NetComm®
www.netcomm.com.au

IP DSLAM

User Guide

Table of Contents

Chapter 1 Preface

This preface describes the "*NCT192 IP-DSLAM System Configuration Guide"* about how it is organized, and its document conventions. It contains the following topics:

- Purpose
- Organization
- Conventions

Purpose

The purpose of this guide is to provide detailed information and description of NCT192 IP-DSLAM, which includes software configuration and other specific features. This document is intended to help system operator to operate the software and understand the NCT192 IP-DSLAM system configurations as quickly as possible.

Organization

This guide contains the following chapters:

- Preface
- NCT192 User Interface
- Initialing the NE
- Managing the System Profiles
- Managing the Subscriber Interface
- Managing the Network Interface
- Managing the Connection Services
- Managing the System Functions
- Diagnosis and Performance Monitoring
- Appendix

Conventions

This section describes the conventions used in this guide.

The NCT192 IP-DSLAM is the Next-Generation xDSL Broadband Access Network comprises a Gigabit Ethernet and a number of ATU-Rs, STU-Rs, and POTS splitter to construct a broadband access network between central office and customer premises. The NCT192 IP-DSLAM uses statistically multiplexing and ATM over xDSL technologies to provide the broadband data communication services, such as high speed Internet access and multimedia services, across existing twisted pair telephone line.

NCT192 IP-DSLAM (Digital Subscriber Line Access Multiplexer) represents NCT192.

All statement in this document applies to the NCT192 IP-DSLAM. However it is noted that the valid range of port and slot are different for each model. The following table lists the valid range of slot and port.

Model Name	Valid range of Network Card	Valid range of Line Card	Range of ADSL/SHDSL port
NCT192	1	1~4	1~48

NE/NEs hereinafter referred as NCT192 medium capacity IP-DSLAM, unless specifically indicated.

ADSL mention in this document covers ADSL, ADSL2, and ADSL2+, unless specifically indicated.

xDSL hereinafter referred as ADSL, unless specifically indicated.

The **xDSL** specified in this document compliance with ITU-T Rec. G.992.1, G.992.2, G.992.3 and G.992.5 for ADSL.

CLI Ex – The command line management with a local console or Telnet through in-band or out-of-band IP interface for CIT (Craft Interface Terminal) connection.

NCT192 LCT – NCT192 Local Craft Terminal (LCT), a stand-along host with SNMP base EMS (Element Management System) provides GUI operation under single section through in-band or out-of-band IP management interface.

This sign indicates the **NOTICE**. A note contains helpful suggestions or reference relay on the topical subjects.

This sign indicates the **TIP**. Performing the information described in the paragraph will help you solve a problem. The tip information might not be troubleshooting or even an action, but could be useful information.

This sign indicates the **CAUTION**. In this situation, you might do something that could result in equipment damage or loss of data.

This sign indicates the DANGER. You are in situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Chapter 2 NCT192 User Interface

This chapter describes the NCT192 user interface, the instructions describe how to using the command-line interface, and also describes the command editing and command history features that enable you to recall previous command entries and edit previously entered commands.

- User Interface Mode
- Access via the Console Port
- Access using the Telnet Session
- Managing the Session Login Account
- Command Syntax and Operating Regulation

User Interface Mode

The NCT192 provides the CLI Ex mode to access the device in either one of the following ways:

- Remote Telnet via in-band port
- Remote Telnet via out-band port
- Local RS232 Console

Access via the Console Port

The NCT192 provides RS232 port for the operator to perform configuration operations via a directly connected VT-100 compatible terminal.

Follow the following procedure to enter the CLI Ex mode via a direct VT100-compatible terminal, for example, the hyper terminal in Microsoft Windows environment.

Step 1 Set the communication parameters of a VT100-compatible terminal shown in Table 2-1.

Table 2-1 NCT192 Console Management Setting

Parameter	Setting
Baud rate	9600
Data bits	8
Parity	None
Start bits	1
Stop bits	1
Flow control	None

Step 2 Connect the VT100-compatible terminal to the Console Port on the NCT192 front panel.

Step 3 Press **<Enter>** a number of times until the "**Login:**" is displayed on the screen.

Step 4 Enter the username and password. The default administration username and password are listed below (case sensitive):

```
Login: admin
Password: admin
```

See the Section “Managing the Session Login Account” of Chapter 2 for detail information.

Access using the Telnet Session

Enter the CLI Ex mode by establishing a Telnet session between the local host and NCT192 though either the in-band (UGE) or out-band (M-ETH) port.

Follow the following procedure to enter the CLI Ex mode:

Step 1 Open the MS-DOS prompt window in Microsoft Windows environment.

Step 2 Type the “telnet xx.xx.xx.xx (IP address)” in the MS-DOS prompt window to establish a telnet connection to the target NCT192.

Step 3 Enter the username and password. The default administration username and password are listed below (case sensitive):

```
User Name: admin
Password: admin
```

If the IP address of NCT192 is changed during configuration, the Telnet session will be broken. The operator needs to build a new Telnet session to continue the configuration process.

If the assigned IP has been changed and forgotten, locally access NCT192 via Console port with the command shown in Example 1 to retrieve the IP address assigned to the system.

The IP address assigned must be unique in use with the device on the network segment. Refer to the Section “Configuring the Management Interface” of Chapter 3 for more information.

Example 1 Display the system management IP addresses

```
CLI# config ip show
    UGE
        IP address      : 172.17.192.1
        subnet mask     : 255.255.0.0
        MAC address     : 00:60:64:dc:7a:17
        UGE VLAN ID     : 4092

    NME
        IP address      : 192.168.192.1
        subnet mask     : 255.255.255.0
        MAC address     : 00:60:64:dc:7a:16

    Gateway
        IP address      : 172.17.192.254
```

The single NE supports up to 12 concurrent telnet sessions. Only one concurrent telnet session is allowed to enter by admin account user at a time (Console access included),the default “**admin**” account user is with administrator privilege level, see the Section “Managing the Session Login Account” of Chapter 2 for detail information.

Session Logout

The following command is to terminate the Telnet session or quit the console session from CLI Ex mode.

To logout the sessions using the "**logout**" command at the prompt for CLI#.

Table 2-2 Session Logout Command

The following command is to logout the session (Telnet or Console).
CLI# logout

If you are using Telnet access for the CLI Ex mode, the command "**logout**" will terminate the current Telnet session, and the CLI Ex will return to the login prompt if using Console access.

Telnet Timeout

The following command is to set the Telnet session time-out timer from CLI Ex mode.
Telnet session will terminate when the telnet time-out times ends, and the CLI Ex will return to the login prompt if using Console access.

Table 2-3 Telnet Session Timeout Command

Use this command to set the telnet time-out of the system.	
CLI(config mgt)# telnet-timeout set <*min*>	
Use this command to view the telnet time-out of the system.	
CLI(config mgt)# telnet-timeout show	
Parameters	**Task**
<*min*>	This specifies the telnet time out of the system **Type:** Mandatory **Valid values:** 1~1440 minutes. **Default values:** 2 minutes

Example 2 Display the telnet time-out of the system

```
CLI(config mgt)# telnet-timeout set 5
OK

CLI(config mgt)# telnet-timeout show

Telnet time-out       : 5 min (5 min)
```

Managing the Session Login Account

For security reason, the CLI Ex mode provides two groups of user account privileges, "**admin**" group and "**guest**" group. Admin group has read/write access privileges while guest group has only the read privileges.

Table 2-4 shows the system default login account and session information.

Table 2-4 NCT192 Default Login Account Index

Group	Default Account	Login Mode	Session	Session Timeout

Admin	Username: admin Password: admin	Console, Telnet	Single session occupying on either Console access or Telnet access.	Console: limitless Telnet: 120 Seconds
Guest	Username: guest Password: guest	Console, Telnet	1 session for Console access, up to 12 sessions for Telnet access.	Console: limitless Telnet: 120 Seconds

The user account management performs how to create, delete and change the user password. Enter to the "**config mgt user**" sub-group directory. Table 2-5 shows the commands to perform user account management. Example 3 presents how to generate a new account user and join to the admin group; Example 4 and Example 5 show how to change the user password and delete a user account respectively.

```
CLI# config mgt user
CLI(config mgt user)#
```

Table 2-5 User Account Management

The following command is to create the account user and its group privileges of console or telnet, while valid user name was defined, the password prompt will appear.
CLI(config mgt user)# add <*name*> **[**<*user-group*>**]**
The following command is to delete a user login of console or telnet.
CLI(config mgt user)# del <*name*>
The following command is to change the user password.
CLI(config mgt user)# set password <*name*>
The following command is to change the user group privileges.
CLI(config mgt user)# set group <*name*> **[**<*user-group* >**]**
The following command is to display information of all the users. Password information is not included.
CLI(config mgt user)# show

Parameters	Task
<*name*>	This specifies the user name and password to be created. **Type:** Mandatory **Valid values:** String of up to 16 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_', '.', '@')
<*user-group* >	This specifies group privilege of the name user. **Type:** Option **Default value:** guest **Valid values:** admin, guest

Example 3 Create a new user account

```
CLI(config mgt user)# add abc
Enter password (up to 16 characters):
Confirm password:

OK

CLI(config mgt user)# set group abc admin
OK

CLI(config mgt user)# show

management VLAN    : 4092
           user    : guest (guest)
```

```
            user    : admin (admin)
            user    : abc (admin)
```

Example 4 Change the user password

```
CLI(config mgt user)# password abc

Enter new password:
Confirm new password:

OK
```

Example 5 Delete a user account

```
CLI(config mgt user)# del abc

OK

CLI(config mgt user)# show

    management VLAN    : 100
               user    : guest (guest)
               user    : admin (admin)
```

Command Syntax and Operating Regulation

This section describes the syntax notation, structure, context-sensitive, command history features, and command syntax help.

Syntax Notation Conventions

CLI Ex command syntax using different bracket form to display syntax notation, Table below lists the notation information.

Table 2-6 Syntax Notation of CLI Ex

Notation	Descriptions
Keyword	Keywords in a command that you must enter exactly as shown.
<*Parameter*>	Parameter values must be specified.
[<*Parameter*>]	Parameter values are optional.
[*Parameter 1* | *Parameter 2* | .. | *Parameter n*]	Parameter values are enclosed in "[.. | ..] " when you optional use one of the values specified.
{*Parameter 1* | *Parameter 2* | .. | *Parameter n*}	Parameter values are enclosed in "{ .. | .. }" when you must use one of the values specified.

Structure of a CLI Command

The CLI Ex commands conform to the following structure in group base. Each group contains sub-group directory or action command that can be used directly with proper syntax.

```
CLI# {[<Group-A> | <Action-A>] | [<Group-B> | <Action-B>] | [<Group-C> | <Action-C>] | <Action-D>}
```

or

```
CLI# [<Group-A> | <Action-A>]
```

```
CLI(Group-A)# [<Group-B> | <Action-B>]
CLI(Group-B)# [<Group-C> | <Action-C>]
CLI(Group-C)# <Action-D>
```

The command structure can complete in a single sentence or access into specific group directories.

Table 2-7 Structure of CLI Ex Mode

Keyword	Descriptions
<Group-#>	This is the group directory of a CLI Ex command which contains relative keywords. It indicates the type of group to be performed. "**config**" is an example of the group directory.
<Action-#>	This is the keyword of a CLI Ex command. It indicates the type of operation to be performed. "**ping**" is an example of this action keyword.
Command	**Descriptions**
exit	Jump to the upper group directory.
exit all	Jump to the root directory **CLI#**
clear	Clear the screen.
Press **Enter / Return**	Execute the command.

Command Syntax and Context Sensitive Help

Fully utilize the " **?** " command to assist your task; this command can be used to browse command and to be assisted on the command keywords or arguments.

To get help specific to a command, a keyword, or argument, perform**s** one of these tasks:

Table 2-8 CLI Ex Syntax Help

Command	Task
?	To list all commands available of CLI Ex mode.
Command ***?***	To list the associated keywords and arguments for a command.
Abbreviated-command-entry <Tab>	Complete a partial command or group directory name.

To list the command keywords, enter a question mark " **?** " to complete the command keywords and arguments. Include a space before the **?**. This form of help is called command syntax help.

The CLI Ex mode provides an error announce that appears in which you have entered an incorrect or incomplete command, syntax, keyword, or argument.

If you have entered the correct command but invalid syntax or a wrong keyword parameters, the CLI Ex will automatically prompt the error messages and reprint the commands with cursor indexed on wrong syntax.

Command History and Editing Features

By default, the system records ten command lines in its history buffer. To recall commands from the history buffer, perform one of these commands:

Table 2-9 Command History and Editing

Command	Task
Press the Up arrow key	To recall commands in the history buffer. Beginning with the most recent commands. Repeat the key sequence to recall the older commands.
Press the Down arrow key	To return to more recent commands in the history buffer. Repeat the key sequence to recall the more recent commands.
Press the left arrow key	To move the cursor back one character.
Press the right arrow key	To move the cursor forward one character.
Press **Backspace**	To erase the character to the left of the cursor.

This CLI Ex mode includes an editing feature. You can move cursor around on the command line to insert or delete the character.

The arrow keys function only on ANSI-compatible terminals such as VT100s.

Ending a Session

If you access using the Telnet session, you can type "**logout**" command to terminate the Telnet session instantly.

Console port will stay in life until you close the terminal session.

This page is leave in blank for note or memo use

Chapter 3 Initialing the NE

This chapter describes how to configure the NCT192 IP-DSLAMs initially, and contains the following sections:

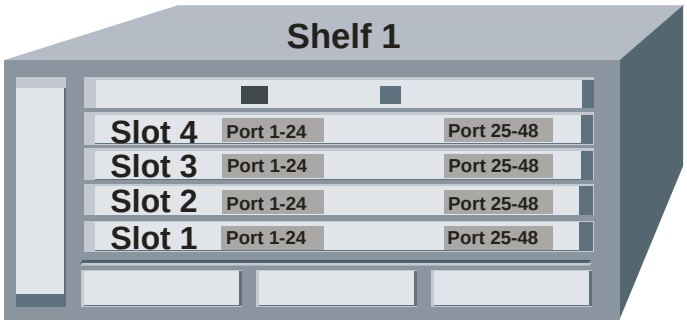
- Port Interface Indication
- Constructing the NE Objects
- Configuring the SNMP Manager
- Configuring the Management Interface
- Maintaining the GE Network Interface
- Maintaining the NE
- Configuring the System Date and Time
- Configuring the Internet Time Server
- Configuring the DNS Server
- Ambient Temperature

Port Interface Indication

The NCT192 IP-DSLAM slot structure is descibed as follows:

- NCT192: single shelf and five slots, 1 for NC (Network Card) and 4 for xDSL LC (Line Card), each xDSL LC contains 48 ADSL ports or 48 SHDSL ports. Figure 3-1 shows the shelf, slot, and port addressing outward on NCT192.

Figure 3-1 NCT192 Port Addressing Diagram



The CLI described in all chapters applies to the NCT192 IP-DSLAM. The following table lists the valid range of slot and port.

Model Name	Valid range of Network Card	Valid range of Line Card	Range of ADSL/SHDSL port
NCT192	NC1	1~4	1~48

Table 3-1 shows the commands to perform the port interface indication format.

Table 3-1 Port Interface Indication Format

Parameters	Descriptions
<*slot-id*>	**Format:** slot_# **Valid values:** slot_# (1 ~ 4) **Default value:** slot _# (1)
<*port-id*>	**Format:** [slot_#] . port_# **Valid values:** slot_# (1 ~ 4), port_# (1 ~ 48) **Default value:** slot_# (1)
<*slot-range*>	**Format (Continuously):** slot_# - slot_# **Format (Individually):** slot_# **Valid values:** slot_# (1 ~ 4) **Default value:** slot _# (1)
<*port-range*>	**Format (Continuously):** [slot_#] . port_# - port_# **Format (Individually):** [slot_#] . port_# **Valid values:** slot_# (1 ~ 4), port_# (1 ~ 48) **Default value:** slot_# (1)

Through the document, the notations <*slot-id*>, <*port-id*>, <*slot-range*>, and <*port-range*> are used to identify the particular slot/port interface or range of slot/port inside the CLI Ex mode. The <*slot-range*> and <*port-range*> parameters use "-" notation to identify the continuously range.

The form of "**slot_#**" is for the slot-based CLI command. Example 6 shows the usage of "**slot_#**" to indicate a specific slot in a slot-based CLI command.

