





































---

The following is an example of pinging the IP address 172.16.11.111.

```
[root @ home]$ ping 172.16.11.111

Pinging 172.16.11.111 (172.16.11.111) with 56 bytes of data:

64 bytes from 172.16.11.111: icmp_seq= 0 ttl=255 time=1 ms
64 bytes from 172.16.11.111: icmp_seq= 1 ttl=255 time=0 ms
64 bytes from 172.16.11.111: icmp_seq= 2 ttl=255 time=0 ms
64 bytes from 172.16.11.111: icmp_seq= 3 ttl=255 time=0 ms

--- 172.16.11.111 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0/0 ms/1

[root @ home]$ █
```

## 2.3 User Account

A default user account is provided to configure, maintain, and operate the router in http (web), cli, and ftp modes. The default user name is **root**, and the default password **12345**. To add, modify, or delete the user name and password, enter the auth directory.

```
[root @ home]$ auth
```

At the auth directory, you can use the 'ls' command to display the available commands:

```
[root @ home]$ auth
[root @ auth]$ ls
A <CMD> adduser
A <CMD> deluser
```

---

A <CMD> `changepasswd`

A <CMD> `modifyuser`

A <CMD> `listusers`

A <CMD> `resetuser`

[root @ auth]\$

## adduser

```
adduser username -o -services [services] -permissions  
[permissions] services : [cli/ftp/http]
```

```
permissions : [admin/ordin]
```

Adds a new user to the system. This command asks to set password for the user. Only administrators can use this command.

### EXAMPLE

```
[root @ auth]$ adduser office1 -o -services ftp -permissions admin  
Enter password:
```

```
Confirm password:
```

```
User Name Succesfully Added.
```

```
[root @ auth]$ █
```

---

## deluser

**Deluser <username>**

Enter this command followed by the name of the user to be deleted. Only administrators can use this command.

## modifyuser

**modifyuser <username> -o**  
**-addservices <cli | ftp | http>**  
**-delservices <cli | ftp | http>**  
**-permissions <admin | ordinary>**

Modifies the properties of a user's account.

**<username>**

The name of the user whose services or permissions are to be modified.

**-addservices <cli | ftp | http>**

Adds **cli**, **ftp**, or **http** services to the user.

**-delservices <cli | ftp | http>**

Removes **cli**, **ftp**, or **http** services from the user.

## EXAMPLE

**modifyuser xyz -o -addservices ftp -permissions ordinary**

Allows user "xyz" ordinary permissions to access the system via ftp. In

---

addition, gives the user "xyz" ordinary permissions. In other words user "xyz" is not an administrator.

**modifyuser abc -o -delservices http**

Prohibits user "abc" from accessing the system via http.

**modifyuser xyz -o -addservices ftp delservices http -permissions ordinary**

Allows user "xyz" to access the system via ftp and prohibits that user from accessing the system via http. In addition, gives the user "xyz" ordinary permissions. In other words user "xyz" is not an administrator.

### [changepasswd](#)

**changepasswd <username>**

Changes password of the existing user. This is an administrators command; ordinary users can not use this.

### [listusers](#)

**listusers**

Lists all registered users to use CLI/http/ftp.

EXAMPLE

```
[root @ auth]$ listusers
1      root      cli http ftp  ADMIN
2      pppoe     http          ADMIN
3      maylyne   http          ORDIN
4      may       http          ADMIN
5      barret    cli           ADMIN
6      office1  http ftp     ORDIN
[root @ auth]$ █
```

---

## resetuser

reset the user password. This is an administrators command; ordinary users can not use this.

```
[root @ auth]$ resetuser  
[root @ auth]$ resetuser root
```

```
Enter New password:
```

```
Confirm New password:
```

```
Password changed  
[root @ auth]$ █
```

## 2.4 Ethernet IP Address

There are two configurable Ethernet interfaces, identified with eth0 and eth1 in CLI. Each Ethernet interface provides two default IP addresses. Interface eth0- 192.168.1.1 and 192.168.1.2.

Interface eth1- 192.168.2.1 and 192.168.2.2

To set up an IP address and subnet mask for the Ethernet interface, use the following command after the prompt of [root @ home]\$.

---

**ifconfig -o <interface-name> inet <address> [parameters]**

**ifconfig -o -a** displays the information of the interfaces

**ifconfig -o -l**

**parameters-** mtu <n 72-1500>, broadcast <address>, netmask <mask>, up, down alias <address>, -alias <address>.

**[root @ home]\$ ifconfig -o**

The following explains the parameters of the command for .

**<interface name>**

The LAN interface to be configured. Type eth0 for Interface Ethernet 1, and type eth0 for Interface Ethernet 2.

**<address>**

The IP address or subnet mask to be assigned to the interface.

Dot-notation is used to enter the IP address (for example 192.168.2.1).

**netmask <mask>**

The netmask is used to extract the network portion of the IP address. It also specifies how much of the IP address is to be reserved for subdividing the network into sub networks, which are taken from the host field of the address. Netmask is added with the interface IP address to get a network ID that is used in routing to indicate that this network is reachable through these interfaces. The mask can be specified as a single hexadecimal number with a leading 0x for example 0xfffff00, or with a dot-notation Internet address 255.255.255.0

---

**alias <address>**

To add the alias IP address

**-alias <address>**

To delete the alias IP address

### 2.4.1 Primary IP address

To assign an IP address of 172.0.0.1 with a 24-bit subnet mask to the eth1 interface, use this command:

```
[root @ home]$ ifconfig eth1 172.0.0.1 netmask 255.255.255.0
```

After typing the command, the [root @ home]\$ prompt displays. Save the changes by typing save. The following message displays and shows that the changes are successful.

**Configuration saved successfully**

### 2.4.2 Alias IP Address

To set up the alias IP address, use this command:

```
[root @ home]$ ifconfig -o <interface name> inet <address> alias  
netmask <address>
```

For example, use the following command to assign an alias IP address of 172.1.1.1 with a 24-bit subnet mask to the eth0 interface.

```
[root @ home]$ ifconfig -o eth0 inet 172.1.1.1 alias netmask  
255.255.255.0
```

---

To delete the alias IP address, use this command:

```
[root @ home]$ ifconfig -o <interface name> inet <address> -alias  
netmask <address>
```

## 2.5 rarpd

This command list is used to get the IP address of diskless system.

### 2.5.1 add

```
[root @ rarpd]$ add <0xH/Waddress > <IPAddress >
```

Used to add Hardware address and IP address into the DataBase.

<0xH/Waddress >

Hardware address in hexadecimal format.

<IPAddress >

IP address in dot notation.

EXAMPLE

```
[root @ rarpd]$ add 0x112233445566 192.168.3.4
```

Adds the H/W address and IP Address mapping in the database.



---

## 2.5.2 delete

```
[root @ rarpd]$ delete <0xH/Waddress >
```

Deletes an entry in the existing RARP DataBase

<0xH/Waddress >

Hardware address in hexadecimal format.

EXAMPLE

```
[root @ rarpd]$ delete 0x112233445566
```

Deletes mapping of H/W address 11:22:33:44:55:66 to IP Address, from the database.

## 2.5.3 list

```
[root @ rarpd]$ list
```

Lists the RARP DataBase entries.

EXAMPLE

```
[root @ rarpd]$ list
```

```
H/W ADDR IP ADDRESS
```

```
11:22:33:44:55:66 192.168.3.4
```

---

## 2.5.4 rarpd

```
[root @ rarpd]$ rarpd <-a | interface>
```

Starts the RARPD on the specified interface or all the interfaces.

### EXAMPLE

```
[root @ rarpd]$ rarpd eth0
```

Starts the RARPD on eth0 interface.

```
[root @ rarpd]$ rarpd eth0
```

If RARPD is already running the above command, it displays : "Rarpd is already running on the interface"

```
[root @ rarpd]$ rarpd -a
```

Starts the RARPD on all the interfaces.

---

## Chapter 3 Quick Configuration

This chapter describes how to configure the device for the first time using the CLI. The router can work after these settings are complete.

### 3.1 RFC 1483 Bridged

To enable the bridging function of the device, enter the **sndcp** directory from the prompt of [root @ sndcp]\$. In the sndcp directory, type **bridge** to enter the bridge directory.

#### 3.1.1 Configuration

##### PART 1 Create a PVC

1. Type **atm** at the [root @ home] prompt to enter the [root @ home]\$ prompt.

2. Type **vcadd 0 35 ubr aal5**

```
[root @ atm]$ vcadd 0 35 ubr aal5
Missing PCR, and is set to default value: 3000
Missing average rate/SCR, and is set to peak rate.
Setting MBS to default value: 45
Setting CDUT to default value: 500000
[root @ atm]$
```

3. At the [root @ atm] prompt, type **home** or **exit** to return to the [root

---

@ home] prompt.

## PART 2 Set the PVC to RFC 1483 Bridged

1. If there is no other RFC 1483 PVC set up, you must join the Ethernet interface to an ATM interface (atm0 to atm7). Therefore, traffic can be transferred between the two interfaces. To do this, type **bridge** to enter the [root @ bridge] prompt.
2. Type **group eth0 atm7**. In this case, atm7 is used. You can choose any other atm interface.
3. If the setup is successful, the [root @ bridge]\$ prompt pops up. If a PVC was set up other than the new one, the message pops up: **Group Exist or Interface Busy**  
You must delete the old PVC or PVCs to add the new group.
4. Under the [root @ bridge] prompt, type **pvc add atm7 0 35 11c**. In this case, atm7 is used. You must choose the atm interface that is joined to the Ethernet interface. The default is atm7.
5. Type **bridge enable**.

```
[root @ atm]$ vcadd 0 35 ubr aal5
Missing PCR, and is set to default value: 3000
Missing average rate/SCR, and is set to peak rate.
Setting MBS to default value: 45
Setting CDVT to default value: 500000
[root @ atm]$ home
[root @ home]$ bridge
[root @ bridge]$ group eth0 atm7
[root @ bridge]$ pvc add atm7 0 35 11c
[root @ bridge]$ bridge enable
[root @ bridge]$
```

- 
6. If the [root @ bridge] prompt pops up, a PVC 0/35 is successfully enabled for the RFC 1483 Bridged mode.

### **PART 3 Delete the PVC for RFC1483 Bridged**

To delete the PVC set up for the RFC 1483 Bridged, you must delete the service first under the [root @ bridge] prompt. Secondly, delete the VC under the [root @ atm] prompt. The following screen is an example.

```
[root @ atm]$ home
[root @ home]$ bridge
[root @ bridge]$ bridge delete
[root @ bridge]$ home
[root @ home]$ atm
[root @ atm]$ deletevc 0 35
Vcc deleted successfully
[root @ atm]$ █
```

### **3.1.2 Additional Commands**

You can use this command to disable or enable the bridging function of the Ethernet interface.

```
bridge eth0 <disable> <vpi> <vci>
```

```
bridge eth0 <enable> <vpi> <vci> -o <-enc encapsulation>
```

#### **enable**

Enables the bridge interface.

#### **disable**

Disables the bridge interface.

---

**<vpi> <vci>**

These are the vpi, vci values on which bridge has to be enabled/disabled. vpi, vci are assigned with the vcadd command. The showatmconn command can also be used to list the current ATM connections with their respective vpi and vci values. (Note the vcadd and showatmconn commands are located in the ihatmld directory).

**-enc LLC / VC**

Specifies the encapsulation type. The possible values are LLC and VC, which represent Logical Link Control and VC multiplexing respectively.

**-t timeout**

Specifies the idle timeout for bridge table entries. The timeout value is in milliseconds.

**Note: about idle time out:**

Whenever there is any traffic passing through the bridge, the bridge will maintain the lookup table with the MAC addresses coming from configured interface (through LAN). If the traffic is destined to any Mac address in the lookup table, that packet is not sent to ATM interface. If there is no traffic from a particular machine for certain time period then that entry is deleted from the lookup table. The time that the bridge will clear the bridge lookup entry is idle timeout.

**EXAMPLE**

To configure the system as a bridge, this **bridge** command is used.

---

**bridge eth0 enable 0 100 -o -enc LLC -t 1000**

This command configures the Ethernet interface eth0 to work as a bridge with the WAN ATM interface. The PVC specified by the vpi, vci with values 0,100 is created with LLC encapsulation. A timeout of 1000 milli seconds is used for bridge table entries.

