	0/0	-
17	AUX	9600/9600	-	-	-	-	-	0	0	0/0	-
* 18	VTY		-	-	-	-	-	1	0	0/0	-
19	VTY		-	-	-	-	-	0	0	0/0	-
20	VTY		-	-	-	-	-	0	0	0/0	-
21	VTY		-	-	-	-	-	0	0	0/0	-
22	VTY		-	-	-	-	-	0	0	0/0	-