Example 6 The usage of "slot_#**" to indicate a specific slot in a slot-based CLI command.**

```
CLI# status
CLI(status)# lc show 4

LC4
    current card type                       : ADSL
    planned card type                       : SHDSL
    hardware version                        : NCT1901-V3
    software version                        : 6.5.7_2.4.0
    serial number                           : NCT1901-8169S009034
    oper status                             : up
    system up time                          : 4day / 19hr / 48min / 26sec
    RFC2684 encapsulation                   : LLC
    tagged mode (configured)                : tagged-only
    tagged mode (run-time)                  : untagged-only
    VLAN tag pass through (configured)      : enabled
    VLAN tag pass through (run-time)        : disabled


CLI# status
CLI(status)# lc show 3-4

LC3
    current card type                       : ADSL
    planned card type                       : ADSL
    hardware version                        : NCT1901-V3
    software version                        : 6.5.7_2.4.0
    serial number                           : NCT1901-8169S009033
    oper status                             : up
    system up time                          : 4day / 20hr / 6min / 32sec
    RFC2684 encapsulation                   : LLC
    tagged mode (configured)                : untagged-only
```

```
    tagged mode (run-time)                    : untagged-only
    VLAN tag pass through (configured)        : disabled
    VLAN tag pass through (run-time)          : disabled

LC4
    current card type                         : ADSL
    planned card type                         : SHDSL
    hardware version                          : NCT1901-V3
    software version                          : 6.5.7_2.4.0
    serial number                             : NCT1901-8169S009034
    oper status                               : up
    system up time                            : 4day / 20hr / 6min / 55sec
    RFC2684 encapsulation                     : LLC
    tagged mode (configured)                  : tagged-only
    tagged mode (run-time)                    : untagged-only
    VLAN tag pass through (configured)        : enabled
    VLAN tag pass through (run-time)          : disabled
```

The form of "**slot_#. port_#**" is for the port-based CLI command. If **slot_#** is not specified, CLI_Ex will apply the default value (slot 1) automatically to the syntax. Example 7shows the usage of "**slot_#. port_#**" to indicate a specific port in a port-based CLI command. It is noted that Example 7 also depicts the CLI commands with different forms of port index which indicates the same port (slot 1, port 6).

Example 7 CLI commands to show the physical status of (slot 1 . port6)

```
CLI# status port show 6
Port: 1.6
    admin status        : enabled
    oper status         : up
    power state         : L0
    line standard           : G.992.5 Annex A

    [physical status]
              item          US      DS
        ----------------  ------  ------
         attainable rate    1343   30644  kbps
             attenuation     0.0     0.0  dB
              SNR margin     6.5     8.5  dB
            output power    12.1    12.6  dBm

    [channel status]
              item          US      DS
        ----------------  ------  ------
                 Tx rate    1342   29204  kbps
        interleave delay       0       0  ms
        CRC block length      39     255  ms
         INP symbol time    0.00    0.00  DMT symbol

CLI# status port show 1.6
Port: 1.6
    admin status        : enabled
    oper status         : up
    power state         : L0
    line standard           : G.992.5 Annex A

    [physical status]
              item          US      DS
        ----------------  ------  ------
         attainable rate    1343   30649  kbps
             attenuation     0.0     0.0  dB
              SNR margin     6.6     8.5  dB
            output power    12.1    12.6  dBm

    [channel status]
              item          US      DS
```

```
        -----------------  ------  ------
                 Tx rate    1342   29204  kbps
        interleave delay       0       0  ms
        CRC block length      39     255  ms
         INP symbol time    0.00    0.00  DMT symbol

CLI(status)# port show 1.6-25

Port: 1.6
    admin status        : enabled
    oper status         : up
    power state         : L0
    line standard           : G.992.5 Annex A

    [physical status]
              item          US      DS
        -----------------  ------  ------
         attainable rate    1343   30644  kbps
             attenuation     0.0     0.0  dB
              SNR margin     6.5     8.5  dB
            output power    12.1    12.6  dBm

    [channel status]
              item          US      DS
        -----------------  ------  ------
                 Tx rate    1342   29204  kbps
        interleave delay       0       0  ms
        CRC block length      39     255  ms
         INP symbol time    0.00    0.00  DMT symbol

Port: 1.21
    admin status        : enabled

    oper status         : down

Port: 1.23
    admin status        : enabled
    oper status         : up
    power state         : L0
    line standard           : G.992.5 Annex A

    [physical status]
              item          US      DS
        -----------------  ------  ------
         attainable rate    1343   30649  kbps
             attenuation     0.0     0.0  dB
              SNR margin     6.4     8.5  dB
            output power    12.1    12.6  dBm

    [channel status]
              item          US      DS
        -----------------  ------  ------
                 Tx rate    1351   29204  kbps
        interleave delay       0       0  ms
        CRC block length      39     255  ms
         INP symbol time    0.00    0.00  DMT symbol
```

Constructing the NE Objects

The NCT192 IP-DSLAM provides the flexibility to be equipped with various card modules such as ADSL-LC and SHDSL-LC. Constructing the NE board type of card module is the first task you need to perform.

Once the equipped card modules to the NCT192 IP-DSLAM are determined, you need to set the

planned type according to their correspondent slot to secure the system operation. For any reason (removed or type error); if the planned type is not the same as the online type detected from the system, the board mismatch alarm message will be reported.

Planning the System Card Type

Enter to the "**config nc**" sub-group directory to plan the NC (Network Control) card.

```
CLI# config nc
CLI(config nc)#
```

Enter to the "**config lc**" sub-group directory to plan the LC (Line Card) card.

```
CLI# config lc
CLI(config lc)#
```

Table 3-2 shows the CLI commands to configure the planned-type of LC/NC in the NE. Example 8~ Example 9 shows the usage of these commands as well as their related parameters.

Table 3-2 Planning the system card type

The following command is to modify the planning NC card type.	
CLI(config nc)# set planned-type <*nc-id*> {*none* | *cpu*}	
The following command is to modify the planning LC card type.	
CLI(config lc)# set planned-type < *lc-range*> <card-*type*>	
Parameters	**Task**
<*nc-id*>	Identify the slot range of the NC card **Type:** Mandatory **Valid values:** 1 ~ 2 (value = 2 does not apply to NCT192)
{*none* | *cpu*}	Identify the NC type.
<*lc-range*>	Identify the slot range of the Line card. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<card-*type*>	Identify the line card type **Valid values:** none, adsl, shdsl

Example 8 CLI commands to modify the planning NC card type

```
CLI# config nc
CLI(config nc)# set planned-type 1 cpu
OK

CLI(config nc)# show

NC:
    planned-type  current-type   tagged-mode
    ------------  ------------  -------------
             CPU           CPU  untagged-only

UGE:
    UGE  oper-status  admin-status  auto negotiation  use-mode
    ---  -----------  ------------  -----------------  --------
      1         down       enabled            enabled    uplink
      2         down      disabled            enabled    uplink

Subtend VLAN ID:
    n/a
```

Example 9 CLI commands shows how to modify the planning LC card type

```
CLI# config lc
CLI(config lc)# set planned-type 1.1 adsl

LC 1. 1: OK

CLI(config lc)# show

        planned  current  rfc2684  vlan-tag  service    configured
    LC   type     type     encap     pass      type     tagged-mode
    --  -------  -------  -------  --------  --------  -------------
     1     ADSL     ADSL      LLC  disabled  disabled  untagged-only
     2    SHDSL      n/p      LLC  disabled  disabled  untagged-only
     3    SHDSL     ADSL      LLC  disabled  disabled  untagged-only
     4    SHDSL      n/p      LLC   enabled  disabled    tagged-only

CLI(config lc)# set planned-type 3-4 adsl
LC 1. 3: OK
LC 1. 4: OK

CLI(config lc)# show

        planned  current  rfc2684  vlan-tag  service    configured
    LC   type     type     encap     pass      type     tagged-mode
    --  -------  -------  -------  --------  --------  -------------
     1     ADSL     ADSL      LLC  disabled  disabled  untagged-only
     2    SHDSL      n/p      LLC  disabled  disabled  untagged-only
     3     ADSL     ADSL      LLC  disabled  disabled  untagged-only
     4     ADSL      n/p      LLC   enabled  disabled    tagged-only
```

Verifying Current Software and Hardware Versions

Follow the commands to display the inventory information of NE software/ hardware version, card serial number, card type etc.

Use the “**nc show**” or “**lc show**” command under the “**status**” group directory to display the system H/W and S/W version of each plug-in card module and slot planning type.

Enter to the “**status**” group directory to verify the software and hardware versions.

```
CLI# status
CLI(status)#
```

Table 3-3 shows the commands to retrieve the NC board-level information. Example 10 shows the usage of these commands.

Table 3-3 Retrieve the software and hardware information of NC card

The following command is to display the version and plugging status of NC card.
CLI(status)# nc show

Example 10 Monitoring the NC board-level information

```
CLI(status)# nc show

NC
    current card type    : CPU Module
    planned card type    : CPU Module
    role                 : active
    hardware version     : NCT1902-V5
    software version     : 1.0v2.0.2@R134
    serial number        : NCT1902-8169S008952
```

```
    oper status          : up
    system up time       : 2day / 0hr / 23min / 14sec
    tagged mode          : untagged-only
```

Table 3-4 shows the commands to retrieve the LC board-level information. 0 shows the usage of these commands.

Table 3-4 Software and Firmware Verify of LC on-board card

The following command is to display the LC card version and plugging status.	
CLI(status)# lc show [*<lc-range >*]	
Parameters	**Task**
<lc-range>	Identify the slot range of the Line card. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.

Example 11 Monitoring the LC board-level information

```
CLI(status)# lc show

LC1
    current card type                  : ADSL
    planned card type                  : SHDSL
    hardware version                   : NCT1901-V3
    software version                   : 6.5.7_2.4.0
    serial number                      : NCT1901-8169S009031
    oper status                        : up
    system up time                     : 0day / 16hr / 5min / 44sec
    RFC2684 encapsulation              : LLC
    tagged mode (configured)           : untagged-only
    tagged mode (run-time)             : untagged-only
    VLAN tag pass through (configured) : disabled
    VLAN tag pass through (run-time)   : disabled
```

It is noted that the NE will drop the tagged Ethernet frames of VLAN-ID not configured by the VC-to-VLAN setting (see Table 6-9) in the following case.
NC tagged mode = Tagged
LC tagged mode Run-Time Status = Tagged
LC VTP Run-Time Status = Enabled

The tagged mode (run-time) indicates the operational status of tagged mode.
Tagged-only: LC (or NC) only forwards the tagged Ethernet frame and drops the untagged Ethernet frame.
Untagged-only: LC (or NC) only forwards the untagged Ethernet frame and drops the tagged Ethernet frame.
It is noted that the value of configured Tagged mode and its Run-Time Status may be different. Please refer to Table 6-9 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.

Configuring the System Information

The system information contains system name, location, and person contact information as defined in RFC1213.

Enter to the "**config sys-info**" sub-group directory to configure the system information.

```
CLI# config sys-info
CLI(config sys-info)#
```

Table 3-5 shows the commands to perform the configuration of system information. Example 12

shows the usage of these commands as well as their related parameters.

Table 3-5 System Information Configuration

Use this command to modify the system location.
CLI(config sys-info)# set location <*string*>
Use this command to modify the system contact information.
CLI(config sys-info)# set contact <*string*>
Use this command to modify the system name.
CLI config (sys-info)# set name <*string*>
Use this command to monitor the system information.
CLI(config sys-info)# show

Parameters	Task
<*string*>	This specifies the textual identification of the information on the given field **Type:** Mandatory **Valid values:** String of up to 255 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').

Example 12 Modifying the name of system information

```
CLI(config sys-info)# set location Sydney
OK

CLI(config sys-info)# set contact NetCommLimited@02-94242000
OK

CLI(config sys-info)# set name NCT192_IP_DSLAM
OK

CLI(config sys-info)# show

    System Name           : NCT192_IP_DSLAM
    System Contact        : NetCommLimited@02-94242000
    System Description    : IP-DSLAM
    System Location       : Sydney
    Telnet time-out       : 2 min (2 min)
```

Configuring the SNMP Manager

SNMP (Simple Network Management Protocol) is an application-layer protocol designed to facilitate the exchange of management information between network devices. By using SNMP, network administrators can more easily manage network performance, find and solve network problems, and plan for network growth.

In NCT192 IP-DSLAM, we use SNMP to exchange management information between a NE and LCT (or NCT192 server). SNMP enables the administrators to manage the NE by the LCT (or NCT192 server). In the term of SNMP, the NE plays the role of SNMP agent and the LCT (or NCT192 server) serves as the SNMP server. This section describes how to configure the SNMP on the NE.

Beware of the SNMP community setting, this will affect the communication between the NCT192 LCT (or NCT192 server) and NE, you must re-login the NCT192 LCT if the SNMP community has been modified.

Configuring the SNMP Community

The SNMP community is a string representing the password to access the MIB of NE with the associated privilege. The NE supports two levels of privilege (Permission) as follows:

- Read / Write / Create – Allow the SNMP server to read and write all objects in the MIB, as well as the community strings.
- Read-only – Only allow the SNMP server to read all objects in the MIB except the community strings.

The community string definitions on your NCT192 LCT (or NCT192 Server) must match at least one of those community string definitions on the NE. Otherwise, the LCT (or NCT192 Server) is not allowed to access the NE.

The SNMP Community setting allows you to assign the community privilege levels. Two privilege levels are supported, read-only and read-write.

Enter to the "**config mgt snmp**" sub-group directory to configure the SNMP community.

```
CLI# config mgt snmp
CLI(config mgt snmp)#
```

Table 3-6 shows the commands to perform the setting of SNMP community. Example 13 shows the usage of these commands as well as their related parameters.

Table 3-6 SNMP Community Setting

The following command is to create new SNMP community information. It is noted that the system supports at most 8 community settings.
CLI(config mgt snmp)# add community <*community-name*> {*rw* | *ro*}
The following command is to delete the SNMP community information.
CLI(config mgt snmp)# del community <*community-name*>
The following command is to monitor the status of SNMP community sets (Community Table).
CLI(config mgt snmp)# show community <*option*>

Parameters	Task
< *community-name* >	This specifies the community name **Type:** Mandatory **Valid values:** String of up to 20 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*option*>	This specifies the community types **Type:** Mandatory **Valid values:** community | trapstation
{*rw* | *ro*}	This specifies the access permissions given by managers with this community name. 'ro' implies read only permission and 'rw' implies read-write permission. **Type:** Mandatory

Example 13 Add a new SNMP community to the system

```
CLI(config mgt snmp)# add community xxx ro
OK

CLI(config mgt snmp)# show

Community Table:
      Community       Permission
 --------------------- ----------
             "public"  read-only
             "netman" read-write
```

```
                "xxx"  read-only

Trap Station Table:
    No entry
```

Configuring the IP Address of SNMP Trap Station

SNMP Trap Manager records the hosts (any SNMP server, like LCT, NCT192 Server, and so on) to be notified whenever the NE encounters abnormalities. When a trap condition happens, the NE sends the corresponding SNMP trap message to the hosts (SNMP server).

Enter to the "**config mgt snmp**" sub-group directory to configure the Trap station.

```
CLI# config mgt snmp
CLI(config mgt snmp)#
```

Table 3-7 shows the commands to perform the setting of SNMP Trap Station. Example 14 shows the usage of these commands as well as their related parameters.

Table 3-7 SNMP Trap Station Setting

The following command is to create a new trap station, system allows of 8 trap stations in maximum.	
CLI(config mgt snmp)# add trapstation <*ip-addr*> <*community-name*>	
The following command is to delete the trap station information.	
CLI(config mgt snmp)# del trapstation <*ip-addr*>	
The following command is to monitor the status of trap stations (Trap Station Table).	
CLI(config mgt snmp)# show <*option*>	
Parameters	**Task**
<*ip-addr*>	This indicates the IP address (Server / Host IP) of SNMP Manager. **Type:** Mandatory
<*community-name*>	This specifies the SNMP trap community of NE (Send Trap). **Type:** Mandatory
<*option*>	This specifies the community types **Type:** Mandatory **Valid values:** community | trapstation

Example 14 Add a new Trap station

```
CLI(config mgt snmp)# add trapstation 192.168.1.1 public
OK

CLI(config mgt snmp)# show trapstation
Trap Station Table:
   IP Address         Community       Version
 ---------------- --------------------- --------
     192.168.1.1             "public"     v2c
```

Configuring the Management Interface

NCT192 provides 2 kinds of management interfaces on the NC (Network Control) card:

- Network management Ethernet interface (nme)
  The nme is an out-of-band management Ethernet port on the NC card. Packets received on this interface will never reach the switching fabric. Instead, packets are transported

between the CPU and the nme port directly.

- Uplink network interface (uge)
  The uge, an in-band management interface connects to the switching fabric, presents the uplink gigabit Ethernet port that has ability to join the VLAN membership. Packets received on this interface are transported to the CPU via switching fabric and vice versa.

This section depicts the CLI commands to configure the IP address of nme and uge ports.

Enter to the "**config ip**" sub-group directory to configure the management interface IP address.

```
CLI# config ip
CLI(config ip)#
```

Enter to the "**config mgt**" sub-group directory to configure the VLAN-ID associated with the uge in-band interface.

```
CLI# config mgt
CLI(config mgt)#
```

Table 3-8 shows the commands to perform the management interface setting of IP address. Example 15 and Example 16 shows the usage of these commands as well as their related parameters.