**bridge eth0 disable 0 100**

Disables the bridge configuration for the Ethernet interface eth0.

## 3.2 RFC 1483 Routed

There are two major parts to set up a RFC 1483 Bridged PVC. The first part is to add a PVC under the atm directory. The second part is to assign the new PVC to the RFC1483 Bridged mode under the bridge directory. The following is an example of adding an RFC1483 Bridged PVC at 0/35.

### PART 1 Create a new VC

1. Type **atm** at the [root @ home] prompt to enter the [root @ home]\$ prompt.
2. Type **vcadd 0 35ubr aal5**

```
[root @ atm]$ vcadd 0 35ubr aal5
Missing PCR, and is set to default value: 3000
Missing average rate/SCR, and is set to peak rate.
Setting MBS to default value: 45
Setting CDUT to default value: 500000
[root @ atm]$
```

- 
3. At the [root @ atm] prompt, type **home** or **exit** to return to the [root @ home] prompt.

#### **PART 2 Set the PVC to RFC 1483 Routed**

1. Return to the [root @ home] prompt.
2. Type **sndcp** at the [root @ home] prompt to enter the [root @ sndcp] prompt.
3. Type **routedbridge atm0 enable 0 35 -o -enc LLC**. In this case, atm0 is used. You must choose other atm interface. In addition, in the command, LLC must be capitalized.
4. If the [root @ sndcp] prompt pops up, a PVC 0/35 is successfully created for RFC 1483 Routed mode.

#### **PART 3 Set up an IP address for the WAN interface**

1. Return to the [root @ home] prompt and type the following command.

```
root @ home]$ ifconfig -o atm0 inet 1.1.1.3 netmask 255.255.255.0
root @ home]$ █
```

If you need the usage of the ifconfig command, type **ifconfig**.

```
[root @ home]$ ifconfig
Usage:
ifconfig -o <interface-name> inet <address> [parameters]
ifconfig -o -a
ifconfig -o -l
parameters- mtu <n 72-1500>, broadcast <address>, netmask <mask>, up, down
[root @ home]$ █
```



---

2. If the WAN IP address is successfully set up, the [root @ home]\$ prompt pops up.

#### PART 4 Delete the PVC to RFC 1483 Routed

To delete the PVC set up for the RFC 1483 Routed, you must disable the service first under the [root @ sndcp] prompt. Secondly, delete the VC under the [root @ atm] prompt. The following screen is an example.

```
[root @ sndcp]$ routedbridge atm0 disable 0 35
[root @ sndcp]$ home
[root @ home]$ atm
[root @ atm]$ deletevc 0 35
Vcc deleted successfully
[root @ atm]$ █
```

### 3.3 IPoA

#### PART 1 create a new VC

1. Type **atm** at the [root @ home] prompt to enter the [root @ home]\$ prompt.
2. Type **vcadd 0 35ubr aal5**

```
[root @ atm]$ vcadd 0 35ubr aal5
Missing PCR, and is set to default value: 3000
Missing average rate/SCR, and is set to peak rate.
Setting MBS to default value: 45
Setting CDUT to default value: 500000
[root @ atm]$
```

3. At the [root @ atm] prompt, type **home** or **exit** to return to the [root

---

@ home] prompt.

## PART 2 Set the PVC to IPoA

1. Return to the [root @ home] prompt.
2. Type **sndcp** at the [root @ home] prompt to enter the [root @ sndcp] prompt.
3. Type **ipoa** to display the command to set up an mer entry. The command usage is shown below.

```
[root @ sndcp]$ ipoa
```

```
ipoa <interface> <disable> <vpi> <vci> -o <default> <-nhp ipaddress>
ipoa <interface> <enable> <vpi> <vci> -o <-enc encapsulation>
                                     <default>
                                     <-nhp ipaddress>
                                     <-vpn OUI vpnId>
      interface          - interface number
      enable/disable    - enables or disable the bridge module
      vpi                - vpi
      vci                - vci
      -enc encapsulation - encapsulation type LLC/VC
      default            - use default PVC
      -nhp ipaddress     - next hop ip address

      -vpn <OUI> <vpnId> - Enable UPN encapsulation
                        OUI   : Organizationally Unique Identifier.
                        vpnId : UPN Index.
```

```
[root @ sndcp]$ █
```

The following is an example of setting up an IPoA entry

```
[root @ sndcp]$ ipoa atm0 enable 0 35 -o
[root @ sndcp]$ █
```

4. If the [root @ sndcp] prompt pops up, a PVC 0/35 is successfully created for the IPoA mode.

---

### PART 3 Delete the PVC for IPoA

To delete the PVC set up for the IPoA, you must delete the profile first under the [root @ sndcp] prompt. Secondly, delete the VC under the [root @ atm] prompt. The following screen is an example.

```
[root @ sndcp]$ ipoa atm0 disable 0 35
[root @ sndcp]$ home
[root @ home]$ atm
[root @ atm]$ deletevc 0 35
Vcc deleted successfully
[root @ atm]$ █
```

## 3.4 PPPoE

### PART 1 Create a new VC

1. Type **atm** at the [root @ home] prompt to enter the [root @ home]\$ prompt.
2. Type **vcadd 0 35 ubr aal5**

```
[root @ atm]$ vcadd 0 35 ubr aal5
Missing PCR, and is set to default value: 3000
Missing average rate/SCR, and is set to peak rate.
Setting MBS to default value: 45
Setting CDUT to default value: 500000
[root @ atm]$
```

3. At the [root @ atm] prompt, type **home** or **exit** to return to the [root @ home] prompt.

---

## PART 2 Set the PVC to PPPoE

1. Return to the [root @ home] prompt.
2. Type **sndcp** at the [root @ home] prompt to enter the [root @ sndcp] prompt.
3. Type **pppoe** to display the command usage to set up a PPPoE entry.

The command is shown below.

```
USAGE :
pppoe <profile> -o <-if Interface> <-encap Encapsulation> <-restarttime Timeout>
>
<-auth Auth> <-myaddr IPAddr> <-peer PeerIPAddr> <-mtu MTU> <-mru MRU>
<-hwaddr Ethaddr> <-service ServiceName> <-acname ACName> <-tag HostTag>
<-user Username> <-pass Password> <-upi Upi> <-vci Vci> <-mode Mode>
<-idletime idleTimeout> <-nat [enable/disable]> <-netmask mask> <-vpn OUI vpnId>
>
Interface          - interface name with unit number (eg ppp0 or ppp1)
Encapsulation      - encapsulation type (LLC or UC)
Timeout            - timeout (in milliseconds)
Auth               - authentication (PAP, CHAP, MSCHAPV1, MSCHAPV2)
IPAddr             - Desired self IP address (in dotted decimal)
PeerIPAddr         - Peer IP Address (in dotted decimal)
MTU                - Maximum Transmission Unit
MRU                - Maximum Receive Unit, negotiated in LCP
Ethaddr            - Ethernet hw addr (specify bytes in decimal and use ':'
                    as delimiter, eg 10:11:12:13:14:15)
ServiceName        - Service Name
ACName             - Access Concentrator name
HostTag            - Use Host unique tag
Username           - Username
Password           - Password
Upi                - Upi
Vci                - Vci
Mode               - Mode in which PPP will run (AUTO, DIRECT)
idleTimeout        - The idle timeout value (in minutes)
nat                - enable/disable(default- disable)
netmask            - netmask for IP address received from Server
vpn                - Enable UPN encapsulation
                    OUI   : Organizationally Unique Identifier.
                    vpnId : UPN Index.

[root @ sndcp]$
```

---

The command covers the basic settings for the PPPoE entry number, encapsulation type, timeout period, authentication, user name, password, VPI, VCI, and NAT. You can complete a PPPoE entry by typing this command that covers these basic settings. If you need a complete setting, refer to the usage instruction above.

```
[root @ sndcp]$ pppoe 0 -o -if ppp0 -encap llc -auth pap -user 12342@m -pass 12345 -vpi 0 -vci 35 -mod auto -idletime 2 -nat enable
[root @ sndcp]$ █
```

4. If the [root @ sndcp] prompt pops up, a PVC 0/35 is successfully created for PPPoE mode.

### PART 3 Delete the PVC for PPPoE

To delete the PVC set up for the PPPoE, you must delete the profile first under the [root @ sndcp] prompt. Secondly, delete the VC under the [root @ atm] prompt. The following screen is an example.

```
[root @ sndcp]$ pppoedel 0
[root @ sndcp]$ home
[root @ home]$ atm
[root @ atm]$ deletevc 0 35
Vcc deleted successfully
[root @ atm]$ █
```

---

### 3.4.1 Additional Commands

After a profile has been configured, a PPPoE session can be started and stopped with the **pppoe** and **pppoe** commands in the `sndcp` directory, type **pppoe** to enter the `pppoe` directory.

```
pppoe <profile> -o <-if Interface> <-encap Encapsulation>  
<-restarttime Timeout> <-auth Auth> <-user Username> <-pass  
Password> <-vpi Vpi> <-vci Vci> <-mode Mode> <-idletime  
idleTimeout> <-nat [enable/disable]> <-netmask mask>
```

Sets up a PPPoE profile.

#### **profile**

Profile number to configure. Specify an integer from 0 to 7.

#### **-if <interface>**

Interface name with unit number. Four PPP interfaces are available:

ppp0 – ppp7

#### **-encap <encapsulation>**

Encapsulation type. Possible values are LLC (Logical Link Control) or VC (VC Multiplexing).

#### **-auth <authentication>**

Authentication type (PAP or CHAP).

#### **-user <user>**

---

User name.

**-pass <password>**

Password.

**-vpi <vpi>**

The ATM vpi value that was assigned in a vcadd command or listed in an atmshowconn command.

**-vci <vci>**

The ATM vci value that was assigned in a vcadd command or listed in an atmshowconn command.

**mode**

Mode in which PPP will run (AUTO, DIRECT). AUTO mode auto-establishes a PPP session when a packet to be transmitted to the Internet is detected. DIRECT mode allows the user to manually establish a PPP session to connect to the Internet. When using DIRECT mode, you also need to configure the ADD PPPOESTART and PPPOESTOP functions. These are described in Sections 4.4.3 and 4.4.4.

**idleTimeout**

The idle timeout value (in seconds)

**nat**

enable/disable(default- disable)

**EXAMPLE**

```
ppoe 0 -o -if ppp0 -encap LLC -auth PAP -user jones -pass
```

---

**Indiana -vpi 0 -vci 100 -mode AUTO -idletime 600**

Defines a PPPoE profile. The ppp0 interface is used with the ATM connection vpi 0 and vci 100. The user name is jones and the password is Indianalo. The mode is auto and the idle time is 600 seconds.

### **pppoestart**

**pppoestart <Profile>**

Starts PPPoE given the specified profile. The profile is specified with an integer (0, 1, 2). The profile was previously specified with the **pppoe** command.

### **pppoestop**

**pppoestop <Profile>**

Stops PPPoE given the specified profile. The profile is specified with an integer (0, 1, 2). The profile was previously specified with the **pppoe** command.



---

## pppoelist

### **pppoelist [-profile Profile]**

Displays the listing of all available free profiles. If **-profile** is not specified, this command will display all the valid configured profiles.

---

## 3.5 PPPoA

### 3.5.1 Configuration

#### PART 1 Create a new VC

1. Type **atm** at the [root @ home] prompt to enter the [root @ home]\$ prompt.

2. Type **vcadd 0 35 ubr aal5**

```
[root @ atm]$ vcadd 0 35 ubr aal5  
Missing PCR, and is set to default value: 3000  
Missing average rate/SCR, and is set to peak rate.  
Setting MBS to default value: 45  
Setting CDVT to default value: 500000  
[root @ atm]$
```

3. At the [root @ atm] prompt, type **home** or **exit** to return to the [root @ home] prompt.

---

## PART 2 Set the PVC to PPPoA

1. Return to the [root @ home] prompt.
2. Type **sndcp** at the [root @ home] prompt to enter the [root @ sndcp] prompt.
3. Type **PPPoA** to display the command to set up a PPPoA entry. The command usage is shown below.

```
[root @ sndcp]$ pppoa
USAGE :
pppoa <profile> -o <-if Interface> <-encap Encapsulation> <-restarttime Timeout>
>
<-auth Auth> <-myaddr IPAddr> <-peer PeerIPAddr> <-mtu MTU> <-mru MRU>
<-user Username> <-pass Password> <-vpi Vpi> <-vci Vci>
<-nat [enable/disable]> <-netmask mask> <-vpn OUI vpnId>
  Interface      - interface name with unit number (eg ppp0 or ppp1)
  Encapsulation  - encapsulation type (LLC or UC)
  Timeout        - timeout (in milliseconds)
  Auth           - authentication (PAP, CHAP, MSCHAPV1, MSCHAPV2)
  IPAddr         - Desired self IP address (in dotted decimal)
  PeerIPAddr     - Peer IP Address (in dotted decimal)
  MTU            - Maximum Transmission Unit
  MRU            - Maximum Receive Unit, negotiated in LCP
  Username       - Username
  Password       - Password
  Vpi            - Vpi
  Vci            - Vci
  nat            - enable/disable(default- disable)
  netmask        - netmask for IP address received from Server
  vpn            - Enable VPN encapsulation
                  OUI   : Organizationally Unique Identifier.
                  vpnId : VPN Index.

[root @ sndcp]$ █
```

The command covers the basic settings for the PPPoA profile number, encapsulation type, timeout period, authentication, user name, password, VPI, VCI, and NAT. You can complete a PPPoA entry by typing this

---

command that covers these basic settings. If you need a complete setting, refer to the usage instruction above.

```
[root @ sndcp]$ pppoa 0 -o -if ppp0 -encap 11c -auth pap -user 1234@m -pass 1234  
-vpi 0 -vci 35  
[root @ sndcp]$ █
```

4. If the [root @ sndcp] prompt pops up, a PVC 0/35 is successfully created for PPPoA mode.

### **PART 3 Delete the PVC for PPPoA**

To delete the PVC set up for the PPPoA, you must delete the profile first under the [root @ sndcp] prompt. Secondly, delete the VC under the [root @ atm] prompt. The following screen is an example.

```
[root @ sndcp]$ pppoadel 0  
[root @ sndcp]$ home  
[root @ home]$ atm  
[root @ atm]$ deletevc 0 35  
Vcc deleted successfully  
[root @ atm]$ █
```

---

### 3.5.2 Additional Commands

**routedbridge** <interface> <disable> <vpi> <vci>

**routedbridge** <interface> <enable> <vpi> <vci>

Configures the specified WAN interface to use PPPoA.

#### **interface**

The name of the WAN interface.

#### **enable**

Enables this PPPoA profile.

#### **disable**

Disables this PPPoA profile.

#### **<vpi> <vci >**

These are the vpi and vci values on which PPPoA has to be enabled/disabled. Vpi and vci are assigned with the **vcadd** command under the atm directory. The **showatmconn** command can also be used to list the current ATM connections with their respective vpi and vci values. (Note the **vcadd** and **showatmconn** commands are located in the ihatmld directory).

#### **-enc LLC | VC**

Specifies the encapsulation type. The possible values are llc or vc which represent Logical Link Control or VC multiplexing respectively.

Note the Maximum Transfer Unit (MTU) for PPPoA is 9182.

---

EXAMPLE

**routedbridge atm0 enable 0 100 -enc LLC**

Establishes a PPPoA connection on the WAN interface atm0. VPI, VCI values 0, 100 is used for the ATM connection. LLC encapsulation will be used.

**routedbridge atm0 disable 0 100**

Disables the PPPoA connection.

---

## 3.6 MER

### PART 1 Create a new VC

1. Type **atm** at the [root @ home] prompt to enter the [root @ home]\$ prompt.
2. Type **vcadd 0 35 ubr aal5**

```
[root @ atm]$ vcadd 0 35 ubr aal5  
Missing PCR, and is set to default value: 3000  
Missing average rate/SCR, and is set to peak rate.  
Setting MBS to default value: 45  
Setting CDUT to default value: 500000  
[root @ atm]$
```

3. At the [root @ atm] prompt, type **home** or **exit** to return to the [root @ home] prompt.

### PART 2 Set the PVC to MER

1. Return to the [root @ home] prompt.
2. Type **sndcp** at the [root @ home] prompt to enter the [root @ sndcp] prompt.
3. Type **1483mer** to display the command to set up an MER entry. The command usage is shown below. For the port parameter specified in the command, always type **mer0**. Only one MER entry can be created.

---

```
[root @ sndcp]$ 1483mer
1483mer add port vpi vci encapsulation
where port      - MER Interface Name.
      vpi       - (0-255)
      vci       - (0-65535)
      encapsulation - llc\vc
[root @ sndcp]$
```

The following is an example of setting up the MER.

```
root @ sndcp]$ 1483mer add mer0 0 35 llc
root @ sndcp]$
```

4. If the [root @ sndcp] prompt pops up, a PVC 0/35 is successfully created for MER mode.

### PART 3 Set up an IP address for the WAN interface

1. Return to the [root @ home] prompt and type the following command.

If you need the usage of the ifconfig command, type ifconfig.

```
[root @ home]$ ifconfig -o mer0 inet 1.2.4.31 netmask 255.255.255.0
[root @ home]$
```

2. If the WAN IP address is successfully set up, the [root @ home]\$ prompt pops up.



---

#### PART 4 Delete the PVC for MER

To delete the PVC set up for the MER, you must delete the profile first under the [root @ sndcp] prompt. Secondly, delete the VC under the [root @ atm] prompt. The following screen is an example.

```
[root @ sndcp]$ mer
mer action
  where action - enable\disable\Delete\Status
[root @ sndcp]$ mer delete
[root @ sndcp]$ home
[root @ home]$ atm
[root @ atm]$ deletevc 0 35
Vcc deleted successfully
[root @ atm]$ █
```

---

## 3.7 Declaring PPP Sessions

In PPPoE or PPPoA mode, you can use this command to declare that a PPP session is established. The command is given in the **SND CP** directory.

**ppptrace** [on | off]

**on**

Declares a PPP session is established

**off**

displays no message when a PPP session is established.

---

## Chapter 4 Advanced Configuration

### 4.1 Static Route

To set up the static route, type **route** at the prompt to display the static route commands. A total of six commands are used to add, delete, modify, and flush the static route table.

```
[root @ home]$ route
    route add -o -dest {dest ip addr} -gateway {gateway ip addr}
[{-option value} *]
    route add -o -dest {dest ip addr} -interface {interface name}
[{-option value } *]
    route delete -o -dest {dest ip addr}
    route change -o -dest {dest ip addr} -gateway {new ip addr}
    route get    -o -dest {ip addr}
    route flush
    list routes
options : mtu & hopcount & netmask[root @ home]$
```

The command **route add -o -dest {dest ip addr} -interface {interface name} [{-option value } \*]** is reserved only.

---

The following is an example of creating a static route.

```
login:
Password:
[cht @ home]$ route add -o -dest 172.16.7.0 -gateway 10.0.0.2 -netmask 255.255.255.0

[cht @ home]$ save
Configuration saved successfully
[cht @ home]$ █
```

## 4.2 Ethernet

The ethernet command is used to configure the Ethernet interface parameters. Ethernet commands are located in the "ethernet" directory.

```
[root @ ethernet]$ ls

A <CMD>  setemac
A <CMD>  rmon
A <CMD>  pread
A <CMD>  pwrite
A <CMD>  elink
A <CMD>  up
A <CMD>  down
A <CMD>  stat
[root @ ethernet]$
```

---

### 4.2.1 MAC Address

Use `setemac xx:xx:xx:xx:xx:xx` to change the MAC address. The following is an example of how to change the MAC address.

```
[root @ ethernet]$ setemac
setemac xx:xx:xx:xx:xx:xx
[root @ ethernet]$ setemac 11:01:0b:ab:00:00
Base MAC address updated. Don't forget to SAVE it
[root @ ethernet]$
```

Sets the Ethernet addresses for the ADSL router. The Ethernet MAC address is specified in standard colon-separated notation.

In order for the MAC changes to take effect, the configuration must be saved (using 'save' command in the home directory) and the system rebooted.

#### <mac address>

The MAC address in colon separated notation. Two hex digits must be supplied between the colons. Twelve hex digits comprise a MAC address. (i.e. "aa:bb:cc:01:22:05").

#### EXAMPLE

```
[root @ ethernet]$ setemac 11:22:33:44:55:66
[root @ ethernet]$home
[root @ home]$save
```

---

### 4.2.2 elink

```
[root @ ethernet]$ elink <interface> -o [[auto] | [10 | 100 |  
auto_speed ] | [half | full | auto_duplex]
```

Configures the speed and/or duplex of the Ethernet interface. The default setting is `auto` for auto negotiation. With auto negotiation, both the speed and duplex are configured based upon what the link is connected to. It is also possible to configure the duplex, say `half` and `full`, and specify `auto_speed` so that only the speed is auto negotiated. Similarly for `auto_duplex`.

`<interface>`

The name of the Ethernet interface. This is `eth0`.

`Auto` specifies that both the speed and duplex are auto negotiated.

**10**

Specifies that the speed is set to 10M bits per second.

**100**

Specifies that the speed is set to 100M bits per second.

**auto\_speed**

Specifies that the speed is auto negotiated.

**half**

Specifies half duplex

**full**

Specifies full duplex

**auto\_duplex**

Specifies that the duplex is auto negotiated.

---

EXAMPLE

```
[root @ ethernet]$ elink eth0 -o 10 half
```

Sets the Ethernet to a speed of 10Mbps half duplex.

```
[root @ ethernet]$ elink eth0 -o auto_speed full
```

The speed will be auto negotiated and the link will use full

### 4.2.3 `pread`

```
pread <interface> <port(decimal)>
```

Reads PHY register

EXAMPLE

```
[root @ ethernet]$ pread eth0 1
```

```
Register 1 value 0xffff
```

Displays the register 1 value of eth0 interface.

### 4.2.4 `pwrite`

```
pwrite <interface> <port(decimal)>  
<value(hex)>
```

Writes PHY register

---

## 4.2.5 rmon

This command reads the EMAC RMON counters. Type `rmon eth0` at the prompt to collect the Ethernet interface statistics.

```
[root @ ethernet]$ rmon eth0
Hardware link statistics
=====
          Rx frames: 27
          Rx octets: 0
          Rx interrupts: 12757

          Rx CRC errors: 0
          Rx frame errors: 0
          Rx internal errors: 0
          Rx length errors: 27
          Rx resource events: 0

          Tx frames: 13
          Tx octets: 0
          Tx interrupts: 5286

          Tx SQE errors: 0
Tx carrier sense errors: 0
          Tx deferred: 0
Tx excessively deferred: 0
          Tx single collisions: 0
          Tx multiple collisions: 0
          Tx late collisions: 0
          Tx internal errors: 0

          Hardware interrupts: 17738
[root @ ethernet]$ █
```



---

### 4.2.6 Disable/Enable the Ethernet Function

The default setting of the Ethernet function is enabled. To disable it, use the **down eth0** command. To enable it, use the **up eth** command. When the Ethernet interface is disabled, the telnet or web session will be terminated. The device can be only accessible from the console port.

## 4.3 Bridge

The bridge command sets up the bridge functions, covering the following commands.

```
[root @ home]$ bridge
[root @ bridge]$ ls

0 <CMD> pvc
0 <CMD> group
0 <CMD> cachetimer
0 <CMD> setmultiport
0 <CMD> list
0 <CMD> stats
0 <CMD> bridge
0 <LIST> stp
0 <CMD> filter
0 <CMD> filterlist
0 <CMD> filterflush
[root @ bridge]$ █
```

The bridge commands are located in the "bridge" directory.

---

### 4.3.1 group

```
group <interface_name> <interface_name> -o -if  
<interface_name> -if <interface_name>
```

Assigns or groups two or more interfaces to the bridge.

#### interface\_name

The name of an interface e.g. eth0, , atm0 ,atm1 etc.

#### EXAMPLE

```
bridge group eth0 -o -if atm0 -if atm1 -if atm2
```

The interfaces eth0, atm1 and atm2 are assigned to the bridge.

```
bridge group eth0 -o -if atm0
```

The interfaces eth0, and atm0 are assigned to the bridge.