Table 3-8 Management Interface IP Address Setting

The following command is to assign the IP address and subnet mask for management Ethernet interface (nme).
CLI(config ip)# set nme <*ip-addr*> <*netmask*> <*gatewayip*>
The following command is to assign the IP address and subnet mask for uplink Network interface (uge).
CLI(config ip)# set uge <*ip-addr*> <*netmask*> <*gatewayip*>
The following command is to assign the default gateway. The NCT192 IP-DSLAM sends all off-network IP traffic to the default gateway.
CLI(config ip)# set gateway <*ip-addr*>
The following command is to monitor the management interface information.
CLI(config ip)# show
The following command is to identify the VLAN ID for in-band management traffic.
CLI(config mgt)# vlan-id set <*vid*>
The following command is to view the VLAN ID for in-band management traffic.
CLI(config mgt)# vlan-id show

Parameters	Task
<*ip-addr*>	This specifies the network IP address for nme and uge interface, this IP address is only for system management. **Type:** Mandatory **Valid values:** Any valid class A/B/C address **Default value:** None
<*gatewayip*>	This specifies the gateway IP address for system, this gateway IP address is only for system management. **Type:** Mandatory **Valid values:** Any valid class A/B/C address
<*netmask*>	This specifies the subnet mask configured for the interface. **Type:** Mandatory **Valid values:** 255.0.0.0 ~ 255.255.255.255
<*vid*>	Assign the in-band interface to the proper VLAN (Making sure the VLAN will be associated with the network to which the IP address belongs). **Type:** Mandatory **Valid values:** 1 ~ 4094

Example 15 Assign the IP address and subnet mask for nme

```
CLI(config ip)# set nme 192.168.192.1 255.255.0.0 100.168.1.254
OK
```

Example 16 Assign the IP address and subnet mask for uge

```
CLI(config ip)# set uge 100.168.1.31 255.255.0.0 100.168.1.254
OK

CLI(config ip)# show

UGE
    IP address     : 100.168.1.31
    subnet mask    : 255.255.0.0
    MAC address    : 00:60:64:dc:7a:17
    UGE VLAN ID    : 4092

NME
    IP address     : 192.168.192.1
    subnet mask    : 255.255.0.0
    MAC address    : 00:60:64:dc:7a:16

Gateway
    IP address     : 100.168.1.254
```

Setting the Management Ethernet (NME) Interface IP Address

Before accessing telnet session to the NCT192 IP-DSLAM or SNMP, you must assign an IP address to either the in-band (uge) interface or the management Ethernet (nme) interface.

You can specify the subnet mask (netmask) in dotted decimal format.

To set the management Ethernet (nme) interface IP address, perform these procedures in CLI Ex mode:

Step 1 Assign an IP address and subnet mask to the management Ethernet (nme) interface.

Step 2 Verify the default gateway, if necessary.

Example 17 depicts the CLI commands with how to assign an IP address and subnet mask to the management Ethernet (nme) interface and how to verify the interface configuration.

Example 17 Setup the out-of-band management interface

```
CLI(config ip)# set nme 172.16.1.1 255.255.0.0 172.16.1.254
OK

CLI(config ip)# show
UGE
    IP address     : 100.168.3.97
    subnet mask    : 255.255.0.0
    MAC address    : 00:60:64:dc:7a:17
    UGE VLAN ID    : 4092

NME
    IP address     : 172.16.1.1
    subnet mask    : 255.255.0.0
    MAC address    : 00:60:64:dc:7a:16

Gateway
    IP address     : 172.16.1.254
```

Setting the in-band Interface (UGE) IP Address

Before accessing telnet session to the NCT192 IP-DSLAM or SNMP, you must assign an IP address to either the in-band (uge) interface or the management Ethernet (nme) interface.

You can specify the subnet mask (netmask) in dotted decimal format.

To set the IP address and VLAN membership of the in-band (uge) management interface, you can perform the following procedures in CLI Ex mode:

Step 1 Assign an IP address and subnet mask to the in-band (uge) management interface.

Step 2 Verify the default gateway, if necessary.

Step 3 Assign the in-band interface to the proper VLAN.

The Example 18 and Example 19 depict the CLI commands with how to assign an IP address, specify the subnet mask, and assign the VLAN for the in-band (uge) interface.

Example 18 Setup the in-band management interface

```
CLI(config ip)# set uge 192.168.100.1 255.255.255.0 192.168.100.254
OK

CLI(config ip)# show
UGE
    IP address     : 192.168.100.1
    subnet mask    : 255.255.255.0
    MAC address    : 00:60:64:dc:7a:17
    UGE VLAN ID    : 4092

NME
    IP address     : 192.168.192.1
    subnet mask    : 255.255.248.0
    MAC address    : 00:60:64:dc:7a:16

Gateway
    IP address     : 192.168.100.254

CLI(config ip)# exit
```

Example 19 Assign the in-band interface to the proper VLAN

```
CLI# config mgt
CLI(mgt)# set vlan 10
OK

CLI(mgt)# show

    management VLAN    : 10
               user    : guest (guest)
               user    : admin (admin)
               user    : abc (admin)
```

Configuring the Default Gateway

A gateway is a node that serves as an entrance to another network, and vice-versa. Gateways are most commonly used to transfer data between private networks and the Internet.

The NCT192 IP-DSLAM sends IP packets destined for other IP subnets to the default gateway (typically a router interface in the same network or subnet as the switch IP address). The NCT192 IP-DSLAM does not use the IP routing table to forward traffic from connected devices, IP traffic only generated by the NCT192 IP-DSLAM itself (for example: Telnet, TFTP, and ping).

The switch sends all off-network IP traffic to the primary default gateway. Both the in-band (uge) and management Ethernet (nme) interfaces are specified with common default gateway, the system forward traffic automatically determines through which interface of the default gateway can be reached.

Configuring the Secured Host

The security host mechanism protects the NCT192 IP-DSLAM against unauthorized access from untrustful host. This feature allows you to specify up to 10 sections of IPs of trusted hosts and authorized services (e.g. SNMP, TELNET, and FTP)

Enter to the "**config secure**" sub-group directory to configure the secured host IP address.

```
CLI# config secure
CLI(config secure)#
```

Enter the "**enable**" CLI command in sub-group directory to enable the secured host.

```
CLI(config secure)# enable

OK
```

Table 3-9 shows the commands to perform the configuration of secured host. Example 20 and Example 21 shows the usage of these commands as well as their related parameters.

Table 3-9 Secured Host Configuration

The following command is to specify the secured host with all permission services.
CLI(config secure)# allow <*index*> **all**
The following command is to specify the secured host without any permission service.
CLI(config secure)# allow <*index*> **none**
The following command is to specify the secured host in a specifics service.
CLI(config secure)# allow <*index*> <*snmp,telnet,ftp,tftp*>
The following command is to enable the secured host feature.
CLI(config secure)# enable
The following command is to disable the secured host feature.
CLI(config secure)# disable
The following command is to specify the secured host IP range.
CLI(config secure)# set <*index*> <*from-ip*> [<*to-ip*>]
The following command is to display the information of secured host.
CLI(config secure)# show [<*index*>]

Parameters	Task
<*index*>	This specifies the entry number of secured host list. **Valid values:** 1 ~ 10
<*snmp,telnet,ftp,tftp*>	This indicates the services (any combination of SNMP, TELNET, FTP and TFTP) the specified secured hosts are allowed. **Valid values:** snmp, telnet, ftp, tftp
<*from-ip*>	This indicates the beginning of the IP address range of the secured hosts. **Valid values:** 0.0.0.0 ~ 255.255.255.255
<*to-ip*>	This indicates the end of the IP address range of the secured hosts. **Valid values:** 0.0.0.0 ~ 255.255.255.255

Example 20 Set the secured host IP range

```
CLI(config secure)# set 2 192.168.192.1 192.168.192.255
OK

CLI(config secure)# show

Secured host configuration:
Admin Status: enabled
    index      from IP          to IP          allowed type
    -----  ---------------  ---------------  --------------------
        1          0.0.0.0  255.255.255.255   SNMP + telnet + FTP
        2    192.168.192.1  192.168.192.255                  none
        3          0.0.0.0          0.0.0.0                  none
        4          0.0.0.0          0.0.0.0                  none
        5          0.0.0.0          0.0.0.0                   all
        6          0.0.0.0          0.0.0.0                  none
        7          0.0.0.0          0.0.0.0                  none
        8          0.0.0.0          0.0.0.0                  none
        9          0.0.0.0          0.0.0.0                  none
       10          0.0.0.0          0.0.0.0                  none
```

Example 21 Allow the secured host with the permission services

```
CLI(config secure)# allow 2 all
OK

CLI(config secure)# show

Secured host configuration:
Admin Status: enabled
    index      from IP          to IP          allowed type
    -----  ---------------  ---------------  --------------------
        1          0.0.0.0  255.255.255.255   SNMP + telnet + FTP
        2    192.168.192.1  192.168.192.255                   all
        3          0.0.0.0          0.0.0.0                  none
        4          0.0.0.0          0.0.0.0                  none
        5          0.0.0.0          0.0.0.0                   all
        6          0.0.0.0          0.0.0.0                  none
        7          0.0.0.0          0.0.0.0                  none
        8          0.0.0.0          0.0.0.0                  none
        9          0.0.0.0          0.0.0.0                  none
       10          0.0.0.0          0.0.0.0                  none
```

Maintaining the GE Network Interface

Configuring the UGE Negotiation Mode

The NE supports auto-negotiable uge Ethernet port. Enter to the "**config nc**" sub-group directory to configure the UGE Negotiation Mode.

```
CLI# config nc
CLI(config nc)#
```

Table 3-10 shows the commands to perform the configuration of the UGE Negotiation Mode. Example 22 shows the usage of these commands as well as its related parameters.

Table 3-10 Configuring the UGE Negotiation Mode

The following command is to modify the UGE negotiation mode.	
CLI(config nc)# set autoneg <*uge-id*> {*off* | *on*}	
Parameters	**Task**
{*off* | *on*}	Identify the auto negotiation mode of specified UGE port. **Type:** Mandatory **Valid values:** off | on
<*uge-id*>	Identify the slot range of the UGE port **Type:** Mandatory **Valid values:** 1 ~ 2

Example 22 The modification of the UGE negotiation mode

```
CLI(config nc)# set autoneg 1 enabled
OK

CLI(config nc)# show

NC:
    planned-type  current-type   tagged-mode
    ------------  ------------  -------------
             CPU           CPU  untagged-only

UGE:
    UGE  oper-status  admin-status  auto negotiation  use-mode
    ---  -----------  ------------  -----------------  --------
      1         down       enabled            enabled    uplink
      2         down      disabled            enabled    uplink

Subtend VLAN ID:
    n/a
```

Checking the SFP module information

NCT192 IP-DSLAM supports 2 SFP (Small Form Pluggable) Mini-GBIC modules on the NC.

Enter to the "**status**" group directory to verify the SFP module information.

Use the "**gbic show**" command under the "**status**" group directory to display the SFP information.

```
CLI# status
CLI(status)#
```

Table 3-11 shows the commands to perform the check of the SFP module information. Example 23 shows the usage of these commands as well as its related parameters.

Table 3-11 Checking the SFP module information

Using this command to display the system plugged SFP mini GBIC module.	
CLI(status)# gbic show <*uge-id*>	
Parameters	**Task**
<*uge-id*>	This specifies the index of UGE. **Type:** Mandatory **Valid values:** 1 | 2

Example 23 Display the system plugged SFP mini GBIC module

```
CLI(status)# gbic show 2

identifier                      : SFP
connector                       : LC
SONET compliance codes          :
ethernet compliance codes       : 1000BASE-LX
fiber channel link length       : long distance (L)
fiber channel transmitter tech  : longwave laser (LC)
fiber channel transmitter media : single mode (SM)
fiber channel speed             : 100 MBytes/Sec
encoding                        : 8B10B
BR,nominal    - 100Mbps         : 13
length(9um)   - km              : 10
length(9um)   - 100m            : 100
length(50um)  - 10m             : 55
length(62.5um)- 10m             : 55
length(Copper)- 1m              : 0
vendor name                     :
vendor OUI                      : 00:00:00
vendor PN                       : SFP-LX
vendor SN                       : 3119980079
laser wave length               : 1310 nm
```

Maintaining the NE

The NE supports the storing, backup/restore configuration and firmware upgrade functions as described in the following sub-sections.

- Storing the Active System Configuration
- Backup and Restore the Active System Configuration
- File System Management
- Managing the Boot Section
- NE Firmware Upgrade
- NE Firmware Upgrade in Cascade mode
- SHDSL Firmware Upgrade

Storing the Active System Configuration

The modified configuration will be lost due to the rebooting of hardware without saving (storing). Use "**save**" command under "**config file**" sub-group directory to save your active configuration in system flash, NCT192 IP-DSLAM will load the saved configurations and execute them whenever the system reboots.

Enter to the "**config file**" sub-group directory to operate.

```
CLI# config file
CLI(config file)#
```

Table 3-12 Store the Active System Configuration

The following command is to save current configuration and backup old configuration.
CLI(config file)# save
The following command is to remove all saved configuration files.
CLI(config file)# erase
The following command is to show configuration information.
CLI(config file)# ls

Saving system configurations takes about 15 seconds to finish.

Example 24 Save the system configuration

```
CLI(config file)# save
OK

CLI(config file)# ls

Listing directory [cfg:]
                    Nov 19 2007 18:14          37   mac.cfg
                    Oct 10 2000 12:58      146150   default.cfg
                    Nov 30 2007 20:43          32   default.md5
                    Oct 11 2000 13:38      146993   config.cfg
                    Oct 11 2000 13:38          32   config.md5
```

Backup and Restore the Active System Configuration

NE provides the backup and restore related CLI commands to backup or restore the NE configuration via FTP. The backup procedures are as following:

Step 1 Open the DOS prompt window (or environment) on personal computer (PC).

Step 2 Go to the directory where the backup file is saved and then login the NCT192 by FTP

Step 3 Get the configuration file from NE to the target partition via FTP by following commands:

ftp> **cd cfg:**
ftp> **get default.cfg**
or
ftp> **put default.cfg**

It is noted that login device via FTP must be used the read-write authorization. The default username/password is **admin/admin**.

It is noted that the NE configuration is saved in “default.cfg” on the NE. The operator can backup the “default.cfg” and save it with a different filename on the local host. However, the operator has to restore (by the ftp “put” command) the NE configuration with filename of “default.cfg”.

Example 25 and Example 26 show the process to backup the configurations and restore the configurations, respectively..

Example 25 Backup the configurations from the NE via FTP.

```
1.
2. D:\>ftp 192.168.192.1
3. Connected to 192.168.192.1.
4. 220-=========================================================================-
5. 220-                Welcome to the IP-DSLAM FTP Server                       -
6. 220-                                                                         -
7. 220- CAUTION: It´s your responsibility to use the FTP service correctly -
8. 220-          , please put the right files into the right file system.  -
9. 220 =========================================================================-
10.   User (192.168.192.1:(none)): admin
11.   331 Password required
12.   Password:
13.   230 User logged in
14.   ftp> cd cfg:
15.   250 Changed directory to "cfg:/"
16.   ftp> get default.cfg D:\DSLAM-TPE-4.txt
17.   200 Port set okay
18.   150 Opening BINARY mode data connection
19.   226 Transfer complete
20.   ftp: 152231 bytes received in 0.45Seconds 335.31Kbytes/sec.
21.   ftp> bye
22.   221 Bye...see you later
23.
24.   D:\>
```

Example 26 Restore the configurations to the NE via FTP.

```
25.
26.   D:\>ftp 192.168.192.1
27.   Connected to 192.168.192.1.
28.   220-=========================================================================-
29.   220-                Welcome to the IP-DSLAM FTP Server                       -
30.   220-                                                                         -
31.   220- CAUTION: It´s your responsibility to use the FTP service correctly -
32.   220-          , please put the right files into the right file system.  -
33.   220 =========================================================================-
34.   User (192.168.192.1:(none)): admin
35.   331 Password required
36.   Password:
37.   230 User logged in
38.   ftp> cd cfg:
39.   250 Changed directory to "cfg:/"
40.   ftp> put DSLAM-TPE-4.cfg default.cfg
41.   200 Port set okay
42.   150 Opening BINARY mode data connection
43.   226- CAUTION:Please wait for 120 seconds -
44.   226 Transfer complete
45.   ftp: 152231 bytes sent in 0.80Seconds 191.01Kbytes/sec.
46.   ftp> bye
47.   221 Bye...see you later
```

File System Management

This section depicts the CLI commands for the maintenance of file system in the on-board flash.