### 4.3.2 pvc

```
pvc add <port> <vpi> <vci> <encap> -o [-vpn <OUI> <vpnId>]
```

```
pvc delete <port> <vpi> <vci> <encap>
```

Attaches a PVC to the WAN interface.

#### add

Adds the specified PVC to the bridge.

#### delete

Deletes the specified PVC to the bridge.

#### <port>

A string identifying the wan interfaces e.g. atm0.

---

**<vpi> <vci>**

Virtual Path Identifier and Virtual Circuit Identifier for the ATM connection.

**<encap>**

Specifies the encapsulation type. The possible values are llc or vc which represent Logical Link Control or VC multiplexing respectively.

**-vpn <OUI> <vpnId>**

Specifies the VPN encapsulation. The OUI (Organizationally Unique Identifier) and VPN identifier are specified as numbers.

### 4.3.3 **cachetimer**

**cachetimer <timeout>**

Specifies the idle timeout for bridge table entries. The timeout value is in seconds. Whenever there is any traffic passing through bridge, bridge will maintain the lookup table with the MAC addresses coming from configured interface( through LAN). If the traffic is destined to any MAC address which is found in the lookup table, that packet is not sent to the ATM interface. If there is no traffic from particular machine for certain time period then that entry is deleted from the lookup table. The time that the bridge will clear the bridge lookup entry is the cachetimer timeout.

### 4.3.4 **setmultiport**

**setmultiport enable | disable**

Enables or disables flooding between ATM PVCs.

---

### 4.3.5 list

#### list

Lists bridge parameters.

### 4.3.6 stats

#### stats

Displays bridge statistics.

### 4.3.7 bridge

#### bridge enable | disable | delete

Enables, disables, or deletes the configuration of the bridge.

### 4.3.8 filter

#### filter <action> <mac\_address> -o [-fwd | -drop]

Configures the filtering capability of MAC addresses for the bridge. Up to 128 addresses maybe specified.

#### <action>

Action may be add, delete, or modify.

#### <mac\_address>

The MAC address that is to be filtered. The address is specified by a hex code for each byte separated by a colon (:). For example:

00:01:33:44:5F:2C.

#### -fwd

When specified, the frame will be forwarded. This is the default.

---

### **-drop**

When specified, the frame will be dropped.

#### EXAMPLE

**filter add 1:2:3:4:5:6**

Forward packets whose MAC destination address is 1:2:3:4:5:6.

**filter add 2:3:4:4:5:2 -o -fwd**

Forward packets whose MAC destination address is 2:3:4:4:5:2.

**filter add 11:22:33:44:55:66 -o -drop**

Drop packets whose MAC destination address is 11:22:33:44:55:66

**filter delete 1:2:3:4:5:6**

Remove the filter action for MAC address 1:2:3:4:5:6

**filter modify 2:3:4:4:5:2 -o -drop**

Change the filter action for MAC address 2:3:4:4:5:2 to drop.

#### **4.3.9 filterlist**

**filterlist**

Lists the contents of the filter database.

#### **4.3.10 filterflush**

**filterflush**

Flush the dynamic entries of the filter database.

---

### 4.3.11 stp

The spanning tree commands are located in the "stp" directory (which is located in the "bridge" directory).

#### port

**port <portname> -o -priority <priority> -linkcost <linkcost>**

Specifies properties of the port or interface of the bridge.

#### <portname>

A string identifying the port e.g. eth0, atm0

#### -priority <priority>

A positive integer indicating the port priority. Must be a value between 0 and 255.

#### -linkcost <linkcost>

A positive integer indicating the cost associated with the port. The value can range from 0 to 65535.

#### EXAMPLE

**port eth0 -o -priority 20 -linkcost 100**

Assigns a priority of 20 to Eth0 with a linkcost of 100.

---

## config

**config -o -priority <priority> -hellotime <hellotime>-maxagettime <maxagettime> -fwddelaytime <fwddelaytime>**

Configuring the bridge wide parameters.

**-priority <priority>**

The priority of the individual bridge. The value can range from 0 to 65000. The lower the number, more the priority.

**-hellotime <hellotime>**

The time interval between HELLO bridge protocol data unit. The time interval can be any value between 1 to 10 seconds.

**-maxagettime <maxagettime>**

The maximum age of the stored BPDUs. The time interval can be any value between 1 and 60 seconds.

**-fwddelaytime<fwddelaytime>**

The time spent by bridge in the listening and learning state before moving to learning or forwarding state respectively. The time interval can be any value between 10 and 200 seconds.

## span

**span enable | disable**

Enables to disable the spanning tree protocol.

---

list

**list**

Lists the spanning tree configuration.



---

## 4.4 SNMP

Snmp commands allow listing and setting of current SNMP configuration.

```
[root @ home]$ snmp
[root @ snmp]$ ls

A <CMD> list
A <CMD> sysconf
A <CMD> shutdown
A <CMD> start
A <CMD> comconf
A <CMD> delcomm
A <CMD> trapconf
A <CMD> agconfig
A <CMD> trap
[root @ snmp]$
```

---

#### 4.4.1 List

##### list

This command lists the current SNMP configuration like system version, system contact, System location, system id etc.

##### EXAMPLE

```
[root @ snmp]$ list
      SNMP Agent
=====
STATUS      : Running
TRANSPORT   : 172.16.11.111/161
System Version Description :
System Contact :
System Location :
System ID   : 4242
=====
Trap Server Configurations
=====
Index  Version  IP-Address  Community  Status
-----
1      SNMP-V1  0.0.0.0    public     disable
2      SNMP-V2  0.0.0.0    public     disable
-----
Communities
=====
Index  IP-Address  Community  Access
-----
[root @ snmp]$
```

---

#### 4.4.2 Set

**set [-d] [-c] [-l] [-i] [-t] [-s1] [-s2] value**

This command allows modification of any current SNMP configuration

**-d value**

System Version Description

**-c value**

System Contact.

**-l value**

System Location

**-i value**

Assigned Enterprise Number.

**-t value**

Trap Server IP Address.

**-r value**

Community for reading MIB.

**-s1 value**

Community for modifying MIB.

**-s2 value**

Community for modifying MIB.

#### 4.4.3 shutdown

**shutdown**

This command shutdown the SNMP agent.

---

#### 4.4.4 `sysconf`

```
[root @ snmp]$ sysconf
sysconf [-d] [-c] [-l] [-i] value
-d: System Version Description
-c: System Contact
-l: System Location
-i: Assigned Enterprise Number
[root @ snmp]$
```

The `sysconf` command configures system version description, system contact, system location, and assigned enterprise number.

#### EXAMPLE

```
[root @ snmp]$ sysconf -d office1
```

This command configures the system version description to office1.

---

## 4.5 Firewall

Stateful dynamic filtering with transparent proxies is provided to meet the demanding security needs of today's Internet. Stateful firewalls store state and context data, which are updated dynamically. This provides virtual session information for tracking connection-oriented and connectionless protocols. Each connection also keeps the set of actions that need to be performed on the packets, to avoid the classification process for further IP datagrams in the same connection. Once the connection entry for a flow is created, then all other packets that belong to the connection only need to recognize the classification for flow identification. This way, the throughput is significantly boosted.

The firewall commands are in the qosc directory. Type qosc at the [root @ home]\$ prompt to enter the directory.

---

### 4.5.1 Firewall on and off

The firewall function is disabled by default. To enable it, use the following command

```
[root @ qosc]$ fw on
```

Use the following command to disable firewall.

```
[root @ qosc]$ fw off
```

### 4.5.2 addrule

Adds a firewall policy

USAGE

```
addrule priority -o [-da address] [-sa address] [-p protocol] [-dp  
portNum] [-spportNum] [-tos serviceType] [-type icmp-types] [-flg  
tcp-flags] [-tc actionID] [-fw actionID]
```

EXAMPLE

```
[root @ qosc]$ addrule 100 -o -sa 192.167.28.190 -p tcp -fw 3
```

---

### 4.5.3 `listrule`

Lists a firewall policy

USAGE

```
listrule <rule id>
```

EXAMPLE

### 4.5.4 `listrules`

Lists all firewall policies

USAGE

```
listrules
```

EXAMPLE

```
[root @ qosc]$ listrules
ID: 1 PRI: 30001 [DST: 192.167.27.190/32] [PROTO: icmp] [FW:1]
ID: 2 PRI: 30000 [SRC: 192.168.1.0/24] [FW: 2]
ID: 3 PRI: 29000 [PROTO: udp] [DP: =67] [FW: 3]
ID: 4 PRI: 29000 [PROTO: udp] [SP: =520] [DP: =520] [FW: 4]
```

---

### 4.5.5 deleterule

Deletes a firewall policy

#### USAGE

**deleterule <rule id> -o -[action type]**

action type : tc/TC or fw/FW. If action type is specified then only the action part is deleted and not the rule. If action type is not specified or if the specified action type is the only action present in the rule then the rule is also deleted.

#### EXAMPLE

```
[root @ qosc]$ deleterule 5 -o -fw
```

### 4.5.6 ADDFW

Adds a firewall action

#### USAGE

**addfw action -o [-ifa interface] [-dir direction] [-time time] [-code icmp-unreach-code]**

#### EXAMPLE

```
[root @ qosc]$ addfw allow -o -ifa eth0 -dir in
```

```
Firewall action Id : 5
```



---

## 4.5.7 LISTFW

Lists the firewall actions

### USAGE:

```
listfw Id          where (0 < id < 1000)
```

### EXAMPLE

```
[root @ qosc]$ listfw 1
      FIREWALL ACTIONS
-----
 Id   Interface  Direction  Day-Time To Day-Time Action
 1    eth0        in         sun 0:00  sat 23:59  allow
[root @ qosc]$ █
```

---

## 4.5.8 LISTALLFW

Lists all configured actions

### USAGE:

```
listallfw
```

### EXAMPLE

```
[root @ qosc]$ listallfw
      FIREWALL  ACTIONS
-----
  Id  Interface  Direction  Day-Time  To Day-Time  Action
  ---  ---
  1   eth0       in         sun 0:00   sat 23:59   allow
  2   eth1       in         sun 0:00   sat 23:59   allow
  3   wlan0      in         sun 0:00   sat 23:59   allow
  4   any        any        sun 0:00   sat 23:59   allow
[root @ qosc]$ █
```

---

#### 4.5.9 DELFW

Deletes specified firewall action

**USAGE:**

delfw Id                    where (0 < id < 1000)

---

## 4.6 NAT (optional)

```
nat -o [-interface <interface>]
[-unregistered_only yes | no]
[-deny_incoming <yes | no>]
[-same_ports yes | no]
[-flush yes | no]
[-permanent_link tcp | udp src:port dst:port alias]
[-alias_address <addr>]
[-redirect_port tcp | udp <local_addr>[:<local_port>]
<public_addr>:<public_port>
[<remote_addr>[:<remote_port>]]]
[-redirect_addr <local_addr> <public_addr>]
[-display]
[-disable]
[-status]
```

Network Address Translation (NAT) hides internal IP addresses of a network from the outside world and provides access to the Internet for multiple machines using a single or fixed number of public IP addresses. The NAT framework supports both dynamic and static NAT. The `nat` command enables dynamic NAT processing.

---

With the nat command, all private addresses are mapped to the IP address of the specified WAN interface.

**<interface>**

Configure the specified WAN interface to use dynamic Network Address Translation. For all packets transmitted from the WAN interface, the source address is modified to use IP address of the WAN interface. The source port of the packet may be modified as required. Packets received on the WAN interface will have their destination address modified appropriately to reach the appropriate machine on the LAN network.

**-alias\_address <ip\_address>**

The source address field of the outbound packets from the WAN interface will be overwritten with the specified ip\_address.

**-unregistered\_only [yes | no]**

If yes, only the outbound packets with unregistered source IP addresses are translated. All the outbound packets with the registered source IP addresses are forwarded on the WAN interface without translation. This is useful if you have one more subnet having a registered IP address that shares the common WAN link with the subnet having an unregistered IP address.

Registered addresses are addresses reachable and advertised in the Internet whereas unregistered addresses are private addresses which are not reachable through the Internet. Currently there is no command to display registered addresses.