Enter the “**filesystem**” in sub-group directory to operate.

```
CLI# filesystem
CLI(filesystem)#
```

Table 3-13 File System Configuration

The following command is to delete a file.
CLI(filesystem)# del {*opCodeA* | *opCodeB* | *cfg*} *<filename>*
The following command is to list files inside file system partition.
CLI(filesystem)# ls [*opCodeA* | *opCodeB* | *cfg*]

Parameters	Task
{*opCodeA* | *opCodeB* | *cfg*}	This specifies the partition of NC on-board flash. *opCodeA/opCodeB*: the partition to store the NE firmware and LC firmware. *cfg*: the partition to store the configuration file.
<filename>	This specifies the file name of file to be stored in the partition of NC on-board flash. **Type:** Mandatory **Valid values:** nct192.enc nct1901fw.enc nct1901br.enc config.cfg config.md5

Example 27 Configuration of file system in NE

```
CLI# filesystem ls
Listing directory [opCodeA:]
                     Dec 18 2007 10:23      2679217   nct192.enc
                     Dec 18 2007 15:55       457808   nct1901fw.enc
                     Dec 18 2007 15:55        32892   nct1901br.enc

Listing directory [opCodeB:]
                     Dec 15 2007 10:21      2679217   nct192.enc
                     Dec 15 2007 13:25       457808   nct1901fw.enc
                     Dec 15 2007 13:25        32892   nct1901br.enc


Listing directory [cfg:]
                     Nov 19 2007 18:14           37   mac.cfg
                     Nov 30 2007 20:43       146150   default.cfg
                     Nov 30 2007 20:43           32   default.md5
                     Oct 15 2000 09:30       146689   config.cfg
                     Oct 15 2000 09:30           32   config.md5

CLI# filesystem del cfg default.cfg
ERROR: Can´t delete default configuration file.
```

It is noted that the follwing files can not be deleted via CLI/LCT.
default.cfg
default.md5
mac.cfg

Two kinds of .cfg files, config.cfg and default.cfg, are kept in the NE for the NE to boot up with a set of deterministic configuration parameters. In order to guarantee these .cfg files are not corrupted, the NE also protect them by MD5 encryption.

Whenever the NE boots up, it executes the following procedure.

1. The NE first reads and checks config.cfg and try to rebuild the previous configuration accordingly.
2. If the config.cfg is absent or is corrupted, the NE will read and check default.cfg and try to rebuild the default configuration accordingly.
3. If the default.cfg is absent or is corrupted, the NE will use its internal setting to rebuild the factory-default configuration accordingly

Managing the Boot Section

The NE supports two boot sections ‘opCodeA’ and ‘opCodeB’, each contains the necessary firmware for the system. With 2 boot sections, the original NE firmware can be kept as it is. As a result, the operator is able to recover the NE whenever it fails to upgrade NE firmware due to any reason (ex. the upgraded firmware is corrupted due to network failure.)

To this end, it is recommened the operator to upload the new firmware to the ‘opCodeA’ if the current boot partition is ‘opCodeB’.

Please refer to Section “NE Firmware Upgrade” of Chapter 3 for the example of their usage.

Use the command “**boot-device**” to manage the boot section of the system.

```
CLI# boot-device
```

Table 3-14 Managing the Boot Section

The following command is to identify the startup boot section.
CLI# boot-device set {opCodeA | opCodeB}
The following command is to display the current boot device and firmware file.
CLI# boot-device show

NE Firmware Upgrade

NE provides NC/ADSL LC Firmware Upgrade related commands to load the new firmware to the NC on-board flash (non-violent memory) by FTP. The firmware upgrade procedures are as follows.

Step 1 Check the current boot partition via the CLI command:.

```
CLI# boot-device show
current boot device    : opCodeB:xxxxx.enc
next boot device       : opCodeB:xxxxx.enc
```

Step 2 Open the DOS prompt window (or environment) on personal computer (PC).

Step 3 Go to the directory where the new firmware is saved, and then login the NCT192 by FTP

Step 4 Upload the new firmware to the target partition via FTP by the following commands. Example 28 shows an example of uploading firmware to NE.

ftp> **cd opCodeB:** (or ftp> **cd opCodeA:**)
ftp> **bin**
ftp> **put xxxxx.enc**

Step 5 Change the next boot partition to let the NE be rebooted by executing the new image (Refers to Table 3-14 Managing the Boot Section)

```
CLI# boot-device set opCodeA
CLI# boot-device show
current boot device    : opCodeB:xxxxx.enc
next boot device       : opCodeA:xxxxx.enc
```

It is noted that login device via FTP must be used the read-write authorization. The default username/password is **admin/admin**.

Example 28 Upload NC/ADSL LC Firmware to Flash Memory of NC through FTP

```
Upgrade nct192.enc (image file of NC)

root@redhat9:/tmp> ftp 192.168.192.1
Connected to 192.168.192.1 (192.168.192.1).

Name (192.168.192.1:axdsl): admin
331 Password required
Password:
230 User logged in
ftp> cd opCodeA:
250 Changed directory to "opCodeA:"
ftp> bin
200 Type set to I, binary mode
ftp> put nct192.enc
200 Port set okay
150 Opening BINARY mode data connection
226- CAUTION:Please wait for 120 seconds or check the Flash LED -
226 Transfer complete
ftp: 3126797 bytes sent in 6.91Seconds 452.70Kbytes/sec.
ftp> bye
221 Bye...see you later
Upgrade nct1901fw.enc (DSP code of LC)

root@redhat9:/tmp> ftp 192.168.192.1
Connected to 192.168.192.1 (192.168.192.1).

Name (192.168.192.1:axdsl): admin
331 Password required
Password:
230 User logged in
ftp> cd opCodeA:
250 Changed directory to "opCodeA:"
ftp> bin
200 Type set to I, binary mode
ftp> put nct1901fw.enc
200 Port set okay
150 Opening BINARY mode data connection
226- CAUTION:Please wait for 120 seconds or check the Flash LED -
226 Transfer complete
ftp: 457808 bytes sent in 1.03Seconds 444.04Kbytes/sec
ftp> bye
221 Bye...see you later
Upgrade nct1901br.enc (Booter of LC)

root@redhat9:/tmp> ftp 192.168.192.1
Connected to 192.168.192.1 (192.168.192.1).

Name (192.168.192.1:axdsl): admin
331 Password required
Password:
230 User logged in
ftp> cd opCodeA:
250 Changed directory to "opCodeA:"
ftp> bin
200 Type set to I, binary mode
ftp> put nct1901br.enc
200 Port set okay
150 Opening BINARY mode data connection
226- CAUTION:Please wait for 120 seconds or check the Flash LED -
226 Transfer complete
ftp: 32892 bytes sent in 0.11Seconds 299.02Kbytes/sec
ftp> bye
221 Bye...see you later
```

Make sure the source image file that you select is accordant to the NE model; else the NE may not run well with the upgraded firmware image after rebooting.

NE Firmware Upgrade in Cascade mode

NE provides NC/ADSL LC Firmware Upgrade related commands to load the new firmware to the NC on-board flash (non-violent memory) by FTP. The Remote-NE firmware upgrade procedures are as follows.

Step 1 "Clogin" to check the current boot partition of Remote-NE via the CLI command:.

```
CLI# clogin 1
CLI#
       Please type "@.<cr>" to locally close connection
Login:admin
Password:

CLI# boot-device show
current boot device    : opCodeB:xxxxx.enc
next boot device       : opCodeB:xxxxx.enc
```

Step 2 Open the DOS prompt window (or environment) on personal computer (PC).

Step 3 Go to the directory where the new firmware is saved, and then login the NCT192 by FTP

Step 4 Upload the new firmware to the target partition via FTP by the following commands. Example 29 shows an example of uploading firmware to Remote-NE.

ftp> **bin**
ftp> **put xxxxx.enc (Client filename) \\1 (Remote ID) \ opCodeB:\xxxxx.enc (Remote filename)**

Step 5 Change the next boot partition to let the Remote-NE be rebooted by executing the new image (Refers to Table 3-14Managing the Boot Section)

```
CLI# boot-device set opCodeA
CLI# boot-device show
current boot device    : opCodeB:xxxxx.enc
next boot device       : opCodeA:xxxxx.enc
```

It is noted that login device via FTP must be used the read-write authorization. The default username/password is **admin/admin**.

Example 29 Upload NC/ADSL LC Firmware to Flash Memory of a Remote-NE through FTP

```
Upgrade nct192.enc (image file of NC)

root@redhat9:/tmp> ftp 192.168.192.1
Connected to 192.168.192.1 (192.168.192.1).

Name (192.168.192.1:axdsl): admin
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put nct192.enc \\1\opCodeA:\nct192.enc
200 Port set okay
150 Opening BINARY mode data connection
226- CAUTION:Please wait for 120 seconds or check the Flash LED -
226 Transfer complete
ftp: 3126797 bytes sent in 6.91Seconds 452.70Kbytes/sec.
```

```
ftp> bye
221 Bye...see you later


Upgrade nct1901fw.enc (DSP code of LC)

root@redhat9:/tmp> ftp 192.168.192.1
Connected to 192.168.192.1 (192.168.192.1).

Name (192.168.192.1:axdsl): admin
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put nct1901fw.enc \\1\opCodeA:\nct1901fw.enc
200 Port set okay
150 Opening BINARY mode data connection
226- CAUTION:Please wait for 120 seconds or check the Flash LED -
226 Transfer complete
ftp: 457808 bytes sent in 1.03Seconds 444.04Kbytes/sec
ftp> bye
221 Bye...see you later
Upgrade nct1901br.enc (Booter of LC)

root@redhat9:/tmp> ftp 192.168.192.1
Connected to 192.168.192.1 (192.168.192.1).

Name (192.168.192.1:axdsl): admin
331 Password required
Password:
230 User logged in
ftp> bin
200 Type set to I, binary mode
ftp> put nct1901br.enc \\1\opCodeA:\nct1901br.enc
200 Port set okay
150 Opening BINARY mode data connection
226- CAUTION:Please wait for 120 seconds or check the Flash LED -
226 Transfer complete
ftp: 32892 bytes sent in 0.11Seconds 299.02Kbytes/sec
ftp> bye
221 Bye...see you later
```

Make sure the source image file that you select is accordant to the Remote-NE model; else the NE may not run well with the upgraded firmware image after rebooting.

SHDSL Firmware Upgrade

This section depicts the procedures to upgrade the firmware version of the SHDSL line card; the higher version will bring new features and functions of the SHDSL line card.

CLI employs a NE SHDSL Firmware Upgrade utility to transfer the new code files to the memory of NC card by FTP (File Transfer Protocol), and then upgrades this new version from memory to SHDSL line card. You can follow the procedures below to update your SHDSL line card if necessary.

Step 1 Open the DOS prompt window and go to the directory where the new firmware is.

Step 2 Upload the new SHDSL firmware to the flash memory of NC through FTP. Example 30 shows an example of uploading SHDSL firmware from local host to the flash memory of NC.

Step 3 Use the commands described in Table 3-15 to upgrade the new firmware to SHDSL line card and wait for the state of upgrade to be finished. Example 31 shows an example of uploading SHDSL firmware from NC to NE.

Example 30 Upload SHDSL Firmware to Flash Memory of NC through FTP

```
D:\image\SHDSL Firmware>ftp 192.168.192.1
Connected to 192.168.192.1.
220-=============================================================================-
220-                Welcome to the IP-DSLAM FTP Server                          -
220-                                                                            -
220- CAUTION: It´s your responsibility to use the FTP service correctly -
220-          , please put the right files into the right file system.  -
220 =============================================================================-
User (192.168.192.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp>
ftp> cd shdsl:
250 Changed directory to "shdsl:/"
ftp> put TEImage.bin.gz
200 Port set okay
150 Opening BINARY mode data connection
226- CAUTION:Please wait for 120 seconds or check the Flash LED -
226 Transfer complete
ftp: 1834196 bytes sent in 1.30Seconds 1414.18Kbytes/sec.
ftp>
ftp> bye
221 Bye...see you later
```

Table 3-15 SHDSL Firmware Upgrade

The following command is to upgrade SHDSL firmware from flash memory to SHDSL line card.	
CLI# shdsl-fw-upgrade start <*lc-range*>	
The following command is to show the upgrade status.	
CLI# shdsl-fw-upgrade show	
Parameters	**Task**
<*lc-range*>	This specifies the slot index of target SHDSL line card. **Type:** Mandatory **Valid values:** 1 ~ 4

Example 31 Upload SHDSL Firmware from NC to SHDSL Line Card

```
CLI# shdsl-fw-upgrade start 4
OK: Please reset LC after "finished" state

CLI# shdsl-fw-upgrade show

SHDSL firmware upgrade state
    LC  type               state
    --  -----  ------------------------------
     1   ADSL                              n/a
     2   ADSL                              n/a
     3   ADSL                              n/a
     4  SHDSL  transmission of firmware image
```

Configuring the System Date and Time

You can set the date and time parameters as part of the initial system configuration and set the system date and time by using the "**datetime**" command at the prompt of CLI#.

The date and time will be reset due to reboot system. However, the NE will synchronize its date and time with the configured time server's.

(Please refer to Section "Configuring the Internet Time Server" for the setting of time server.

Table 3-16 shows the CLI commands to perform the configuration of system data and time. Example 32 shows the usage of these commands as well as its related parameters.

Table 3-16 System Date and Time Configuration

The following command is to set the system date time.
CLI# datetime set <*date*> <*time*>
The following command is to set the GMT time zone for system.
CLI# datetime timezone <*zone*>
The following command is to monitor the current system time.
CLI# datetime show

Parameters	Task
<*date*>	Identify the year, month, and date. **Type:** Mandatory **Valid values:** yyyy-mm-dd
<*time*>	Identify the time in hour, minute, and second. **Type:** Mandatory **Valid values:** hh:mm:ss
{*zone*}	Identify the GMT time zone. **Type:** Mandatory **Valid values:** -12 ~ +13

Example 32 Configure the system date and time

```
CLI# datetime set 2005-03-10 10:38:00
OK

CLI# datetime timezone +8
OK

CLI# datetime show
datetime: 2005-03-10 10:38:11 GMT+8
```

Configuring the Internet Time Server

A time server is a server that reads the actual time from a reference clock and distributes this information to its clients using a computer network. The NE supports to synchronize its date and time with the configured time server's via the Simple Network Time Protocol (SNTP)

We use the following steps to configure the time sever of NCT192 IP-DSLAM:

Step 1: Set the time server to let the clock of NCT192 IP-DSLAM be synchronized with an Internet time server's.

Step 2: Enter the "**config time-service**" sub-group directory to configure the Internet time server.

```
CLI# config time-service
CLI(config time-service)#
```

Table 3-17 shows the CLI commands to perform the Internet Time Server setting. Example 33 shows the usage of these commands as well as their related parameters.

Table 3-17 Internet Time Server Setting

The following command is to enable the time server IP address or domain name.
CLI(config time-service)# servers set <*server1* | *server2* | *server3*> <*address*>
The following command is to disable the time server.
CLI(config time-service)# servers delete <*server1* | *server2* | *server3*>
The following command is to define the synchronization protocol.
CLI(config time-service)# set protocol <*none* | *sntp*>
The following command is to define the synchronization time period.
CLI(config time-service)# set timezone <*zone-value*>
The following command is to define the synchronization time period.
CLI(config time-service)# set period <*time*>
The following command is to display the time server configuration information.
CLI(config time-service)# show
The following command is to manually synchronize with time server.
CLI(config time-service)# update

Parameters	Task
<*address*>	This specifies the network IP address or domain name for Internet time server. **Type:** Mandatory **Valid values:** Any valid class A/B/C IP address or domain name
<*zone-value*>	Identify the GMT time zone. **Type:** Mandatory **Valid values:** -12 ~ +13
<*time*>	This specifies the automatic synchronizing time period **Type:** Mandatory **Valid values:** 1 ~ 1440 Minutes

Example 33 Set the time server IP address or domain name

```
CLI(config time-service)# servers set server1 220.130.158.52
OK

CLI(config time-service)# set protocol sntp
OK

CLI(config time-service)# set timezone +12
OK

CLI(config time-service)# update
OK

CLI(config time-service)# show

Time protocol: SNTP
Update period: 12 hr 0 min
Time servers:
    [server1]
      internet address: 220.130.158.52
                status: backup mode
    [server2]
      internet address:
                status: not set
    [server3]
      internet address:
                status: not set
```

```
[time zone]  GMT+12
```

Configuring the DNS Server

The DNS (Domain Name System) server is used for the resolution of domain name. For example, a query for www.cisco.com will receive a reply with the IP address of the web server of Cisco. Therefore the DNS Server is designed for the resolution of domain name. In other words, the DNS replies the corresponding IP address to the URL like the given example.

Enter to the "**config dns**" sub-group directory to configure the DNS server.

```
CLI# config dns
CLI(config dns)#
```

Table 3-18 shows the CLI commands to perform the DNS server setting. Example 34 shows the usage of these commands as well as its related parameters.

Table 3-18 DNS Server Setting

The following command is to define the DNS server IP address.	
CLI(config dns)# set {*dns1* | *dns2* | *dns3*} <*ip-addr*>	
The following command is to delete the DNS server.	
CLI(config dns)# del {*dns1* | *dns2* | *dns3*}	
The following command is to display the DNS server.	
CLI(config dns)# show	
Parameters	**Task**
<*ip-addr*>	This specifies the DNS server IP address. **Type:** Mandatory

Example 34 Add a new DNS server to the system

```
CLI(config dns)# set dns1 168.95.1.1
Set OK.

CLI(config dns)# set dns2 168.95.1.88
Set OK.

CLI(config dns)# show
DNS server IP
             dns1             dns2             dns3
    ---------------  ---------------  ---------------
       168.95.1.1      168.95.1.88          0.0.0.0
```

Ambient Temperature

Ambient temperature is a common term to denote a certain temperature within enclosed space in which the NCT192 IP-DSLAM is accustomed.

Enter the "**config hw-sensor**" sub-group directory to set the temperature threshold of hardware sensor of NCT192 IP-DSLAM.

```
CLI# config hw-sensor
CLI(config hw-sensor)#
```

Table 3-19 shows the CLI commands to perform the configuration of ambient temperature. Example 35 shows the usage of these commands as well as its related parameters.

Table 3-19 Configuring Ambient Temperature

The following command is to set the temperature threshold of the system.	
CLI(config hw-sensor)# set temp <*temp-high*> <*temp-low*>	
The following command is to show the current setting.	
CLI(config hw-sensor)# show	
Parameters	**Task**
<*temp-high*>	This specifies the high temperature threshold. Whenever the ambient temperature is higher than <*temp-high*> , the NE sends alarm traps to the configured trap hosts (NCT192 LCT or NCT192 server) **Type:** Mandatory **Valid values:** -20 ~ 100 (degrees centigrade)
<*temp-low*>	This specifies the low temperature threshold. Whenever the ambient temperature is lower than <*temp-low*> , the NE sends alarm traps to the configured trap hosts (NCT192 LCT or NCT192 server) **Type:** Mandatory **Valid values:** -20 ~ 100 (degrees centigrade)

Example 35 Set the temperature threshold of the system

```
CLI(config hw-sensor)# set temp 70 -10
OK

CLI(config hw-sensor)# show

    sensor temperature thresholds: high  low
                                   ----  ----
                                     70   -10
```

Chapter 4 Managing the System Profiles

A profile is a named list of configuration parameters with a value assigned to each parameter. By using a profile, the operator can configure the NE without keying in a lot of configuration parameters. However, when the operator modifies a profile, the modification will affect all ports using that profile.

This chapter describes the management of two kinds of profiles, data transport related profiles and alarm definition profile. The alarm definition profile defines the attributes of the report (alarm) of abnormality launched by the NE.

As to the data transport related profiles, they are

- xDSL Profile
- VLAN Profile

The xDSL Profile indicates the ADSL Profile and SHDSL Profile. It defines the attributes of the connection established via the xDSL subscriber loop. As to the VLAN Profile, it defines the attributes of services/applications applied to the xDSL subscriber.

Figure 4-1 and Table 4-1 help you to understand each profile and their interrelationship.

As shown in Figure 4-1, NE forwards traffic on 2 kinds of connections, unicast connection and multicast connection, on the Data Level. For the unicast connection, it carries all traffic (unicast and broadcast) except multicast traffic. The attributes of unicast connection are specified by the IP Traffic Profile. As for the multicast connection, its attributes are specified by the Multicast Channel Profile. Moreover, the NE also supports to restrict the subscriber to receive a set of specific Multicast Channels. Multicast Service Profile records the set of specific Multicast Channels.

Figure 4-1 Interrelationship of Data Transport Related Profiles

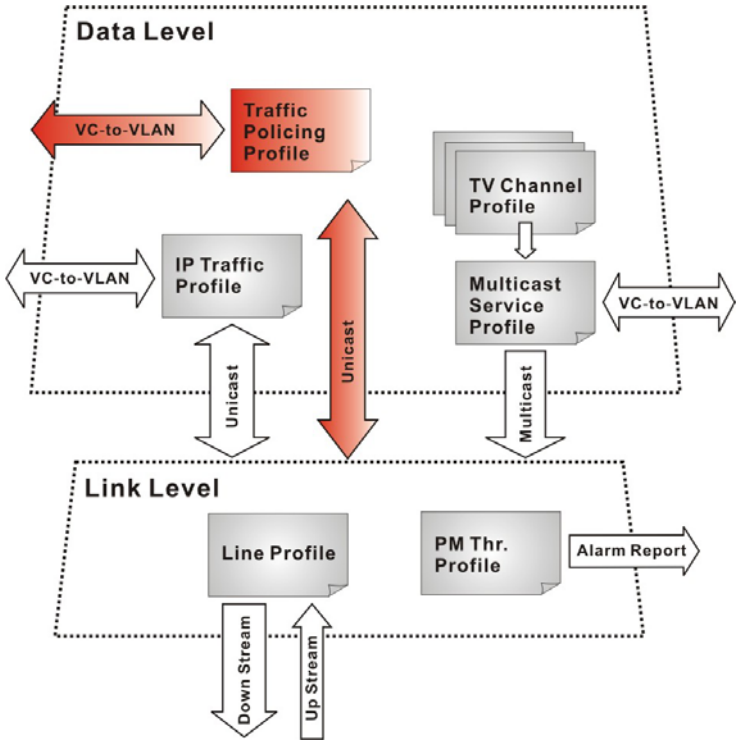


Table 4-1 Data Transport Related Profiles

Profile		Capacity	Level	Category	Description
xDSL Profile	Line Profile	60 sets	Link	Loop	Define the attributes of xDSL loop connection.
	PM Threshold Profile	60 sets	Link	Loop	Report the message if loop connection error across the threshold.
	Traffic Policing Profile (ADSL LC only)	60 sets	Data	User Data	Define the rule of traffic policing for user data.
VLAN Profile	IP Traffic Profile	60 sets	Data	Unicast	Define the traffic bandwidth of Unicast connection.
	Multicast Service Profile	60 sets	Data	Multicast	A set of service selected from menu list.
	Multicast Channel Profile	800 sets	Data	Multicast	A menu list of multicast channel, it also defines the traffic bandwidth of Multicast connection.

To make Traffic Policing Profile take effect, it needs to set IP Traffic Profile properly. Please refer to the NOTE under “Configuring the Traffic Policing Profile”.

To make an xDSL line work normally, the IP Traffic Profile is essential. As to the Traffic Policing Profile, it is optional and is only applicable to ADSL LC.

A profile is a named list of configuration parameters with a value assigned to each parameter. When you delete a profile you will affect the change on all port or connection using that profile. If you want to change a single port or a subset of ports, you can create another profile with desired parameters, and then assign the new profile to the desired port.

This chapter contains the following sections:

- Configuring the xDSL Profile
  - Configuring the ADSL Connection Profile
  - Configuring the ADSL Performance Alarm Profile
  - Configuring the Traffic Policing Profile
  - Configuring the SHDSL Connection Profile
  - Configuring the SHDSL Performance Alarm Profile
- Configuring the VLAN Profile
  - VLAN Profile contains 2 categories of profiles.
- Configuring the IP Traffic Profile
- Configuring the Multicast Service Related Profile

Configuring the xDSL Profile

The xDSL profiles enable you to simplify the process to configure the different xDSL loops with the same loop/data connection attributes. For example, you may classify the subscribers to several categories like category of residential customers, category of small office customers, category of enterprise customers and so on. Each category of subscribers is with the same loop/data connection attributes. Different categories are with their specific attributes like the line speed and performance parameters to secure their particular service quality. Once the profiles are created, you can easily assign the xDSL subscriber with the request xDSL loop attributes.

This section depicts the supported xDSL profiles.

- Configuring the ADSL Connection Profile
- Configuring the ADSL Performance Alarm Profile
- Configuring the Traffic Policing Profile
- Configuring the SHDSL Connection Profile
- Configuring the SHDSL Performance Alarm Profile

Configuring the ADSL Connection Profile

The ADSL connection profile indicates the expected overall physical parameters of the ADSL line port. This profile describes the communication at the ADSL layer. A number of parameters will be specified such as fast/interleaved, rate adaptation mode, noise margin, power spectrum density, and transmit rate.

Enter to the "**config profile adsl-conf**" sub-group directory to manage the ADSL connection profile.

```
CLI# config profile adsl-conf
CLI(config profile adsl-conf)#
```

Table 4-2 shows the connection profile configuration of the ADSL line. Example 36 shows the usage of these commands as well as its related parameters

Table 4-2 ADSL Connection Profile Configuration

The following command is to generate a new ADSL connection profile.
CLI(config profile adsl-conf)# add <*profile-name*>
The following command is to remove the specific ADSL connection profile.
CLI(config profile adsl-conf)# del <*profile-name*>
The following command is to activate the specific ADSL connection profile.
CLI(config profile adsl-conf)# enable <*profile-name*>
The following command is to deactivate the specific ADSL connection profile.
CLI(config profile adsl-conf)# disable <*profile-name*>
The following command is to modify the profile rate mode to adaptive with desired parameters.
CLI(config profile adsl-conf)# set adaptive-rate <*profile-name*> <*us-min-rate*> <*us-max-rate*> <*ds-min-rate*> <*ds-max-rate*>

Table 4-2 ADSL Connection Profile Configuration (continued)

The following command is to modify the profile rate mode to dynamic with desired parameters.
CLI(config profile adsl-conf)# set dynamic-rate <*profile-name*> <*us-min-rate*> <*us-max-rate*> <*ds-min-rate*> <*ds-max-rate*> <*us-down-shift*> <*us-up-shift*> <*ds-down-shift*> <*ds-up-shift*>
The following command is to modify the profile rate mode to fix with desired parameters.
CLI(config profile adsl-conf)# set fixed-rate <*profile-name*> <*us-rate*> <*ds-rate*>
The following command is to modify the profile line mode to interleaved path with latency.
CLI(config profile adsl-conf)# set line-mode <*profile-name*> **interleave** <max-*us-latency*> <max-*ds-latency*> <*min-us-inp*> <*min-ds-inp*>
The following command is to modify the profile line mode to fast path.
CLI(config profile adsl-conf)# set linemode <*profile-name*> **fast**
The following command is to modify the profile PSD (Power Spectrum Density) with desired parameters.
CLI(config profile adsl-conf)# set psd <*profile-name*> <*us-psd*> <*ds-psd*>
The following command is to modify the upstream or downstream shelf SNR margin due to dynamic rate mode.
CLI(config profile adsl-conf)# set snr-margin <profile-name> {us | ds} <target-snr> <min-snr><max-snr>
The following command is to modify the upstream or downstream shelf SNR margin due to dynamic rate mode.
CLI(config profile adsl-conf)# set shift-snr <profile-name> {us | ds} <down-shift-snr> <up-shift-snr>
The following command is to modify the ADSL2/ADSL2+ power automatic management for L2 state.
CLI(config profile adsl-conf)# set pwr-mgt <profile-name> **l2 automatic** <l2-min-rate> <l2-max-rate> <l2-low-time> <l0-time>
The following command is to modify the ADSL2/ADSL2+ power manual management for L2 state.
CLI(config profile adsl-conf)# set pwr-mgt <profile-name> **l2 manual** <l2-min-rate> <l2-max-rate>
The following command is to modify the ADSL2/ADSL2+ power management for L3 state.
CLI(config profile adsl-conf)# set pwr-mgt <*profile-name*> **l3** <*denied* | *accepted*>
The following command is to monitor the ADSL connection profile information.
CLI(config profile adsl-conf)# show [<*profile-name*>]

Table 4-2 ADSL Connection Profile Configuration (continued)

Parameters	Task
<profile-name>	This specifies the ADSL connection profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<us-min-rate>	Defines upstream minimum transmit rate, this parameter is available for adaptive and dynamic rate mode. **Type:** Mandatory **Valid values:** 64 ~ 2976 (multiple of 32 kbps) **Default value:** 64 kbps (due to profile generated)
<us-max-rate>	Defines upstream maximum transmit rate, this parameter is available for adaptive and dynamic rate mode. **Type:** Mandatory **Valid values:** 64 ~ 2976 (multiple of 32 kbps) **Default value:** 64 kbps (due to profile generated)
<ds-min-rate>	Defines downstream minimum transmit rate, this parameter is available for adaptive and dynamic rate mode. **Type:** Mandatory **Valid values:** 32 ~ 29984 (multiple of 32 kbps) **Default value:** 32 kbps (due to profile generated)
<ds-max-rate>	Defines downstream maximum transmit rate, this parameter is available for adaptive and dynamic rate mode. **Type:** Mandatory **Valid values:** 32 ~ 29984 (multiple of 32 kbps) **Default value:** 32 kbps (due to profile generated)
<us-rate>	Defines upstream transmit rate, this parameter is available for fixed rate mode. **Type:** Mandatory **Valid values:** 64 ~ 2976 (multiple of 32 kbps) **Default value:** 64 kbps (due to profile generated)
<ds-rate>	Defines downstream transmit rate, this parameter is available for fixed rate mode. **Type:** Mandatory **Valid values:** 32 ~ 29984 (multiple of 32 kbps) **Default value:** 32 kbps (due to profile generated)
< us-down-shift >	Defines the minimum time interval during which the upstream noise margin should stay below the Downshift SNR before the ATU-R triggers the SRA process to decrease the line rate. **Type:** Mandatory **Valid values:** 0 ~ 16383 (seconds) **Default value:** 0 sec (due to profile generated)
< us-up-shift >	Defines the minimum time interval during which the upstream noise margin should stay above the Upshift SNR before the ATU-R triggers the SRA process to increase the line rate. **Type:** Mandatory **Valid values:** 0 ~ 16383 (seconds) **Default value:** 0 sec (due to profile generated)

Table 4-2 ADSL Connection Profile Configuration (continued)

Parameters	Task
< *ds-down-shift* >	Defines the minimum time interval during which the downstream noise margin should stay below the Downshift SNR before the ATU-C triggers the SRA process to decrease the line rate. **Type:** Mandatory **Valid values:** 0 ~ 16383 (seconds) **Default value:** 0 sec (due to profile generated)
< *ds-up-shift* >	Defines the minimum time interval during which the downstream noise margin should stay above the Upshift SNR before the ATU-C triggers the SRA process to increase the line rate. **Type:** Mandatory **Valid values:** 0 ~ 16383 (seconds) **Default value:** 0 sec (due to profile generated)
< max-*us-latency*>	Defines the maximum upstream interleaved path latency. It applies only to the interleave channel and defines the mapping between subsequent input bytes at the inter-leaver input and their placement in the bit stream at the interleave output. Larger numbers provide greater separation between consecutive input bytes in the output bit stream, allowing for improved impulse noise immunity at the expense of payload latency. **Type:** Mandatory **Valid values:** 1 ~ 255 (milliseconds) **Default value:** 0 msec (due to profile generated)
< max-*ds-latency*>	Defines the maximum downstream interleaved path latency. It applies only to the interleave channel and defines the mapping between subsequent input bytes at the inter-leaver input and their placement in the bit stream at the interleave output. Larger numbers provide greater separation between consecutive input bytes in the output bit stream, allowing for improved impulse noise immunity at the expense of payload latency. **Type:** Mandatory **Valid values:** 1 ~ 255 (milliseconds) **Default value:** 0 msec (due to profile generated)
<*min-us-inp*>	Defines the minimum upstream INP (Impulse Noise Protect) capability. It indicates the multiple of INP symbol. **Type:** Mandatory **Valid values:** {0 | 1/2 | 1 | 2 | 4 | 8 | 16} **Default value:** 0 (due to profile generated)
<*min-ds-inp*>	Defines the minimum downstream INP (Impulse Noise Protect) capability. It indicates the multiple of INP symbol. **Type:** Mandatory **Valid values:** {0 | 1/2 | 1 | 2 | 4 | 8 | 16} **Default value:** 0 (due to profile generated)
<*us-psd*>	Defines upstream power spectrum density level. **Type:** Mandatory **Valid values:** -40.0 ~ 4.0 (dB/Hz) **Default value:** 0 dB/Hz (due to profile generated)
<*ds-psd*>	Defines downstream power spectrum density level. **Type:** Mandatory **Valid values:** -40.0 ~ 4.0 (dB/Hz) **Default value:** 1.0 dB/Hz (due to profile generated)

Table 4-2 ADSL Connection Profile Configuration (continued)

Parameters	Task
<target-snr>	Defines target SNR (Signal-to-Noise Ratio) margin for upstream or downstream signal. **Type:** Mandatory **Valid values:** 0.0 ~ 31.0 (dBm) **Default value:** 6.0 dBm (due to profile generated)
<min-snr>	Defines minimum SNR margin for upstream or downstream signal. **Type:** Mandatory **Valid values:** 0.0 ~ 31.0 (dBm) **Default value:** 0 dBm (due to profile generated)
<max-snr>	Defines maximum SNR margin for upstream or downstream signal. **Type:** Mandatory **Valid values:** 0.0 ~ 31.0 (dBm) **Default value:** 31.0 dBm (due to profile generated)
<down-shift-snr>	Defines down-shift SNR margin for upstream or downstream signal. **Type:** Mandatory **Valid values:** 0.0 ~ 31.0 (dBm) **Default value:** 0 dBm (due to profile generated)
<up-shift-snr>	Defines up-shift SNR margin for upstream or downstream signal. **Type:** Mandatory **Valid values:** 0.0 ~ 31.0 (dBm) **Default value:** 0 dBm (due to profile generated)
<mode>	Defines line power management L2 mode to be either 'automatic' or 'manual'. Automatic – This mode enables the ADSL line to automatically transfer from the L0 (full-on) state to the L2 (low power) state whenever the downstream net data rate is lower than expected. And it also enables the ADSL line to automatically transfer from the L2 state to the L0 state once the NE begins to drop the downstream data. Manual –This mode allows the operator to manually force the specific ADSL line to transfer from the L2 state to the L0 state, and vice versa. **Type:** Mandatory **Valid values:** {automatic | manual} **Default value:** manual
< l2-min-rate>	Defines minimum rate and low-bound to data rate for power management L2 state in 32 kbps steps. **Type:** Mandatory **Valid values:** 32 ~ 29984 kbps **Default value:** 64 kbps
< l2-max-rate>	Defines maximum rate to data rate for power management L2 state in 32 kbps steps. **Type:** Mandatory **Valid values:** 32 ~ 29984 kbps **Default value:** 29984 kbps
<l2-low-rate-time>	It specifies the contiguous time interval for which the downstream mean net data rate is below the 'L2 State Min & Low Rate' on a ADSL line. (See the Note below) **Type:** Mandatory **Valid values:** 0 ~ 65535 seconds **Default value:** 300 seconds
<l0-time>	It specifies the minimum time (seconds) the ADSL line must stay at the L0 state. During this time interval, the ADSL line is not allowed to transfer to the L2 state. It is the so-called L0-TIME as defined in ITU-T G.997.1. (See the Note below) **Type:** Mandatory **Valid values:** 0 ~ 65535 seconds **Default value:** 900 seconds
<denied | accepted>	Defines the management L3 request. If it is, the ADSL lines applied this profile will accept request from CPE and transfer their power management state into L3 by the CPE request. **Type:** Mandatory **Valid values:** {denied | accepted} **Default value:** accepted

Comparison of ADSL '**adaptive-rate** mode' and '**dynamic-rate** mode'.