**-deny\_incoming [yes | no]**

If yes, nat will not allow any incoming connections. The default is yes.

---

**-same\_ports [yes | no]**

If yes, nat will try to retain the source port without modification for outgoing packets. This can only be done if the port is not already in use by another connection. The default is yes.

**-flush [yes | no]**

If yes, all the permanent links (Redirect links) will be flushed.

**-permanent\_link tcp|udp src:port dest:port alias**

Defines a permanent link for an incoming connection.

**-alias\_address <addr>**

Enables NAT on the interface associated with the specified IP address (<addr>).

**-redirect\_port tcp|udp <local\_addr>[:<local\_port>]**

**<public\_addr>:<public\_port>[<remote\_addr>[:<remote\_port>]]**

Redirects incoming packets from the WAN to a specified IP address on the LAN. Packets arriving with a destination IP address of public\_addr and a port of public\_port are forwarded to the machine with the IP address of local\_addr. The port number is modified to local\_port if specified.

Note the protocol (tcp/udp) must be specified. Optionally the source IP address and source port can be specified (remote\_addr and remote\_port).

**-redirect\_addr <local\_addr> <public\_addr>**

Redirects incoming packets from the WAN to a specified address (local\_addr) on the LAN without changing port numbers. Packets arriving with a destination IP address of public\_addr are forwarded to the machine with the IP address of local\_addr.

**-disable**

The Option is used to disable the nat interface.

---

**-status**

This will display all the configured options on the nat interface.

**-display**

This will display all the configured redirect addresses and redirect port mappings.

**EXAMPLE**

**nat -o -interface atm0**

Configures the WAN interface atm0 to use network address translation.

**nat -o -alias\_address 202.54.30.50**

Configures alias address as 202.54.30.50 and maps this IP address to a interface and takes that as NAT interface.

**nat -o -unregistered\_only yes**

Tells the NAT module to translate only those outgoing packets that bears an unregistered IP address in the source address field of the packet header.

**nat -o -same\_ports yes**

Tells the NAT to try retaining same source port while translating outbound packets. However, if this causes conflict with existing entries in the NAT table then source port will be modified.

**nat -o -disable**

Disables the nat interface.

**nat -o -status**

Displays all the options on nat interface.

---

## 4.7 HTTP proxy

Proxy servers restrict users from communicating directly with the public servers. A proxy server takes the user's request for Internet services (such as HTTP, FTP and Telnet) and forwards them to the actual servers after proper authentication. Secondary sets of rules are applied to the application data to provide further security from the known threats associated with these applications. These proxies support URL filtering (specified web links).

### 4.7.1 HTTPPROXY

Configures HTTP proxy including authentication and display of statistics.

#### DESCRIPTION

The option "-auth" enables or disables user authentication.

The option "-display" displays the authentication mode.

The option "enable" enables the HTTP proxy.

The option "disable" disables the HTTP proxy.

The option "-stat" displays all the statistics information.

#### USAGE

```
httpproxy -o [-auth {enable/disable}]
```

```
httpproxy -o -display
```

```
httpproxy -o enable
```

```
httpproxy -o disable
```

```
httpproxy -o -stat
```



---

## 4.8 DHCP server

The `dhcpserver` command configures the DHCP server function. All the commands to set up the DHCP server are shown below.

```
[root @ home]$ dhcpserver
[root @ dhcpserver]$ ls

O <CMD>  start
O <CMD>  stop
O <CMD>  subnet
O <CMD>  host
O <CMD>  lease
```

### 4.8.1 start

#### **start**

Starts the DHCP server. The `subnet` and `host` commands are used to configure DHCP server.

### 4.8.2 stop

#### **stop**

Stops the DHCP server. This command is available in the `dhcpserver` directory.

---

### 4.8.3 subnet

**subnet if add** -o -subnet <subnet> -netmask <mask> -startip <startip> -endip <endip> -leasetime <lease time in days> -broadcast <broadcast-address> -dns <name-server> -dns2 <name-server2> -gateway <gateway> -server <serverip> -file <filename>

**subnet if delete**

**subnet if list**

Configuration of DHCP to serve the specified IP addresses. The add option is used to specify the IP addresses and other aspects of the configuration. The list option shows the configured subnets. The delete command removes the serving of the specified subnet.

These commands take effect after the start command has been issued.

These commands are available in the dhcpserver directory.

**-subnet <subnet>**

The subnet that the server will serve IP addresses on.

**-netmask <mask>**

The subnet mask for the subnet that the server will serve IP addresses on.

**-startip <startip> -endip <endip>**

The range of IP addresses that will be served. The startip and endip define this range with the beginning and ending IP addresses to be served. These addresses are specified in dot notation.

**-gateway <gateway-address>**

The IP address of the gateway. This information is passed to the DHCP clients which they use for a default route entry. By default the IP address of this router is passed to the DHCP clients as the gateway.

---

**-leasetime <leasetime>**

The amount of time the DHCP lease of the IP address will last. This is specified in days. The default is 7 days.

**-broadcast <broadcast-address>**

The IP broadcast address that the server will listen to for DHCP requests. By default a standard broadcast address for the subnet is used.

**-dns <name-server>**

The IP address of the DNS server that should be passed to DHCP clients. By default the dns address configured on the WAN interface from the Internet Service Provider (via DHCP server or PPPoA/PPPoE) is used.

**-server <server> -file <filename>**

These options are used to support Bootp clients. The client will go to the specified server to retrieve the specified file as the boot image. The 6680 based router does not support storage of a file for a remote client to boot from. So the server specified will be another machine on the network.

EXAMPLE

```
subnet add -o -subnet 192.168.5.0 -startip 192.168.5.200 -endip  
192.168.5.210 \-leasetime 3 -dns 192.168.5.7
```

IP addresses will be assigned to up to 11 DHCP clients. The IP addresses assigned will begin with 192.168.5.200 and end with 192.168.5.210. The length of the IP address assignment (the lease) is 3 days. The address of the DNS server (192.168.5.7) will also be sent to the DHCP clients.

```
subnet delete -o -subnet 192.168.5.0
```

The DHCP server will no longer serve address for the 192.168.5.0 network.

---

#### 4.8.4 host

```
host add -o -macaddr <mac-address> -ipaddr <ipaddr>  
[-leasetime <lease time>][-gateway <gateway-address>]  
[-broadcast <broadcast-address>][-dns <name-server>]  
[-server <server-name>] [-file <filename>]
```

```
host list
```

```
host delete -o -macaddr <mac_address>
```

These commands control the configuration of specific hosts and are useful when specific machines need to have permanent IP addresses assigned to specific machines. The host commands have precedence over subnet commands. The add option is used to specify the IP address for a particular host. The list option shows the configured hosts. The delete option will remove a host configuration. These commands are available in the dhcpserver directory.

EXAMPLE

```
host add -o -macaddr 00.00.00.d1.26.95 -ipaddr 192.168.5.34
```

Specifies that the machine with the MAC address of 00.00.00.d1.26.95 will be assigned the IP address 192.168.5.34.

```
host delete -o -macaddr 00.00.00.d1.26.95
```

Removes this host configuration for the machine with the MAC address of d1.26.95.

---

#### 4.8.5 lease

**lease list**

**lease delete -o -ipaddr <ipaddr>**

Displays or deletes the lease configuration. Leases represent which IP addresses are allocated to which machines and for how long. The list option lists all outstanding leases.

**delete -o -ipaddr <ipaddr>**

Deletes the lease for the specified IP addresses. Dot notation is used to specify the IP address.

#### 4.9 DHCP relay

**dhcpr start -o <remote\_server>**

**dhcpr stop**

**dhcpr status**

The dhcpr command is used for setting up the DHCP relay function. The system acts as a proxy for DHCP requests. When enabling the DHCP Relay, the address of the DHCP server is specified and DHCP requests are relayed to the specified server. On enabling DHCP relay functionality, the DHCP server functionality gets disabled (if it is enabled) and vice versa.

**start -o <remote\_server>**

Starts DHCP relay. The remote\_server is the IP address of the DHCP server.

---

**stop**

Disables or stops the DHCP relay service.

**status**

Shows the status of the DHCP Relay.

## 4.10 ADSL

The `adsl` command configures and displays all the ADSL-relevant functions.

Those commands are shown below.

```
[root @ home]$ adsl
[root @ adsl]$ ls
O <CMD> setmode
O <CMD> showmode
O <CMD> readblkcmv
O <CMD> readcmv
O <CMD> writecmv
O <CMD> mon
O <CMD> eread
O <CMD> ewrite
O <CMD> mread
O <CMD> mwrite
O <CMD> addusercmv
O <CMD> delusercmv
O <CMD> listusercmv
O <CMD> adslup
O <CMD> adslown
O <CMD> tone
O <CMD> bitalloc
O <CMD> adslstat
[root @ adsl]$
```

---

#### 4.10.1 **setmode**

**setmode <mode>**

Sets the mode of the ADSL link to ANSI (T1.413), G.DMT, G.Lite, or multi-mode. After executing this command, the configuration can be saved and the next time the machine is rebooted, the mode will take effect.

**<mode>**

The mode may be ansi, gdmt, glite, or multi.

#### 4.10.2 **readcmv**

**readcmv <cmv\_index> <offset>**

The ADSL Configuration and Management Variables (CMV) can be read with the readcmv command. The CMV variables are documented in "CMV Reference Manual". This command will only provide meaningful results when the link is operational.

**<cmv\_index>**

The cmv index may be one of the following values.

Note that they must be specified in uppercase: ADPT, CNTL, CODE, DIAG, DOPT, FLAG, INFO, INTL, MASK, OPTN, PFCL, PFRX, PFTX, PSDM, RATE, RXDA, STAT, TEST, TONE, TXDA, UOPT.

**<offset>**

This is a numeric value between 0 and 65535.

---

### 4.10.3 writecmv

**writecmv <cmv\_index> <offset> <value>**

The ADSL Configuration and Management Variables (CMV) can be written with the writecmv command. The CMV variables are documented in "CMV Reference Manual". This command will take effect only after the link is reconnected.

**<cmv\_index>**

The cmv index may be one of the following values. Note they must be specified in uppercase: ADPT, CNTL, CODE, DIAG, DOPT, FLAG, INFO, INTL, MASK, OPTN, PFCL, PFRX, PFTX, PSDM, RATE, RXDA, STAT, TEST, TONE, TXDA, UOPT.

**<offset>**

This is a numeric value between 0 and 258.

**<value>**

The value for the variable specified in hexadecimal format.

### 4.10.4 mon

**mon**

Displays the state of the ADSL connection. Only gives meaningful information when the link is operational.



---

#### 4.10.5 **addusercmv**

**addusercmv** <cmv\_name> <offset> <value> <command>  
<msgid>

Allows the adding or setting of a CMV. The CMV values will be used the next time the system is rebooted. Note that the configuration must be saved after using this command in order for them to take effect on the next reboot.

**<cmv\_name>**

The following values are permitted for the cmv name: MASK, OPTN, PSDM, RXDA, TEST, TXDA, or ADPT.

**<offset>**

The offset value which is a decimal in the range of 0 to 65535.

**<value>**

Value of the CMV. Value is expected in hexadecimal format.

**<command>**

Type of operation ( Read or Write ).

**<msgid>**

Message Id in decimal digits.

#### 4.10.6 **delusercmv**

**delusercmv** <index>

Deletes the specified user CMV. The user cmv was added with the "addusercmv" com-mand.

**<index>**

Index of CMV as displayed by "listusercmv".

---

#### 4.10.7 listusercmv

##### listusercmv

Lists the User CMVs added by the 'addusercmv' command.

#### 4.10.8 erread

##### erread <offset> <size>

Displays the Eagle 16 bit data memory

<offset >

0 - 3ffff (hexadecimal)

< size >

1 - 256 (decimal)

#### 4.10.9 ewrite

##### ewrite <offset> <value>

Write 1 16-bit word into Eagle 16 bit data memory

<offset >

0 - 3ffff (hexadecimal)

< value >

0 - ffff (hexadecimal)

#### 4.10.10 mwrite

##### mwrite <offset> <value>

Write 1 32-bit word into Eagle 16 bit data memory

---

**<offset >**

0xa0000000 - 0xbfffffff (hexadecimal)

**< value >**

0 - ffffffff (hexadecimal)

#### **4.10.11 mread**

**mread <offset> < size >**

Displays the Falcon 32 bit data memory.