- **Adaptive-rate** mode: When the ADSL loop is in the '**adaptive-rate** mode', the NE will re-try to establish a new lower-rate connection with the ATU-R whenever the NE or ATU-R detects 10 consecutive SESs (Severely Error Seconds) in this mode.
- **Dynamic-rate** mode: When the ADSL loop is in the '**dynamic-rate** mode', the NE will trigger the SRA (Seamless Rate Adaptation) process to change the line rates without losing the connection with ATU-R whenever the physical loop environment varies in this mode.

The associated parameters of the **Dynamic-rate** mode are as follows.

'<*up-shift-snr*>', '<*down-shift-snr*>', '< *us-up-shift* >/< *ds-up-shift* >' and '< *us-down-shift*>/< *ds-down-shift* >'

In the **Dynamic-rate** mode, the NE will lose the connection with ATU-R if it fails to complete the SRA process to change the line rates

The following relationship holds when setting their values.

<*min-snr*> ≤ <*down-shift-snr*> ≤ <*target-snr*> ≤ <*up-shift-snr*> ≤ <*max-snr*>.

Comparison of ADSL '**interleave** channel mode' and '**fast** channel mode'

- **Interleave** channel mode: When the ADSL loop is in the '**Interleave** channel mode', it enhances the immunity to the impulse noise like lighting. However, its side effect is to introduce the transmission latency. Hence it is suitable for the time-insensitive data transmission, like file transfer.
- **Fast** channel mode: When the ADSL loop is in the '**fast** channel mode', the latency introduced by the ADSL link is shortest. Hence, it is suitable for the transmission of time-sensitive information such as audio.

The default upstream/downstream PSD spectrums in G.992.1 ADSL, G.992.3 ADSL2 and G.992.5 ADSL2+ are different. To simply the configuration effort, <*us-psd*> and <*ds-psd*> here indicate the deviation from the default upstream and downstream PSD spectrums in G.992.x, respectively. Hence, it is recommended to set <*us-psd*> and <*ds-psd*> as zero in normal case.

The relationship among <*us-psd*>, observed upstream SNR margin, observed ADSL line upstream rate and ADSL line reach.

- Higher <*us-psd*> results in either higher observed SNR margin or higher observed ADSL line rate or longer ADSL line reach.
- Higher <*us-psd*> also results in more severe Cross Talk.

Hence, for fixed ADSL reach, you will observe either high SNR margin or high ADSL line rate. When you do not need high SNR margin or high ADSL line rate, you can lower the <*us-psd*> to save power (save money).

The above description applies to the relationship among <*ds-psd*>, observed downstream SNR margin, observed ADSL line downstream rate and ADSL line reach.

In order to save power, G.992.3 and G.992.5 define the power management function. The operator can either configure the ADSL line Transmission (Tx) power be either manually or automatically managed.

The automatic power management function enables the ADSL line to automatically transfer from the L0 (full-on) state to the L2 (low power) state whenever the downstream net data rate is lower than expected. And it also enables the ADSL line to automatically transfer from the L2 state to the L0 state once the NE begins to drop the downstream data.

Concepts about the setting of automatic L0/L2 power management (**l2 pwr-mgt)**

- The default values are to let the ADSL line be always in the L0 state. If you want to save power, you can alter these values.
- Whenever the ADSL chip detects that the subscriber's data traffic is low on this ADSL line, and it meets the criterion constructed by the setting of <l2-min-rate>, <l2-max-rate>, <l2-low-time> and <l0-time>. The ADSL chip will let the ADSL line enter L2 state to save power. (The ADSL chip will lower the PSD Spectrum to achieve this purpose)

In order to let the ADSL line avoid going into and out of L2 too often, the following L0↔L2 state transition criteria are adopted.

L0→L2:

- The ADSL line must stay at the L0 state for a period specified by 'L0 State Min Time to Start Monitoring' (i.e., the L0-TIME as defined in ITU-T G.997.1)
- After the L0-TIME, the NE begins to compute the mean net-data rate for a period of 'L2 State Low Rate Min Contiguous Time' on an ADSL line.
- The ADSL line transfers to the L2 state once the computed mean net-data rate is below the 'L2 State Min & Low Rate'.
- Once an ADSL line is at the L2 state, its downstream ADSL line rate is in the range from 'L2 State Min & Low Rate' to 'L2 State Max Rate'.

L2→L0:

- The ADSL line immediately transfers to the L0 state once the NE detects packet loss on the ADSL line in the down stream direction.

Example 36 Add a new ADSL connection profile with desired values

```
CLI(config profile adsl-conf)# add bank
OK

CLI(config profile adsl-conf)# set adaptive-rate bank 512 2048 1024 8192
OK

CLI(config profile adsl-conf)# set line-mode bank interleave 10 10 1 1
OK

CLI(config profile adsl-conf)# enable bank
OK

CLI(config profile adsl-conf)# show bank

profile [bank]
    status       : enabled
    line mode    : interleave
    rate mode    : adaptive
                                        up-stream   down-stream
                                       -----------  -----------
    fast rate (min/max)             :    512/2048    1024/8192 kbps
    interleave rate (min/max)       :    512/2048    1024/8192 kbps
    interleave max delay            :          10          10 ms
    interleave min INP symbol time  :           1           1
    target SNR margin               :         6.0         6.0 dB
    min./max. SNR margin            :    0.0/31.0    0.0/31.0 dB
    down/up shift SNR margin        :    3.0/20.0    3.0/20.0 dB
    down/up shift time              :   1000/1000    1000/1000 sec
    PSD                             :         0.0         0.0 dBm/Hz
    power management setting:
         L2-mode   L2-min-rate  L2-max-rate   CPE L3
        ---------  -----------  -----------  --------
           manual      32 kbps   29984 kbps  accepted
```

Attaching the ADSL connection profile to the proper ADSL line port can be tasked to the "**config port**" sub-group directory. It refers to the Section "Configuring the ADSL Line Port"of Chapter 5.

Once the ADSL connection profile is created, the operator can apply it to distinct ADSL line port by the CLI commands in the "**config port**" sub-group directory. Please refers to the Section "Configuring the ADSL Line Port"of Chapter 5. for the related command.

Configuring the ADSL Performance Alarm Profile

The PM threshold profile sets the threshold values for the performance parameters associated with the ADSL line. The NE will report the threshold-over trap (i.e. TCA, Threshold-Crossing Alarm) to the NCT192 LCT (or NCT192 Server) when the specified performance threshold is over.

During the accumulation cycle, if the current value of a performance parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the system and sent to trap station. TCAs provide early detection of performance degradation. When a threshold is crossed, the ADSL line port continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the NE never sends the corresponding TCA.

The NE supports to define the Near-End and Far-End thresholds of ES (Errored Seconds), SES (Severely Errored Seconds), and UAS (Unavailable Seconds) conditions in 15 minutes and 1 day interval. The definition of ES, SES and UAS are as follows.

- ES (Error Second)
  ES corresponds to "ES-L" defined in ITU-T G.997.1 (2003 Edition)
  ITU-T G.997.1 defines ES as a count of 1-second intervals with one or more CRC-8 anomalies summed over all received bearer channels, or one or more LOS defects, or one or more SEF defects, or one or more LPR defects.

- SES (Several Error Second)
  SES corresponds to the "SES-L" defined in ITU-T G.997.1 (2003 Edition).
  ITU-T G.997.1 defines ES as a count of 1-second intervals with 18 or more CRC-8 anomalies summed over all received bearer channels, or one or more LOS defects, or one or more SEF defects, or one or more LPR defects.

- UAS (UnAvailable Second)
  UAS corresponds to the "UAS-L" defined in ITU-T G.997.1 (2003 Edition).
  ITU-T G.997.1 defines ES as a count of 1-second intervals for which the ADSL line is unavailable. The ADSL line becomes unavailable at the onset of 10 contiguous SES-Ls. The 10 SES-Ls are included in unavailable time. Once unavailable, the ADSL line becomes available at the onset of 10 contiguous seconds with no SES-Ls. The 10 seconds with no SES-Ls are excluded from unavailable time. Some parameter counts are inhibited during unavailability

Enter to the "**config profile adsl-alarm**" sub-group directory to manage the ADSL performance alarm profile.

```
CLI# config profile adsl-alarm
CLI(config profile adsl-alarm)#
```

Table 4-3 shows the performance alarm profile configuration of the ADSL line. Example 37 shows the usage of these commands as well as its related parameters.

Table 4-3 ADSL Performance Alarm Profile Configuration

The following command is to generate a new ADSL performance alarm profile.
CLI(config profile adsl-alarm)# add <*profile-name*>
The following command is to remove the specific ADSL performance alarm profile.
CLI(config profile adsl-alarm)# del <*profile-name*>
The following command is to activate the specific ADSL performance alarm profile.
CLI(config profile adsl-alarm)# enable <*profile-name*>
The following command is to deactivate the specific ADSL performance alarm profile.
CLI(config profile adsl-alarm)# disable <*profile-name*>
The following command is to modify the performance ADSL alarm profile parameters at Near-End and Far-End.
CLI(config profile adsl-alarm)# set <*profile-name*> <*15min-es*> <*15min-ses*> <*15min-uas*> <*1day-es*> <*1day-ses*> <*1day-uas*> [*near* | *far*]
The following command is to monitor the ADSL performance alarm profile information.
CLI(config profile adsl-alarm)# show [<*profile-name*>]

Parameters	Task
<*profile-name*>	This specifies the performance alarm profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*15min-es*>	When the keyword "*near*" is set, This field indicates the threshold of Errored Seconds (ES) on the CO (Central Office) side during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. When the keyword "*far*" is set, This field indicates the threshold of Errored Seconds (ES) on the RT side (CPE) during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. **Type:** Mandatory **Valid values:** 0 ~ 900 **Default value:** 0 (due to profile generated)
<*15min-ses*>	When the keyword "*near*" is set, This field indicates the threshold of Severely Errored Seconds (SES) on the CO (Central Office) side during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. When the keyword "*far*" is set, This field indicates the threshold of Severely Errored Seconds (SES) on the RT side (CPE) during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. **Type:** Mandatory **Valid values:** 0 ~ 900 **Default value:** 0 (due to profile generated)

Table 4-3 ADSL Performance Alarm Profile Configuration (continued)

Parameters	Task
<15min-uas>	When the keyword "*near*" is set, This field indicates the threshold of Unavailable Seconds (UAS) on the CO (Central Office) side during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. When the keyword "*far*" is set, This field indicates the threshold of Unavailable Seconds (UAS) on the RT side (CPE) during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. **Type:** Mandatory **Valid values:** 0 ~ 900 **Default value:** 0 (due to profile generated)
<1day-es>	When the keyword "*near*" is set, This field indicates the threshold of Errored Seconds (ES) on the CO (Central Office) side during the last 1 day. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 1 day. When the keyword "*far*" is set, This field indicates the threshold of Errored Seconds (ES) on the RT side (CPE) during the last 1 day. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 1 day.. Type: Mandatory **Valid values:** 0 ~ 86400 **Default value:** 0 (due to profile generated)
<1day-ses>	When the keyword "*near*" is set, This field indicates the threshold of Errored Seconds (SES) on the CO (Central Office) side during the last 1 day. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 1 day. When the keyword "*far*" is set, This field indicates the threshold of Severely Errored Seconds (SES) on the RT side (CPE) during the last 1 day. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 1 day. **Type:** Mandatory **Valid values:** 0 ~ 86400 **Default value:** 0 (due to profile generated)
<1day-uas>	When the keyword "*near*" is set, This field indicates the threshold of Unavailable Seconds (UAS) on the CO (Central Office) side during the last 1 day. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 1 day. When the keyword "*far*" is set, This field indicates the threshold of Unavailable Seconds (UAS) on the RT side (CPE) during the last 1 day. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 1 day. **Type:** Mandatory **Valid values:** 0 ~ 86400 **Default value:** 0 (due to profile generated)
[*near* | *far*]	Identify the given performance parameter value in Near-End or Far-End side, CLI Ex will apply the same performance parameter value for Near-End and Far-End if not specify. **Type:** Optional **Valid values:** near, far

Example 37 Add a new performance alarm profile with correspond performance parameter values

```
CLI(config profile adsl-alarm)# add bank_pm
OK

CLI(config profile adsl-alarm)# set bank_pm 10 15 20 30 40 50
OK

CLI(config profile adsl-alarm)# enable bank_pm
```

```
OK

CLI(config profile adsl-alarm)# show

profile [bank_pm]: enabled
    side-end  15min-es  15min-ses  15min-uas  1day-es  1day-ses  1day-uas
    --------  --------  ---------  ---------  -------  --------  --------
    near end        10         15         20       30        40        50
     far end        10         15         20       30        40        50
```

Once the performance alarm profile is created, the operator can apply it to distinct ADSL line port by the CLI commands in the "**config port**" sub-group directory.

Please refer to the Section "Configuring the ADSL Line Port" of Chapter 5 for the related command.

Configuring the Traffic Policing Profile

Traffic policing is to monitor network traffic for conformity with the Service Level Agreement (SLA) between subscribers and ISP (or NSP).

According to the SLA, the edge network equipment (NE) either drops or marks subscriber's out-of-profile traffic with designated DSCP values to enforce compliance with that SLA. The traffic policing profile serves to keep the rules per the SLA.

Once the traffic policing profile is created, the operator can apply it to distinct ADSL line port by the CLI commands in the "**config port**" sub-group directory. Please refer to the Section "Configuring the ADSL Line Port" of Chapter 5 for the related command.

One example of application of traffic policing is as follows.

Suppose that the SLA defines that the subscriber can send upstream traffic at the rate up to 1.5Mbps. However, the NSP has the right to remark the DSCP value of traffic higher than 1Mbps when the network is in congestion.To accomplish this SLA, the operator can set the CIR to be 1Mbps, and set the out-of-profile action to remark the DSCP value to BE.

To verify the aforementioned setting, you can send 1.5Mega bit in one second in the upstream direction, then set the SmartBit (which connects to GE port to receive the upstream traffic) to capture the upstream traffic. And you will see that the DSCP of IP packet about 0.5Mbit is the value what you set "out-of-profile action"

Enter to the "**config profile metering"** sub-group directory to manage the traffic policing profile.

```
CLI# config profile metering
CLI(config profile metering)#
```

Table 4-4 shows the commands to perform the configuration of traffic policing profile.0 shows the usage of these commands as well as their related parameters.

Table 4-4 Traffic Policing Profile Configuration

The following command is to generate a new traffic policing profile.
CLI(config profile metering)# add <*profile-name*>
The following command is to remove the specific traffic policing profile.
CLI(config profile metering)# del <*profile-name*>
The following command is to modify the traffic policing profile and it desired parameters.
CLI(config profile metering)# set <*profile-name*> <*cir*> <*action*>
The following command is to monitor the traffic policing profile information.
CLI(config profile metering)# show [<*profile-name*>]

Parameters	Task
<*profile-name*>	This specifies the traffic policing profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*cir*>	Defines the committed information rate of traffic policing profile. **Type:** Mandatory **Valid values:** 0 ~ 2 (mbps)
<*action*>	This identifies which value will DSCP be replace, drop packets or do nothing when user's upstream traffic exceeds CIR. **Type:** Mandatory **Valid values:** no-action | drop | BE | AF11 | AF12 | AF13 | AF21 | AF22 | AF23 | AF31 | AF32 | AF33 | AF41 | AF42 | AF43 | EF

Example 38 Add a new traffic policing Profile with desired values

```
CLI(config profile metering)# add Adsl_tp
OK

CLI(config profile metering)# set Adsl_tp 100 AF32
OK

CLI(config profile metering)# show

Traffic Policing  [Adsl_tp]
    CIR (Mbps)  action
    ----------  ---------
           100  DSCP-AF32
```

The "Service Type Control" should be enabled when Traffic Policing Profile is assigned to xDSL subscribers (refers to Section "Defining the Line Card Operation Mode" of Chapter 5 for the commands related to the setting of "Service Type Control").