**<offset >**

0xa0000000 - 0xbfffffff (hexadecimal)

**< size >**

1 - 100 (decimal)

#### **4.10.12 adslup**

**adslup**

Starts the ADSL link

#### **4.10.13 adslidown**

**adslidown**

Terminates the ADSL link

---

#### 4.10.14 `tone`

`tone offset1 offset2`

offset1 and offset2 are the numeric value from 0 to 287

To read all the tone information, enter the command:

`Tone 0 287`

To read the tone 11 to 20 information, enter the command:

`Tone 11 20`

#### 4.10.15 `bitalloc`

`bitalloc`

read the bit allocation information

#### 4.10.16 `adslstat`

`adslstat`

display the current ADSL link status. For example, if the ADSL link is down, it displays the following information after typing `adslstat`.

```
[root @ adsl]$ adslstat
```

```
The current ADSL status is STATE_UNTRAINED.
```

```
[root @ adsl]$
```

---

## 4.11 DNS

Commands for setting DNS parameters are in the "dns" directory. From the "home" directory, type "dns" to enter the directory. The available commands are shown below after typing ls. Among the commands, **help** is used to give instructions about how to use the other commands.

```
[root @ home]$ dns
[root @ dns]$ ls

A <CMD> list
A <CMD> help
A <CMD> set
A <CMD> dnsr
[root @ dns]$
```

### 4.11.1 set

**set -d <domain\_name>**

**set [-n1 <name\_server>] [-n2 <name\_server>]**

Sets DNS entries for the system. The domain\_name specifies the name of this domain for the router. The name\_server specifies the IP address of the server resolving DNS requests. To clear a domain entry, specify double quotes ("") for the domain name. To clear the name server entry, specify

---

0 as the name server.

**-n1 <name\_server>**

Used to specify the primary name server.

**-n2 <name\_server>**

Used to specify the secondary name server.

EXAMPLE

```
[cli @ dns]$ set -d wang.com
```

Sets the domain name to "wang.com".

```
[cli @ dns]$ set -d ""
```

Removes the domain name.

```
[cli @ dns]$ set -n1 137.23.41.2
```

Sets the primary name server for DNS queries.

```
[cli @ dns]$ set -n1 0
```

Removes the primary name server.

#### 4.11.2 **dnsm**

```
dnsm start -o [<server1>] [<server2>]
```

```
dnsm stop -o [<server1>] [<server2>]
```

Enables/Disables the DNS relay function.

**start**

Starts the DNS relay function

**stop**

Stops the DNS relay function.

---

**<server1>**

IP address of the primary DNS server.

**<server2>**

IP address of the secondary DNS server.

### **4.11.3 list**

**list**

Lists DNS domain name and name server.

### **4.11.4 dhcpr**

**dhcpr start -o <remote\_server>**

**dhcpr stop**

**dhcpr status**

---

## 4.12 IGMP Proxy

To set up the igmp proxy, use the command `igmp proxy` to display the commands for IGMP.

```
[root @ home]$ igmp help
    igmp -o -proxyif <interface> : To set proxy interface
    igmp -o -routerif <interface> : To set router interface
    igmp -o -deleteif <interface> : To delete either proxy or router
interface
    igmp -o -display : To display the groups in all interfaces
[root @ home]$
```

**igmp -o -proxyif <interface>**

**igmp -o -routerif <interface>**

**igmp -o -deleteif <interface>**

**igmp -o -display**

Used for configuring igmp proxy and router interfaces.

**-proxyif <interface>**

Sets the proxy interface. Typically a LAN interface (eth0) is specified.

**-routerif <interface>**

Sets the router interface. Typically a WAN interface (ATMO, PPP0) is specified.



---

**-deleteif <interface>**

Deletes either the proxy or router interface.

**-display**

Displays the group in all interfaces.

## 4.13 Rip

RIP is a protocol that automatically updates the routing entries on the system. This is done by cooperating with other nearby routers. The RIP commands are located in the "rip" directory. Two commands are available: rip and ver. In order for any configuration changes to take effect, the configuration must be saved (with "save" command) and the system rebooted. The available commands are shown below.

```
[root @ home]$ rip
[root @ rip]$ ls

O <CMD>  rip
O <CMD>  ver
O <CMD>  silent
O <CMD>  list
[root @ rip]$
```

---

### 4.13.1 rip

**rip -o <ON|OFF>**

rip starts and stops automated updates of routing tables. When RIP is enabled, the system communicates with other routers in the network to update and maintain the IP routing tables. By default, RIP is not enabled. If RIP is enabled but no version is specified, RIP version 1 is used. This command is available in the "rip" directory.

To enable RIP, type the following command with ON capitalized.

```
[root @ rip]$ rip -o ON
```

A change success message displays.

```
RIP Status changed successfully.
```

To disable the RIP function, use the following command with OFF capitalized.

```
[root @ rip]$ rip -o OFF
```

### 4.13.2 ver

**ver -o <1|2>**

Specifies the version of the RIP protocol that will be used. The permissible values are 1 or 2.

---

### 4.13.3 silent

**silent -o <mode>**

**mode - enable or disable**

Sets up the RIP silent. The default is disabled.

### 4.13.4 list

**list**

Lists the routes currently available.

## 4.14 SNDCP

The SNDCP commands are located in the "sndcp" directory.

### 4.14.1 pppoe

pppoe <profile> -o -if <interface> -user <user> -pass <password> -vpi  
<vpi> -vci <vci> [-encap <encapsulation>] [-restarttime <timeout>]  
[-auth <authentication>] [-myaddr <ip\_addr>] [-peer <peer\_addr>]  
[-mtu <mtu>] [-mru <mru>] [-hwaddr <addr>] [-service  
<service\_name>] [-acname <ac\_name>] [-tag <host\_tag>][[-mode  
AUTO|DIRECT] [-idletime <idletime>][[-nat enable|disable] [-netmask  
<mask>][[-vpn <OUI> <vpnid>]

Sets up a PPPoE profile.

---

**profile**

Profile number to configure. Specify an integer number from 0 through 7.

**-if <interface>**

Interface name with unit number. Four PPP interfaces are available: ppp0, ppp1, ppp2, ppp3, ppp4, ppp5, ppp6, ppp7

**-user <user>**

Username. This string can be up to 30 characters.

**-pass <password>**

Password. This string can be up to 30 characters.

**-vpi <vpi>**

The ATM vpi value which was assigned in a vcadd command or listed in a atmshowconn command.

**-vci <vci>**

The ATM vci value which was assigned in a vcadd command or listed in a atmshowconn command.

**-encap <encapsulation>**

Encapsulation type. Possible values are LLC (Logical Link Control) or VC (VC Multiplex-ing).

**-restarttime <timeout>**

Timeout in milliseconds. The default is 3 seconds (3000 milli seconds).

---

**-auth <authentication>**

Authentication type (pap, chap, mschapv1, mschapv2).

**-myaddr <ip\_addr>**

Desired self IP Address (eg 192.168.26.7). Expressed in dot notation.

**-peer <peer\_addr>**

Peer IP Address to optionally specify the address of the Internet Service Provider. Expressed in dot notation.

**-mtu <mtu>**

Maximum Transmission Unit expressed in bytes. The default is 1492.

**-mru <mru>**

Maximum Receive Unit, negotiated in LCP. The default is 1492.

**-hwaddr <addr>**

Hardware address of the router for this connection. Typically one of the Ethernet hardware addresses of the router are used for this. The address is specified with ':' used as a delimiter between byte values (eg 10:11:12:13:14:15).

**-service <service\_name>**

Service Name.

**-acname <ac\_name>**

Access Concentrator name.

---

**-tag <host\_tag>**

Use host unique tag.

**-mode <mode>**

Mode can be AUTO or DIRECT. In case of mode being set to AUTO the PPPoE negotiation starts only when the system identifies any traffic required to be transferred on the link and in case of DIRECT the PPPoE negotiation is started manually using "pppoestart" command. The default is DIRECT.

**-idletime <idletime>**

The value of idletime is given in minutes and this value indicates how long the link remains up when there is no data transfer over the link. The idle time works only when used in combination with mode AUTO. The default is 60 seconds.

**-nat enable | disable**

Enables or disables NAT (Network Address Translation) for this PPP interface. The default is for NAT to be disabled.

**-netmask <mask>**

Specifies the netmask for the PPP interface. The mask is specified in dot notation (i.e.255.255.255.0).

**-vpn <OUI> <vpnId>**

Specifies the VPN encapsulation. The OUI (Organizationally Unique Identifier) and VPN identifier are specified as numbers.

---

EXAMPLE

**pppoe 1 -o -if ppp0 -vpi 0 -vci 100 -user jones -pass Indiana**

Defines a PPPoE profile. The ppp0 interface is used with the ATM connection vpi 0 and vci 100. The user name is "jones" and the password is "Indiana".

#### 4.14.2 **pppoedefault**

**pppoedefault <profile>**

Configures the specified profile as the default PPPoE connection. This profile must be using "auto" mode. Out of all the profiles which are using the "auto" option, only one can be run at a time. This command is used to specify that profile. If the "pppoedefault" command is not used, the first profile that used the "auto" option is used as the default.

#### 4.14.3 **pppoestart**

**pppoestart <Profile>**

Starts PPPoE given the specified profile. The profile is specified with an integer (0, 1, 2). The profile was previously specified with the pppoe command.

#### 4.14.4 **pppoestop**

**pppoestop <Profile>**

Stops PPPoE given the specified profile. The profile is specified with an integer (0, 1, 2). The profile was previously specified with the pppoe

---

command.

#### 4.14.5 `pppoelist`

**`pppoelist [-profile Profile]`**

Displays the listing of all available free profiles. If `-profile` is not specified, this command will display all the valid configured profiles.

#### 4.14.6 `pppoedel`

**`pppoedel <profile> | all`**

Deletes the specified profile. Profile is specified as a number (see `pppoe` command). If `all` is specified the all profiles are deleted. This command only deletes inactive profiles. If a profile is in use, it must be stopped before it can be deleted.



---

#### 4.14.7 pppoa

```
pppoa <profile> -o -if <interface> -user <user> -pass  
<password> -vpi <vpi> -vci <vci>[-encap <encapsulation>]  
[-restarttime <timeout>] [-auth <authentication>] [-myaddr  
<ip_addr>] [-peer <peer_addr>] [-mtu <mtu>] [-mru  
<mru>][[-nat enable | disable] [-netmask <mask>][[-vpn <OUI >  
<vpnid>]
```

Sets up a PPPoA profile.

##### **profile**

Profile number to configure. Specify an integer number from 0 through 7.

##### **-if <interface>**

Interface name with unit number. Four PPP interfaces are available: ppp0, ppp1, ppp2, ppp3, ppp4, ppp5, ppp6, and ppp7.

##### **-user <user>**

Username.

##### **-pass <password>**

Password.

##### **-vpi <vpi>**

The ATM vpi value which was assigned in a vcadd command or listed in a atmshowconn command.

##### **-vci <vci>**

The ATM vci value which was assigned in a vcadd command or listed in a atmshowconn command.

---

**-encap <encapsulation>**

Encapsulation type. Possible values are LLC or VC.

**-restarttime <timeout>**

Timeout in milliseconds. The default is 3 seconds (3000 milli seconds).

**-auth <authentication>**

Authentication type (PAP or CHAP).

**-myaddr <ip\_addr>**

Desired self IP Address (eg 192.168.26.7). Expressed in dot notation.

**-peer <peer\_addr>**

Peer IP Address to optionally specify the IP address of the Internet Service Provider. Ex-pressed in dot notation.

**-mtu <mtu>**

Maximum Transmission Unit expressed in bytes. The default is 1500.

**-mru <mru>**

Maximum Receive Unit, negotiated in LCP. The default is 1500.

**-nat enable | disable**

Enables or disables NAT (Network Address Translation) for this PPP interface. The default is for NAT to be disabled.

**-netmask <mask>**

Specifies the netmask for the PPP interface. The mask is specified in dot notation (i.e.255.255.255.0).

---

**-vpn <OUI> <vpnId>**

Specifies the VPN encapsulation. The OUI (Organizationally Unique Identifier) and VPN identifier are specified as numbers.

EXAMPLE

**pppoa 1 -o -if ppp0 -vpi 0 -vci 100 -user jones -pass Indiana**

Defines a PPPoA profile. The ppp0 interface is used with the ATM connection with vpi 0 and vci 100. The user name is "jones" and the password is "Indiana".

#### **4.14.8 pppoastart**

**pppoastart <Profile>**

Starts PPPoA given the specified profile. The profile is specified with an integer (0, 1, 2). The profile was previously specified with the pppoa command.

#### **4.14.9 pppoastop**

**pppoastop <Profile>**

Stops PPPoA given the specified profile. The profile is specified with an integer (0, 1, 2). The profile was previously specified with the pppoa command.

#### **4.14.10 pppoalist**

**pppoalist [-profile Profile]**

Displays the listing of all available free profiles. If -profile is not specified, this command will display all the valid configured profiles.

---

#### 4.14.11 `pppoadel`

**`pppoadel <profile> | all`**

Deletes the specified profile. Profile is specified as a number (see `pppoa` command). If `all` is specified, then all profiles are deleted. This command only deletes inactive profiles. If a profile is in use, it must be stopped before it can be deleted. Displays the listing of all available free profiles. If `-profile` is not specified, this command will display all the valid configured profiles.

#### 4.14.12 `pppoadefault`

**`pppoadefault <profile>`**

Configures the specified profile as the default PPPoA connection. This profile must be using "auto" mode. Out of all the profiles which are using the "auto" option, only one can be run at a time. This command is used to specify that profile.

#### 4.14.13 `list`

**`list <param>`**

Displays the configurations of IPOA/BRIDGE/ROUTEDBRIDGE.

**`<param>`**

param can be bridge / routedbridge / ipoa.

EXAMPLE

**`list bridge`**

Displays Bridge parameters.

**`list routedbridge`**

Displays Routed Bridge parameters.

---

### **list ipoa**

Displays IPoA parameters.

#### **4.14.14 ipoa**

```
ipoa <interface> enable <vpi><vci> -o [-enc LLC|VC] [default]  
[-nhp <ip_address>][-vpn <OUI> <vpnId>] ipoa <interface>  
disable <vpi><vci> -o [default] [-nhp <ip_address>]
```

Configures the specified WAN interface to use IPoA, which is Classical IP over ATM including Inverse ATM Arp. IPoA uses Inverse ATM Arp to get the peer IP address. The Maximum Transfer Unit (MTU) for IPoA is 9182. Note: In this case, if the peer does not support Inverse ATM Arp, then there will not be any traffic flow. If the nexthop (-nhp option) or default PVC is configured per IPoA, then it does not use Inverse ATM Arp to get the peer IP address.

#### **interface**

The name of the WAN interface. Typically this is 'atm0'.

#### **enable**

Enables this IPoA interface.

#### **disable**

Disables this IPoA interface.

#### **<vpi> <vci >**

These are the vpi, vci values on which ipoa has to be enabled/disabled. vpi,vci are assigned with the vcadd command. The showatmconn command can also be used to list the current ATM connections with their

---

respective vpi and vci values. (Note the vcadd and showatmconn commands are located in the "atm" directory).

**-enc LLC | VC**

Specifies the encapsulation type. The possible values are 'llc' or 'vc' which represent Logical Link Control or VC multiplexing respectively.

**default**

If an entry does not exist for the destination in the inverse ATM Arp table, then the packet is forwarded on the PVC specified.

**-nhp <ip\_address>**

Specifies the next hop IP address of the peer-end.

**-vpn <OUI> <vpnId>**

Specifies the VPN encapsulation. The OUI (Organizationally Unique Identifier) and VPN identifier are specified as numbers.

**EXAMPLE**

**ipoa atm0 enable 0 100 -o -enc LLC**

Establishes an IPoA connection on the WAN interface atm0. VPI, VCI values 0, 100 is used for the ATM connection. LLC encapsulation will be used.

**ipoa atm0 disable 0 100**

Disables the IPoA connection.

---

#### 4.14.15 routedbridge

**routedbridge <interface> disable <vpi><vci>**

**routedbridge <interface> enable <vpi><vci> -o <-encapsulation> <-vpn OUIvpnId>**

Configures the specified WAN interface to use Routed Bridge which is RFC 2684 routing. Note the Maximum Transfer Unit (MTU) for the Routed Bridge is 9182.

##### **interface**

The name of the WAN interface. Typically this is 'atm0'.

##### **enable**

Enables this Routed Bridge interface.

##### **disable**

Disables this Routed Bridge interface.

**<vpi> <vci >**

These are the vpi, vci values on which the Routed Bridge has to be enabled/disabled. vpi,vci are assigned with the vcadd command. The showatmconn command can also be used to list the current ATM connections with their respective vpi and vci values. (Note the vcadd and showatmconn commands are located in the "atm" directory).

**-enc LLC | VC**

Specifies the encapsulation type. The possible values are 'llc' or 'vc' which represent Logical Link Control or VC multiplexing respectively.

---

### **-vpn OUI vpnId**

Enables VPN encapsulation. OUI is organizationally unique identifier.

VpnId is VPN index.

EXAMPLE

#### **routedbridge atm0 enable 0 100 -o -enc LLC**

Establishes a Routed Bridge connection on the WAN interface atm0. VPI, VCI values 0, 100 is used for the ATM connection.. LLC encapsulation will be used.

#### **routedbridge atm0 disable 0 100**

Disables the Routed Bridge connection.

### **4.14.16 1483mer**

#### **1483mer add port vpi vci encapsulation**

Configures the specified WAN interface to use 1483MER (MAC Encapsulation Routing). The "mer" command is used to enable the configuration.

#### **port**

The MER interface name (mer0).

#### **<vpi> <vci >**

These are the vpi, vci values on which the 1483 is configured. vpi,vci are assigned with the vcadd command. The showatmconn command can also be used to list the current ATM connections with their respective vpi and



---

vci values. (Note the vcadd and showatmconn com-mands are located in the "atm" directory). The vpi value is between 0 - 255. The vci value is between 0 - 65535.

**-encapsulation llc | vc**

Specifies the encapsulation type. The possible values are 'llc' or 'vc' which represent Logical Link Control or VC multiplexing respectively.

#### 4.14.17 mer

**mer enable | disable | delete | status**

Enables, disables, deletes or gives status of the 1483MER configurations.

#### 4.14.18 relay

**relay**

**relay -o -client <-if interface> <-pvc vpi vci>**

**relay -o -server <-if interface> <-pvc vpi vci>**

**relay -o enable | disable**

**relay -o -display**

Configures and enables PPPoE relay.

**-client <-if interface> <-pvc vpi vci>**

Specifies the server interface for the PPPoE Relay. The PPPoE server is connected to this interface. The interface may be ppp0, ppp1, ppp2, ppp3, ppp4, ppp5, ppp6, or ppp7.

---

**-server <-if interface> <-pvc vpi vci>**

Specifies the client interface for the PPPoE Relay. The PPPoE clients are connected to this interface. Typically eth0 is specified.

**enable**

Enables the PPPoE Relay feature.

**disable**

Disables the PPPoE Relay feature.

**-display**

Displays the PPPoE Relay configuration.

#### **4.14.19 liststat**

**liststat bridge | routedbridge | ipoa | pppoe | pppoa**

Lists the statistics of the specified module.

#### **4.14.20 Ppptrace**

**ppptrace [on | off ]**

Enables or Disables PPP console messages.

---

## 4.15 atm

### 4.15.1 vcadd

```
vcadd <vpi> <vci> <service> <encaps> -o [-peak <val>] [-avg  
<val>] [-mbs <val>] [-cdvt <val>]
```

Establishes a Permanent Virtual Circuit (PVC) with the specified traffic descriptors. The service specifies the traffic type of the PVC. Permissible values are: cbr, rtvbr, nrtvbr, or ubr. The adaptation parameter is used to specify the type of ATM adaptation layer for which permissible values are aal5 for data connections and aal2 for voice connections.

**<vpi> <vci>**

Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) that identifies this ATM connection. The vpi is an integer number which can range from 0 to 255. The vci is an integer number which can range from 0 to 65,535.

**<service>**

The service specifies the kind of traffic shaping. The possible values are cbr, rtvbr, nrtvbr, or ubr.

**<encaps>**

Specifies whether ATM Adaptation Layer is aal2 or aal5. For voice connections, AAL2 must be specified. For data connections, AAL5 must be specified.

---

**-peak <value>**

Defines the fastest rate a user can send cells to the network. It is expressed in units of cells per second.

**-avg <value>**

Defines the maximum sustainable/average rate a user can send cells to the network. It is expressed in cells per second. This specifies the bandwidth utilization. This value must always be less than or equal to the Peak Cell Rate (see -pcr option).

**-mbs <value>**

Maximum number of cells the user can send at the peak rate in a burst, within the sustainable rate.

**-cdvt <value>**

Constrains the number of cells the user can send to the network at the maximum line rate. It is expressed in microseconds.

**EXAMPLE**

**vcadd 0 38 cbr aal2 -o -peak 1600 -mbs 25 -cdvt 50000**

The following creates a PVC (vpi - 0,vci - 38). Service class is cbr (Constant Bit Rate) and encapsulation as aal2 (for voice). The traffic descriptors are set for peak cell rate of 1600kbps, burst size of 25 cells and cell delay variation of 50000 microseconds.

**vcadd 0 39 ubr aal5**

---

#### 4.15.2 deletevc

**deletevc <vpi> <vci>**

Deletes the specified PVC. The PVC is identified by the vpi / vci values.

EXAMPLE

**deletevc 0 39**

Deletes a PVC with vpi=0 and vci=39.

#### 4.15.3 showatmconn

**showatmconn**

Lists the existing PVCs.

EXAMPLE

**Showatmconn**

**ATM INTERFACE CONFIGURATION INFORMATION**

**MAX INTERFACE VPC's : 10**

**MAX INTERFACE VCI's : 255**

**ILMI VPI VALUE AT THIS INTERFACE : 0**

**ILMI VCI VALUE AT THIS INTERFACE : 16**

**INTERFACE ADMINISTRATIVE ADDRESS : 137.71.139.250**

**ACTIVE VCC CONNECTIONS AT THIS INTERFACE : 2**

---

#### 4.15.4 atmstats

##### **atmstats**

Lists the AAL5 and ATM statistics.

#### 4.15.5 f5lb

**f5lb <vpi> <vci> <flow\_type> -o <LLID>**

This command initiates an F5 loopback.

**<vpi>**

Virtual Path Identifier for the ATM connection.

**<vci>**

Virtual Circuit Identifier for the ATM connection.

**<flow\_type>**

Specifies segment (seg) or end-to-end (ete).

**<LLID>**

The loopback identifier. This is specified as 32 hex digits. The default is:

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

#### 4.15.6 vpadd

**f5lb <vpi> <vci> <flow\_type> -o <LLID>**

This command allows to add and configure VP level atm connection

**<id>**

Connection identification

---

**< vpi >**

vpi number

**< service >**

cbr / rtvbr / nrtvbr / ubr

**< service >**

cbr / rtvbr / nrtvbr / ubr

**<peak val>**

Peak cell rate (in cells/s)

**<avg val >**

Average/minimum (SCR) cell rate (in cells/s)

**<mbs val >**

Burst size in cells

**<cdvt val >**

Cell delay variation tolerance (in micro secs)

---

## 4.16 remote web/telnet/ftp/snmp

remote [web|telnet|ftp|snmp] [on|off][root @ home]\$

Enables or disables the remote access via web, telnet, ftp, or snmp.