Please refer to Figure 6-4 and accompany paragraphs for more details of Differentiated Service Code Point.

Configuring the SHDSL Connection Profile

A profile corresponds to a particular set of parameters, and can be referenced to by separated SHDSL line port.

Enter to the "**config profile shdsl-conf**" sub-group directory to manage the SHDSL connection profile.

```
CLI# config profile shdsl-conf
CLI(config profile shdsl-conf)#
```

Table 4-5 shows the connection profile configuration of the SHDSL line. Example 36 shows the usage of these commands as well as its related parameters.

Table 4-5 SHDSL Connection Profile Configuration

The following command is to generate a new SHDSL connection profile.
CLI(config profile shdsl-conf)# add <*name*>
The following command is to remove the specific SHDSL connection profile.
CLI(config profile shdsl-conf)# del <*name*>
The following command is to activate the specific SHDSL connection profile.
CLI(config profile shdsl-conf)# enable <*name*>
The following command is to deactivate the specific SHDSL connection profile.
CLI(config profile shdsl-conf)# disable <*name*>
The following command is to set the line probe state before training with STU-R.
CLI(config profile shdsl-conf)# set line-probe <*name*> <*enabled-state*>
The following command is to set the PSD mask of the SHDSL connection profile.
CLI(config profile shdsl-conf)# set psd <*name*> <*psd-value*>
The following command is to set the single-pair minimum/maxmum rate of the SHDSL connection profile.
CLI(config profile shdsl-conf)# set rate <*name*> <*min-rate*> <*max-rate*>
The following command is to set the SNR margin of the SHDSL connection profile.
CLI(config profile shdsl-conf)# set snr-margin <*name*> <*down-current-snr*> <*down-worst-snr*> <*up-current-snr*> <*up-worst-snr*>
The following command is to set the transmission mode of the SHDSL connection profile.
CLI(config profile shdsl-conf)# set transmission <*name*> <*transmission-mode*>
The following command is to set the used SNR margins of the SHDSL connection profile.
CLI(config profile shdsl-conf)# set used-snr <*name*><*used-snr-list*>
The following command is to monitor the SHDSL connection profile information.
CLI(config profile shdsl-conf)# show [<*name*>]

Parameters	Task
<*name*>	It specifies the the SHDSL connection profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*min-rate*>	It specifies the minimum transmit rate, this parameter is available for adaptive. rate mode. **Type:** Mandatory **Valid values:** 72 ~ 2312 (multiple of 64 kbps) **Default value:** 72 kbps (due to profile generated)
<*max-rate*>	It specifies the maximum transmit rate, this parameter is available for adaptive . rate mode. **Type:** Mandatory **Valid values:** 72 ~ 2312 (multiple of 64 kbps) **Default value:** 72 kbps (due to profile generated)
<*psd-value*>	It specifies the setting of PSD Mask to be symmetric or asymmetric. **Type:** Mandatory **Valid values:** 1 = symmetric, 2 = asymmetric **Default value:** 1

Table 4-5 SHDSL Connection Profile Configuration (continued)

Parameters	Task
<*transmission-mode*>	It specifies the e transmission mode, Annex A, Annex B, or both. **Type:** Mandatory **Valid values:** 1:Annex.A or 2:Annex.B or 3:Both. **Default value:** 3
<*down-current-snr*>	It specifies the downstream current target SNR margin. **Type:** Mandatory **Valid values:** -10 ~ 21 (dBm) **Default value:** 6 dBm (due to profile generated)
<*down-worst-snr*>	It specifies the downstream worst target SNR margin **Type:** Mandatory **Valid values:** -10 ~ 21 (dBm) **Default value:** 6 dBm (due to profile generated)
<*up-current-snr*>	It specifies the upstream current target SNR margin. **Type:** Mandatory **Valid values:** -10 ~ 21 (dBm) **Default value:** 6 dBm (due to profile generated)
<*up-worst-snr*>	It specifies the upstream worst target SNR margin **Type:** Mandatory **Valid values:** -10 ~ 21 (dBm) **Default value:** 6 dBm (due to profile generated)
<*used-snr-list*>	It specifies that it uses SNR bit-map, 0:down-current, 1:down-worst, 2:up-current, 3:up-worst **Type:** Mandatory **Valid values:** 0, 1, 2, 3
<*enabled-state*>	It specifies to enable or disable the line probe state before training with STU-R. Enable: To make the 'line rate limit' up to 2312Kbps. Disable: To make the 'line rate limit' up to 1.5Mbps. **Type:** Mandatory **Valid values:** 1 =enable, 2= disable.

In the case that <*minrate*> is equal to <*maxrate*>, the SHDSL line is to be in the '**fixed-rate** mode'.

In the case that <*minrate*> is not equal to <*maxrate*>, the SHDSL line is to be in the '**adaptive-rate** mode'.

Example 39 Add a new SHDSL Connection Profile with desired values

```
CLI(config profile shdsl-conf)# add shdsl_conf
OK

CLI(config profile shdsl-conf)# set line-probe shdsl_conf 1
OK

CLI(config profile shdsl-conf)# set psd shdsl_conf 1
OK

CLI(config profile shdsl-conf)# set rate shdsl_conf 300 2312
OK

CLI(config profile shdsl-conf)# set snr-margin shdsl_conf 6 6 6 6
OK

CLI(config profile shdsl-conf)# set transmission shdsl_conf 1
OK

CLI(config profile shdsl-conf)# set used-snr shdsl_conf dc
OK
```

```
CLI(config profile shdsl-conf)# show

profile  [shdsl_conf]
    status                              : disabled
    single-pair minimum/maxmum rate     : 264K/2312K
    PSD mask                            : symmetric
    transmission mode                   : region1-Annex.A
    line probe support                  : enabled

    SNR margin:
        current down   worst down    current up     worst up      used SNR
        ------------  ------------  ------------  ------------  ------------
                   6             6             6             6            DC
```

Configuring the SHDSL Performance Alarm Profile

The PM threshold profile sets the threshold values for the performance parameters associated with the SHDSL line. The NE will report the threshold-over trap (i.e. TCA, Threshold-Crossing Alarm) to the NCT192 LCT (or NCT192 Server) when the specified performance threshold is over.

During the accumulation cycle, if the current value of a performance parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the system and sent to trap station. TCAs provide early detection of performance degradation. When a threshold is crossed, the SHDSL line port continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the NE never sends the corresponding TCA.

The NE supports to define the Near-End and Far-End thresholds of ES (Errored Seconds), SES (Severely Errored Seconds), and UAS (Unavailable Seconds) conditions in 15 minutes interval. The definition of ES, SES and UAS are as follows.

- ES (Error Second)
  ES corresponds to “ES-L” defined in ITU-T G.997.1 (2003 Edition)
  ITU-T G.997.1 defines ES as a count of 1-second intervals with one or more CRC-8 anomalies summed over all received bearer channels, or one or more LOS defects, or one or more SEF defects, or one or more LPR defects.

- SES (Several Error Second)
  SES corresponds to the “SES-L” defined in ITU-T G.997.1 (2003 Edition).
  ITU-T G.997.1 defines ES as a count of 1-second intervals with 18 or more CRC-8 anomalies summed over all received bearer channels, or one or more LOS defects, or one or more SEF defects, or one or more LPR defects.

- UAS (UnAvailable Second)
  UAS corresponds to the “UAS-L” defined in ITU-T G.997.1 (2003 Edition).
  ITU-T G.997.1 defines ES as a count of 1-second intervals for which the ADSL line is unavailable. The ADSL line becomes unavailable at the onset of 10 contiguous SES-Ls. The 10 SES-Ls are included in unavailable time. Once unavailable, the ADSL line becomes available at the onset of 10 contiguous seconds with no SES-Ls. The 10 seconds with no SES-Ls are excluded from unavailable time. Some parameter counts are inhibited during unavailability

Enter to the “**config profile shdsl-alarm**” sub-group directory to manage the SHDSL performance alarm profile.

```
CLI# config profile shdsl-alarm
CLI(config profile shdsl-alarm)#
```

Table 4-6 shows the performance alarm profile configuration of the SHDSL line. Example 40 shows the usage of these commands as well as its related parameters

Table 4-6 SHDSL Performance Alarm Profile Configuration

The following command is to generate a new SHDSL performance alarm profile.
CLI(config profile shdsl-alarm)# add <*name*>
The following command is to remove the specific SHDSL performance alarm profile.
CLI(config profile shdsl-alarm # del <*name*>
The following command is to activate the specific SHDSL performance alarm profile.
CLI(config profile shdsl-alarm # enable <*name*>
The following command is to deactivate the specific SHDSL performance alarm profile.
CLI(config profile shdsl-alarm)# disable <*name*>
The following command is to modify the SHDSL performance alarm profile parameters at Near-End.
CLI(config profile shdsl-alarm)# set <*name*> [**atte** <*atte*> **snr** <*snr*> **es** <*es*> **ses** <*ses*> **crc** <*crc*> **losws** <*losws*>**uas** <*uas*>]
The following command is to monitor the SHDSL performance alarm profile information.
CLI(config profile shdsl-alarm)# show <*name*>

Parameters	Task
<*name*>	This specifies the performance alarm profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*atte*>	This identifies the attenuation threshold. **Type:** Mandatory **Valid values:** 1 ~ 127
<*es*>	This field indicates the threshold of Errored Seconds (ES) on the CO (Central Office) side during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. **Type:** Mandatory **Valid values:** 0 ~ 900 **Default value:** 0 (due to profile generated)
<*ses*>	This field indicates the threshold of Errored Seconds (SES) on the CO (Central Office) side during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. **Type:** Mandatory **Valid values:** 0 ~ 900 **Default value:** 0 (due to profile generated)
<*crc*>	This identifies the CRC error threshold. **Type:** Mandatory **Valid values:** 0 ~ 44100
<*losws*>	This identifies the LOSWS error threshold. **Type:** Mandatory **Valid values:** 0 ~ 900
<*uas*>	This identifies the LOSWS error threshold. **Type:** Mandatory **Valid values:** 0 ~ 900
<*usa*>	This field indicates the threshold of Unavailable Seconds (UAS) on the CO (Central Office) side during the last 15 minutes. When the threshold is set to 10, the NE launches a trap (alarm) if the count of specific errors exceeds 10 during the last 15 minutes. **Type:** Mandatory **Valid values:** 0 ~ 900 **Default value:** 0 (due to profile generated)

Example 40 Add a new SHDSL port alarm profile with desired values

```
CLI(config profile shdsl-alarm)# add shdsl_ex
OK
```

```
CLI(config profile shdsl-alarm)# set shdsl_ex atte 127 snr 10 ses 100 crc 12800 losws 100 uas 100
OK

CLI(config profile shdsl-alarm)# enable shdsl_ex
OK

CLI(config profile shdsl-alarm)# show

Profile  [shdsl_ex]
    Status         : enabled
    Attenuation    : 127
    SNR margin     : 10

      ES          SES         CRC         LOSWS       UAS
    -------     -------     -------     -------     -------
         0      100         12800       100         100
```

Configuring the VLAN Profile

VLAN Profile contains 2 categories of profiles which are described in the following 2 sub-section.

- Configuring the IP Traffic Profile
- Configuring the Multicast Service

As shown in Figure 4-1, NE forwards traffic on 2 kinds of connections, unicast connection and multicast connection, on the Data Level. For the unicast connection, it carries all traffic (unicast and broadcast) except multicast traffic. The attributes of unicast connection are specified by the IP Traffic Profile. As for the multicast connection, its attributes are specified by the Multicast Channel Profile. Moreover, the NE also supports to restrict the subscriber to receive a set of specific Multicast Channels. Multicast Service Profile records the set of specific Multicast Channels.

Configuring the IP Traffic Profile

Similar to the traffic policing profile, the IP traffic profile serves to keep the rules to enforce compliance with that SLA. (Please refer to Section “Configuring the Traffic Policing Profile” of Chapter 4 for the description of traffic policing)

However, it is noted that the scope of traffic policing profile is to police the traffic on a whole ADSL line. As to the IP traffic profile, its scope of is to police the traffic on a PVC in an ADSL line.

The operator can create the IP Traffic Profile according to the SLA and apply it to the corresponding VC-to-VLAN on demand.

By configures IP Traffic Profile, the following traffic attributions of a PVC is specified.

- The maximum upstream/downstream net-data rate limit.
  The system drops upstream/downstream packets whenever it exceeds the corresponding specified rate
- The downstream priority of the PVC
  The system forwards the downstream packets in a differentiated manner. That is, the system only forwards the traffic on PVC of lower priority whenever either one of the following conditions happened:
  - There is no traffic on PVC of higher priority to be forwarded.
  - The volume of traffic on PVC of higher priority exceeds the specified downstream net-data rate in a unit time.
- The filtering of the downstream broadcasts traffic

Enter to the "**config profile ip-traffic**" sub-group directory to manage the IP traffic profile.

```
CLI# config profile ip-traffic
CLI(config profile ip-traffic)#
```

Table 4-7 shows the commands to perform the configuration of IP traffic profile. Example 41 shows the usage of these commands as well as their related parameters.

Table 4-7 IP Traffic Profile Configuration

The following command is to generate a new IP traffic profile.
CLI(config profile ip-traffic)# add <*name*>
The following command is to remove a new IP traffic profile.
CLI(config profile ip-traffic)# del <*name*>
The following command is to configure the rate limit of specific IP traffic profile.
CLI(config profile ip-traffic)# set <*name*> <*us-rate*> <*ds-rate*> <*vc-priority*> <*bcast-filter*>
The following command is to display the IP traffic profile information.
CLI(config profile ip-traffic)# show

Parameters	Task
<*name*>	This specifies the IP traffic profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*us-rate* >	This specifies the upstream rate limit for subscriber IP traffic. **Type:** Mandatory **Valid values:** nolimit | 32k | 64k | 128k | 256k | 384k | 512k | 768k
<*ds-rate*>	This specifies the downstream rate limit for subscriber IP traffic. **Type:** Mandatory **Valid values:** 32 ~ 29984 kbps (multiple of 32 kbps)
< *vc-priority* >	This defines the downstream priority, the lower the priority, the higher the chance to get drop due to traffic congestion. **Type:** Mandatory **Valid values:** low | medium | high | highest
<*bcast-filter*>	This defines the downstream broadcast filter of ip-traffic profile. Available on the VLAN ID in which PVC used this ip-traffic. **Type:** Mandatory **Valid values:** drop | forward

Example 41 Add a new IP traffic profile with desired values

```
CLI(config profile ip-traffic)# add Adsl_iptraffic

OK

CLI(config profile ip-traffic)# set Adsl_iptraffic no-limit 128 low forward

OK

CLI(config profile ip-traffic)# show

profile [Adsl_iptraffic]
    index               : 1
    US rate             : no Limit
    DS rate             : 128 (kbps)
    VC priority         : low
    broadcast filter    : forward
```

Configuring the Multicast Service Related Profile

The NE supports to prevent the subscriber to receive un-booked TV channel (multicast channel) by checking the received “IGMP join” packet with a preconfigured Multicast Service Profile. Here, a Multicast Service Profile represents a set of Multicast (TV) Channel Profiles. Each Multicast (TV) Channel Profile describes the attributes of a multicast stream (TV channel). In other words, the subscriber is restriced to receive the TV channels described recorded in the Multicast Service Profile.

This section depicts the concept and configuration of Multicast Service Profileand Multicast Channel Profile.

Multicast Channel Profile Setting

The multicast channel profile sets value of multicast group IP and the associated downstream bandwidth resource, it is a menu list of the Multicast Channel (multicast group; i.e. a TV channel) provided by the Content Service Provider (CSP) or Application Service Provider (ASP).

Enter to the “**config profile mcast**” sub-group directory to manage the multicast channel profile.

```
CLI# config profile mcast
CLI(config profile mcast)#
```

Table 4-8 shows the commands to perform the configuration of multicast channel profile.Example 42 shows the usage of these commands as well as their related parameters.

Table 4-8 Multicast Channel Profile Configuration

The following command is to generate a new multicast group profile.
CLI(config profile mcast)# add <*profile-name*>
The following command is to remove the specific multicast group profile.
CLI(config profile mcast)# del <*profile-name*>
The following command is to activate the specific multicast group profile.
CLI(config profile mcast)# enable <*profile-name*>
The following command is to deactivate the specific multicast group profile.
CLI(config profile mcast)# disable <*profile-name*>
The following command is to modify the profile multicast group member and it desired parameters.
CLI(config profile mcast)# set <*profile-name*> <*group-ip*> <*rate*> {*low* | *medium* | *high* | *highest*}
The following command is to monitor the multicast group profile information.
CLI(config profile mcast)# show [<*profile-name*>]

Parameters	Task
<*profile-name*>	This specifies the multicast channel profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*group-ip*>	Defines class D IP addressing for multicast channel. **Type:** Mandatory **Valid values:** 224.0.1.0 ~ 239.255.255.255 **Default value:** 0.0.0.0 (due to profile generated)
<*rate*>	Defines the downstream transmission limit rate of multicast channel. **Type:** Mandatory **Valid values:** 32~29984 +32 kbps **Default value:** 32 kbps (due to profile generated)
{*low* | *medium* | *high* | *highest*}	Defines the downstream forwarding priority of the associated multicast channel **Type:** Mandatory **Valid values:** low, medium, high, highest **Default value:** low (due to profile generated)

Example 42 Add a new multicast service Profile with desired values

```
CLI(config profile mcast)# add Adsl_ms
OK

CLI(config profile mcast)# set Adsl_ms 224.0.1.1 1024 high
OK

CLI(config profile mcast)# enable Adsl_ms
OK

CLI(config profile mcast)# show

profile [Adsl_ms]
       grouip-ip     rate(kbps)  priority   status
    ---------------  ----------  --------  --------
          224.0.1.1        1024      high   enabled
```

Multicast Service Profile Setting

The multicast service profile is a set of Multicast Channel profiles. Once the Multicast Channel profiles are created, you can generate the multicast service profile to bind suitable Multicast Channel profiles. Each multicast service profile is viewed as a service package for the subscriber to book. The operator then applies the booked multicast service profile to the distinct VC-to-VLAN associated with the subscriber. Please refer to the Section “Configuring a VC-to-VLAN Connection for the VC of RFC2684 Bridged Mode” and Section “Configuring a VC-to-VLAN Connection for the VC of RFC2684 Routed Mode”of Chapter 7 for the related command.