EXAMPLE

**[root @ home]\$ remote web on**

enables the remote web access

**[root @ home]\$ remote telnet on**

enables the remote telnet access



---

## Chapter 5 Performance Monitoring

### 5.1 Bitmap

This bitmp show the allocation status of bitmaps like sockets, mbufs and clusters.

```
[root @ home]$ bitmap
sbitmap          : Used = 3 Max = 256
radixMaskBitmap : Used = 1 Max = 10
radixHeadBitmap : Used = 2 Max = 10
rnkeyBitmap      : Used = 5 Max = 300
Route Entries   : Used = 5 Max = 300
UDP connections : Used = 10 Max = 128
rtInfoBitmap    : Used = 0 Max = 10
RAW connections : Used = 0 Max = 10
TCP Connections : Used = 5 Max = 128
Sockets         : Used = 10 Max = 128
Arp entries     : Used = 2 Max = 256
cluBit512       : Used = 0      Max = 75      Failed = 0
cluBit1024      : Used = 1      Max = 75      Failed = 0
cluBit1536      : Used = 0      Max = 120     Failed = 0
cluBit2048      : Used = 54     Max = 600   Failed = 0
mbufBit        : Used = 65     Max = 800   Failed = 0
[root @ home]$ █
```

---

## 5.2 Logger

The logger command displays all the recorded log events. The commands are displayed as follows.

```
[root @ logger]$ ls
A <CMD> logseverity
A <CMD> log
A <CMD> logftpserver
A <CMD> loginfo
A <CMD> logadd
[root @ logger]$
```

This command list is used for display of logging messages.

### 5.2.1 log

**log -o [module name/ log level]**

**log -o [modulename] [log level]**

This command is used to display the log messages based on module name, severity level or log messages based on severity level and module name

**< loglevel >**

Loglevel can be given as exception, error or info.

**< module name >**

---

Module name can be

all,ip,tcp,udp,sockets,rawip,icmp,arp,igmp,app,cdcli,if,telnet,  
dns,snmp,http,ping,ftp,ftpd, tftp, bootp, dhcpc, dhcps, qosbw, ipsec,  
ike,nat,firewall, diffserv, logger, queuing, ipoa, pppoa, ethoa, httpproxy,  
ftpproxy

EXAMPLE

**[root @ logger]\$ log -o all**

“Exception” level log messages and the error or info level log messages ( if enabled) will be logged from all modules.

**[root @ logger]\$ log -o info**

“info” level log messages from all modules or from the modules that have been enabled will be logged.

**[root @ logger]\$ log -o tcp error**

“error” level log messages from tcp module will be logged.

### 5.2.2 logSeverity

logSeverity -o [error/info] [on/off ]

This command is used to set the specified loglevel as ON or OFF. By default, error and info log level messages are off. There is no on/off option for exception log level messages. The exception log messages are always displayed (on).

EXAMPLE

**[root @ logger]\$ logSeverity -o error on**

---

Sets the loglevel error on so that error level log messages are displayed.

```
[root @ logger]$ log -o info off
```

Sets the loglevel info off, so that info level log messages are not displayed.

### 5.2.3 logFtpServer

```
logFtpServer [server_address] [username] [password]
```

This command is used to configure the server address, user name and password of the external ftp server. The log messages are directed to the ftp server given and are logged into a file by name "fwlogfile".

#### EXAMPLE

```
[root @ logger]$ logFtpServer 192.168.1.1 xyz xyz123
```

A file "fwlogfile" having the log message will be created in the ftp server 192.168.1.1

---

## 5.3 Elapsed time

The time command reveals the elapsed time of how long the device is powered on.

```
[root @ home]$ time  
System Elapse Time : 00:37:54:  
[root @ home]$
```

## 5.4 Statistic

The statistic command collects the information about IP, TCP, UDP, and ICMP protocols.

For example, to display the IP statistics, type **statistic IP** to display the IP information.

---

```
[root @ home]$ statistic
      statistic parameter
      parameters - IP|TCP|UDP|ICMP.[root @ home]$ IP
Command not found.
[root @ home]$ statistic IP

IP statistics
ips_total      9018  ips_badsum      0      ips_fragments   0
ips_forward    5192  ips_tooshort    0      ips_badhlen     0
ips_badhlen    0      ips_fragdropped 0      ips_fragtimeout 0
ips_fastforward 0      ips_cantforward 0      ips_redirectsent 0
ips_noproto    60     ips_delivered   8958  ips_localout    5192
ips_odropped   0      ips_reassembled 0      ips_fragmented  0
ips_ofragments 0      ips_cantfrag    0      ips_badoption   0
ips_noroute    0      ips_badvers     0      ips_rawout      0
ips_toolong    0      ips_notmember   0      qosqFullDropped 0
etherqFullDropped 0      ipcqFullDropped 0
```

---

## Chapter 6 TFTP Upload & Download

The TFTP application provides both upload and download functions for the software and configuration settings.

The upload enables the device software (put app) or configurations (put param) uploaded as a file, which can be used for backup and maintenance purposes. The download (get app) of the software is used to upgrade the software, and the download of the configuration (get param) is used to apply the settings of the configuration file to the device.

At the tftp prompt, type ? to display the commands.

```
[root @ home]$ tftp
tftp> ?
Commands may be abbreviated.  Commands are:
connect      connect to remote tftp
mode         set file transfer mode
put          send file
get          receive file
bye          exit tftp
binary       set mode to octet
ascii        set mode to netascii
?            print help information
tftp> █
```

---

Run a TFTP server program. At the TFTP prompt, connect to the TFTP server by typing `connect xxx.xxx.xxx.xxx`. `xxx.xxx.xxx.xxx` is the IP address of the TFTP server. A “connected to : `xxx.xxx.xxx.xxx`” message pops up if the TFTP server is successfully connected. The following is an example.

```
tftp> connect 172.16.4.16  
connected to : 172.16.4.16
```

There are two file transfer mode: binary and ASCII. After connecting to the TFTP server, choose a transfer mode. If you are sure of the mode in use, type `mode` at the prompt.

```
tftp> mode  
Using octet mode to transfer files. or Using netascii mode to transfer files.
```

The message “Using octet mode to transfer files” or “using netascii mode to transfer files” displays for your reference.

To return to the root prompt, use the `bye` command.

The following sections of this chapter will describe the procedures for the upload and download. In all the examples used in these sections, the TFTP server IP address, `172.16.4.16` and file name are only used for reference. You must change them to fit your own settings if they are different in real application.



---

## 6.1 Uploading the software file

1. At the tftp prompt, type connect xxx.xxx.xxx.xx.

```
tftp> connect 172.16.4.16
```

```
connected to : 172.16.4.16
```

A connected to : xxx.xxx.xxx.xxx pops up if successful.

2. Type the transfer mode (binary or ascii).

```
tftp> binary
```

```
mode set to octet
```

A message, mode set to octet/netascii, pops up.

3. Type put app \*\*\*. \*\*\* is the software file name.

```
tftp> put app ***
```

You can also skip the file name by simply typing put app. The file will then be saved as app at the target location.

4. The following message pops up if the software upload is successful.

```
putting app to xxx.xxx.xxx.xxx : *** [octet]
```

---

**Sent bytes in seconds**

```
tftp> connect 172.16.4.16
connected to : 172.16.4.16
tftp> binary
mode set to octet
tftp> put app sw2003.bin

putting app to 172.16.4.16 : sw2003.bin [octet]

Sent 983040 bytes in 3 seconds
tftp>
```

---

## 6.2 Uploading the configuration file

To upload the configuration file, use the put param command.

1. At the tftp prompt, type connect xxx.xxx.xxx.xx.

```
tftp> connect 172.16.4.12
connected to : 172.16.4.12
```

A message, "connected to : xxx.xxx.xxx.xxx," pops up if successful.

2. Type the transfer mode (binary or ascii).

```
tftp> binary
mode set to octet
```

A message, "mode set to octet/netascii," pops up.

3. Type put param \*\*\*. \*\*\* is the configuration file name.

```
tftp> put param ***
```

If the configuration file name is param, you can also skip the file name by simply typing put param.

4. The following message pops up when the upload is successful.

---

putting param to xxx.xxx.xxx.xxx : config.txt [octet]

Sent bytes in seconds

Below is an example of the configuration upload procedures.

```
[root @ home]$ tftp
tftp> connect 172.16.4.16
connected to : 172.16.4.16
tftp> put param config.txt

putting param to 172.16.4.16 : config.txt [octet]

Sent 8192 bytes in 3 seconds
tftp>
```

---

## 6.3 Upgrading the software

1. At the tftp prompt, type connect xxx.xxx.xxx.xx.

```
tftp> connect 172.16.4.12
connected to : 172.16.4.12
```

A message, "connected to : xxx.xxx.xxx.xxx," pops up if successful.

2. Type the transfer mode (binary or ascii).

```
tftp> binary
mode set to octet
```

A mode set to octet/netascii pops up.

3. Type get app when the file name is app, or type get app \*\*\* to specify the name. If the software file name is app, you can also skip the file name by simply typing get app.

---

4. The tftp prompt pops up when the upgrade is successful.

5. Below is an example of the software upgrade procedures.

```
tftp> connect 172.16.4.16
connected to : 172.16.4.16
tftp> binary
mode set to octet
tftp> get app
tftp>

Sent 983040 bytes in 3 seconds
tftp>
```

---

## 6.4 Downloading the Configurations

1. At the tftp prompt, type connect xxx.xxx.xxx.xx.

```
tftp> connect 172.16.4.16
connected to : 172.16.4.16
```

A message, "connected to : xxx.xxx.xxx.xxx," pops up if successful.

2. Type the transfer mode (binary or ascii).

```
tftp> binary
mode set to octet
```

A message, "mode set to octet/netascii," pops up.

3. Type get para. The configuration file is saved as param at the target location. If the configuration file name is param, you can also skip the file name by simply typing get param.
4. The tftp prompt pops up when the download is successful.

```
tftp> get param
tftp> █
```

---

## Chapter 7 Wireless LAN

This chapter is only relevant for devices that have wireless LAN functionality. The parameters listed below are available from the [root @ home]\$ directory.

The prefix for each command is: **wlan -o -option [value]**

For example: **wlan -o -radio off**

radio	[on   off]	Sets the wireless broadcast to on or off
ssid	[ string ]	The SSID should match with client adapters. The SSID (Service Set ID) allows you to uniquely identify your Access Point in the radio environment. This can be useful in case multiple WLAN networks are present nearby your location.
channel	[1 ~ 14]	This value should match with client adapters. The Direct Sequence Spread Spectrum (DSSS) channel number is an identifier for the frequency on which your WLAN connectivity is enabled in the WLAN network. Although the configurable DSSS channel number range is from 1 up to 13, restrictions apply depending on the country



		where the Wireless ADSL-Router is used: FCC: channels 1 to 11 ETSI: channels 1 to 13.
beacon	[ integer ]	Specify the Beacon Interval value. Enter a value between 1 and 1000. The value represents the time in nano-seconds that Beacon packets are sent by an Access Point to synchronize a wireless network.
rts	[0 ~ 3000]	This value should normally remain at its default setting of 2,432. Should you encounter inconsistent data flow, only minor modifications are recommended. The value must match with remote clients.
frag	[256 ~ 2346]	This field is used to specify the fragmentation threshold. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2,346. Setting the Fragmentation Threshold too low may result in poor performance. The default value is 2346, this value must match client adapters.
dtim	[1 ~ 65535]	Enter a value between 1 and 65535, Default = 3. This number represents the time

		between sending delivery traffic identification messages (DTIMs) used for power saving and multicast/broadcast delivery. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages.
rate	[1,2,5,11 ]	The transfer rate of the router should be equal to or greater than the clients.
preamble	[long   short]	<b>long, short</b> . Should match client adapters. Short enables faster throughput, but it can only be used when all network elements comply with the IEEE 802.11b standard.
auth	[open   share]	<b>Open System</b> [no security], <b>Shared Key</b> [select this option if you wish to enable WEP security].
weptype	[0 64 128]	This parameter must match with the remote-clients. "0": disables the wep security "64": enables 64 bits wep security

---

		"128": enables 128 bits wep security
dkey	[0 ~ 3]	Select a Key from 0~3. This key will be the active hexadecimal password for access.
k0/k1/k2/k3	[Hex String]	enter a hexadecimal password for each key. This hexadecimal password will be required to be set on any wireless client that you wish to connect with your access point.
hidessid	[on   off]	This parameter determines whether the SSID will be displayed or not. Select <b>On</b> to display the ID.
macfilter		[add   del] [xx:xx:xx:xx:xx:xx] [open   share]