Whenever the subscriber clicks his remote controller to watch a TV channel transmitted via the ADSL line, the set-top-box sends the corresponding IGMP report packet. The NE will forward IGMP packet if its multicast IP hits the associated multicast service profile. Otherwise, the NE drops the IGMP packet. As a result, the subscriber is restricted to watch the TV progrNCT192 that he booked.

Attaching the multicast profile to the proper ADSL line port can be tasked at “**config profile mservice**” sub-group directory, refers to Section “Multicast Service Management”of Chapter 7.

Enter to the “**config profile mservice**” sub-group directory to manage the multicast service profile.

```
CLI# config profile mservice
CLI(config profile mservice)#
```

Table 4-9 shows the commands to perform the configuration of multicast service profile. Example 43 and Example 44 show the usage of these commands as well as their related parameters.

Table 4-9 Multicast Service Profile Configuration

The following command is to generate a new multicast service profile.
CLI(config profile mservice)# add <*service-name*>
The following command is to remove the specific multicast service profile.
CLI(config profile mservice)# del <*service-name*>
The following command is to add the multicast channel profile into specific multicast service profile.
CLI(config profile mservice)# subscribe <*service-name*> <*profile-list*>
The following command is to remove the multicast channel profile from specific multicast service profile.
CLI(config profile mservice)# cancel <*service-name*> <*profile-list*>
The following command is to monitor the multicast service profile information.
CLI(config profile mservice)# show

Parameters	Task
<*service-name*>	This specifies the multicast service profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*profile-list*>	This specifies the multicast group profile name. **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@'). **Format:** xxx or xxx|xxx|…|xxx (xxx indicate as multicast group profile)

Example 43 Create a new multicast channel profile with desired values

```
CLI(config profile mcast)# add HBO
OK

CLI(config profile mcast)# add ESPN
OK

CLI(config profile mcast)# add CNN
OK

CLI(config profile mcast)# set HBO 224.1.1.10 29984 high
OK

CLI(config profile mcast)# set ESPN 224.1.1.11 29984 medium
OK

CLI(config profile mcast)# set CNN 224.1.1.12 29984 highest
OK

CLI(config profile mcast)# show
profile [HBO]
       grouip-ip     rate(kbps)  priority   status
    ----------------  ----------  --------  --------
         224.1.1.10       29984      high  disabled

profile [ESPN]
       grouip-ip     rate(kbps)  priority   status
    ----------------  ----------  --------  --------
         224.1.1.11       29984    medium  disabled

profile [CNN]
       grouip-ip     rate(kbps)  priority   status
    ----------------  ----------  --------  --------
         224.1.1.12       29984   highest  disabled
```

Example 44 Subscribe sets of multicast channel into service profile

```
CLI(config profile mservice)# add program-1
OK

CLI(config profile mservice)# subscribe program-1 HBO|ESPN
OK

CLI(config profile mservice)# add program-2
OK

CLI(config profile mservice)# subscribe program-2 HBO|ESPN|CNN
OK

CLI(config profile mservice)# show

Profile  [program-1]
    Mcast Profile: "HBO", "ESPN",
Profile  [program-2]
    Mcast Profile: "HBO", "ESPN", "CNN",
```

Chapter 5 Managing the Subscriber Interface

This chapter describes the CLI commands to apply the relative profile to Subscriber interface in the following sections:

- Configuring the ADSL Line Port
- Monitoring the ADSL Connection Status
- Configuring the SHDSL Line Port
- Monitoring the SHDSL Connection Status
- Subscriber Interface Administrating

Configuring the ADSL Line Port

This section depcits the CLI commands to apply the following ADSL-related profiles to the ADSL line port in interest.

- ADSL Connection Profile
- ADSL Performance Alarm Profile
- Traffic Policing Profile

This section also depcits the CLI commands to manually perform the power management of the ADSL line port in interest.

On the other hand, the NE allows the operator to specify Agent Remote ID with an ASCII string of up to 63 characters. As to the Agent Circuit ID, it is not permitted to be modified. The format of Agent Circuit ID is as follows.

"NE-InbandIP-userSrcMAC atm slot-port:VPI.VCI"

Here is one example Agent Circuit ID

"IP_DSLAM-100.168.3.97-00:11:d8:80:93:23 atm 3-1:100.33",

which represents

NE's inband IP=100.168.3.97,

MAC address of subscriber's personal computer (or the CPE)= 00:11:d8:80:93:23,

slot = 3, port = 1, vpi = 100, vci = 33.

The xDSL Port Agent ID List keeps the Agent Circuit ID (intended for circuits terminated by the system hosting the Relay agent) and Agent Remote ID (intended to identify the remote host end of a circuit).

xDSL Port Agent ID is to be inserted into either all upstream DHCP messages sent by the client and all upstream PPPoE discovery stage packets

Enter to the "**config port**" sub-group directory to configure the relative profile on the ADSL line port.

```
CLI# config port
CLI(config port)#
```

Table 4-9 shows the commands to perform the configuration of multicast service profile. Example 45 shows the usage of these commands as well as their related parameters.

Table 5-1 ADSL Port Interface Configuration

The following command is to apply the PM alarm profile to specific ADSL line ports.
CLI(config port)# set adsl-alarm-profile <*port-range*> <*profile-name*>
The following command is to apply connection profile to specific ADSL line ports.
CLI(config port)# set adsl-conf-profile <*port-range*> <*profile-name*>
The following command is to force the ADSL2/ADSL2+ power management status. (manual mode only)
CLI(config port)# set adsl-pwr-mgt <*port-range*> <*pwr-state*>
The following command is to apply the traffic policing profile to specific ADSL line ports.
CLI(config port)# set metering <*port-range*> <*profile-name*>
The following command is to apply an "Agent Remote ID" to specific xDSL line port.
CLI(config port)# set remote-id <*port-range*> <*idstring*>
The following command is to remove the remote ID from specific subscriber port.
CLI(config port)# clean remote-id <*port-range*>
The following command is to remove traffic policing profile from specific subscriber port.
CLI(config port)# clean metering <*port-range*>
The following command is to remove the PM alarm profile from specific subscriber port.
CLI(config port)# clean alarm-profile <*port-range*>
The following command is to apply the PM alarm profile to specific SHDSL line port.
CLI(config port)# set shdsl-alarm-profile <*port-range*> <*profile-name*>
The following command is to apply connection profile to specific SHDSL line port.
CLI(config port)# set shdsl-conf-profile <*port-range*> <*profile-name*>
The following command is to view the configuration status of ADSL line port in interest.
CLI(config port)# show <*port-range*>

Parameters	Task
<*port-range*>	Identify the port range of the system to apply the relevance profile of line port. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*profile-name*>	Defines the profile name; connection profile, performance alarm profile or traffic policing profile. **Type:** Mandatory **Valid values:** The name of "connection profile", "performance alarm profile" or "traffic policing profile"
<*pwr-state*>	Defines the ADSL2/ADSL2+ power management operating status, switch between L0, L2 and L3 will only be available if ADSL power management is in "Manual" mode. **Type:** Mandatory **Valid values:** L0, L2,L3
<*idstring*>	Identify the remote ID information which is used for the DHCP option 82 tag and PPPoE tag.

The "Service Type Control" should be enabled when Traffic Policing Profile is assigned to xDSL subscribers (refers to Section "Defining the Line Card Operation Mode" of Chapter 5 for the commands related to the setting of "Service Type Control").

Example 45 Apply the profile to the specify of ADSL line port

```
CLI(config port)# set adsl-conf-profile 1.6 ADSL_P1
```

```
OK

CLI(config port)# set adsl-alarm-profile 1.6 ADSL_PM
OK

CLI(config port)# set remote-id 1.6 1234
OK

CLI(config port)# set metering 1.6 ADSL_TRAF
OK: But LC1 STC is disabled. The traffic policing is not active until STC enabled.

CLI(config port)# show 1.6

Port: 1.6
    admin status            : enabled
    oper status             : up
    ADSL config profile     : "ADSL_P1"
    ADSL alarm profile      : "ADSL_PM"
    SHDSL config profile    : ""
    SHDSL alarm profile     : ""
    traffic policing        : "ADSL_TRAF"
    circuit ID              : "IP_DSLAM-172.17.192.1-00:00:00:00:00:00 atm 1/6:0.0"
    remote ID               : "1234"
```

Monitoring the ADSL Connection Status

The NE supports to display the actual ADSL connection status as follows.

Enter to the "**status**" group directory to monitor the ADSL line Connection status.

```
CLI# status
CLI(status)#
```

Table 5-2 shows the commands to monitor of ADSL connection status. Example 46 shows the usage of these commands as well as their related parameters.

Table 5-2 ADSL Connection Status Monitor

The following command is to view the ADSL line Connection status.	
CLI(status)# port show [*<port-range>*]	
Parameters	**Task**
<port-range>	Identify the port range of the system to view the status of line port. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.

Example 46 Display the ADSL Connection Status

```
CLI(status)# port show 1.6

Port: 1.6
    admin status        : enabled
    oper status         : up
    power state         : L0
    line standard       : G.992.5 Annex A

    [physical status]
              item          US      DS
        ----------------  ------  ------
         attainable rate    1343   30649  kbps
             attenuation     0.0     0.0  dB
```

```
            SNR margin     6.4     8.4  dB
         output power    12.1    12.6  dBm

[channel status]
          item          US      DS
    ----------------  ------  ------
            Tx rate    1342   29204  kbps
    interleave delay      0       0  ms
    CRC block length     39     255  ms
     INP symbol time   0.00    0.00  DMT symbol
```

Configuring the SHDSL Line Port

This section depcits the CLI commands to apply the following SHDSL-related profiles to the SHDSL line port in interest.

- SHDSL Connection Profile
- SHDSL Performance Alarm Profile

Enter to the "**config port**" sub-group directory to configure the relative profile on the SHDSL line port.

```
CLI# config port
CLI(config port)#
```

Table 5-3 shows the commands to configuration of SHDSL port interface.Example 47 shows the usage of these commands as well as their related parameters.

Table 5-3 SHDSL Port Interface Configuration

The following command is to apply the PM alarm profile to specific ADSL line port.
CLI(config port)# set adsl-alarm-profile <*port-range*> < *profile-name* >
The following command is to apply connection profile to specific ADSL line port.
CLI(config port)# set adsl-conf-profile <*port-range*> < *profile-name* >
The following command is to apply the PM alarm profile to specific SHDSL line port.
CLI(config port)# set shdsl-alarm-profile <*port-range*> <*profile-name*>
The following command is to apply connection profile to specific SHDSL line port.
CLI(config port)# set shdsl-conf-profile <*port-range*> <*profile-name*>
The following command is to view the SDSL line port operation status.
CLI(config port)# show [<*port-range*>]

Parameters	Task
<*port-range*>	Identify the port range of the system wish to apply the relevance profile of line port. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*profile-name*>	Defines the profile name; connection profile or performance alarm profile. **Type:** Mandatory **Valid values:** The name of "connection profile" or "performance alarm profile"

Example 47 Display the Configuration of SHDSL Port Interface

```
CLI(config port)# show 4.1
Port: 4.1
    admin status            : enabled
    oper status             : down
```

```
ADSL config profile     : ""
ADSL alarm profile      : ""
SHDSL config profile    : " SHDSL "
SHDSL alarm profile     : " SHDSL_PM "
traffic policing        : "SHDSL_TRAF"
circuit ID              : "IP_DSLAM-172.17.192.1-00:00:00:00:00:00 atm 4/1:0.0"
remote ID               : ""
```

Monitoring the SHDSL Connection Status

The NE supports to display the actual SHDSL connection status as follows.

Enter to the "**status port**" group directory to monitoring the SHDSL line Connection status.

```
CLI# status port
CLI(status port)#
```

Table 5-4 shows the commands to monitor of SHDSL connection status. Example 48 shows the usage of these commands as well as their related parameters.

Table 5-4 SHDSL Connection Status Monitor

The following command is to view the ADSL line Connection status.	
CLI(status port)# show *<port-range>*	
Parameters	**Task**
<port-range>	Identify the port range of the system to view the status of line port. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.

Example 48 Display the SHDSL connection status

```
CLI(status port)# show 2.37
port: 2.37
    admin status        : enabled
    oper status         : up
```

Subscriber Interface Administrating

Enter to the "**config port**" sub-group directory to administrate (enable/disable) the ADSL line port or the SHDSL line port.

```
CLI# config port
CLI(port)#
```

Table 5-5 shows the commands to perform the subscriber service administration. Example 49 shows the usage of these commands as well as their related parameters.

Table 5-5 Subscriber Interface Administration

The following command is to activate the subscriber service of ADSL line port or the SHDSL line port.	
CLI(config port)# enable <*port-range*>	
The following command is to deactivate the subscriber service of ADSL line port or the SHDSL line port.	
CLI(config port)# disable <*port-range*>	
Parameters	**Task**
<*port-range*>	Identify the port range of the system to enable or disable the connection of ADSL line port. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.

Example 49 Administrating the connection of ADSL line port

```
CLI(config port)# enable 1.6
OK

CLI(config port)# show 1.6

Port: 1.6
    admin status            : enabled
    oper status             : up
    ADSL config profile     : "ADSL_P1"
    ADSL alarm profile      : "ADSL_PM"
    SHDSL config profile    : ""
    SHDSL alarm profile     : ""
    traffic policing        : "ADSL_TRAF"
    circuit ID              : "IP_DSLAM-172.17.192.1-00:00:00:00:00:00 atm 1/6:0.0"
    remote ID               : ""        CRC block length       7      15  ms
```

Defining the Line Card Operation Mode

You are allowed to plan the expecting card type address in specific slot; there will have an alarm arise if the planned card type and the actual plug-in card type are mismatch.

The NCT192 support the following functions on a per LC basis.

- Planning the card type of a LC slot
  To ease the operator to plan the usage of each LC slot in advance, the NE support to configure the planned type of a LC slot. There will be an alarm arise if the planned card type and the actual plug-in card type are different.
- RFC 2684 encapsulation method for ADSL line card, either LLC or VCMUX.
- "Service Type Control" for ADSL line card.
  Operator can define the service which allow user to pass, they are "DHCP", "PPPoE" and "Static IP".
- VLAN tag pass-through function for ADSL line card
  Whenever the VLAN tag pass-through (VTP) is configured as enabled, the LC provides transparent transportation of the VLAN traffic from subscriber interface to network interface without any VLAN tag attachment. The LC will not attach any VLAN tag to the upstream subscriber traffic. In the mean time, the LC will also not replace the existing VLAN tag of the upstream subscriber traffic.
  On the other hand, in the case that the VTP function is configured as disabled, the LC will attach a VLAN tag to all the traffic from subscriber interface to network interface.
- IEEE 802.1Q VLAN forwarding function for ADSL line card
  The operator can set the xDSL subscriber ports as well as the GE ports to only forward either tagged traffic or untagged traffic. This section depicts the commands to set the IEEE 802.1Q VLAN forwarding function on the xDSL subscriber ports. As to the setting on the GE ports, please refer to Section "Network Interface Administrating" of Chapter 6 for the

configuration of GE ports to either only forward either tagged traffic or untagged traffic.

Please refer to Section “Verifying Current Software and Hardware Versions” of Chapter 3 for the run-time status of the tagged mode on NC and LC.

It is noted that the run-time status of Tagged mode and VTP on LC may be different to their corresponding configuration. In this case, the behavior of the NE is per the run-time status of NE instead of their configuration. Please refer to Table 6-9 for the expected NE behavior.

The ADSL LC needs to be reset to perform the expected system behavior as depicted in Table 6-9 whenever its run-time status changes.

It is noted that the NE will drop the tagged Ethernet frames of VLAN-ID not configured by the VC-to-VLAN setting (see Table 6-9) in the following case.

NC tagged mode = Tagged
LC tagged mode Run-Time Status = Tagged
LC VTP Run-Time Status = Enabled

The tagged mode (run-time) indicates the operational status of tagged mode.
Tagged-only: LC (or NC) only forwards the tagged Ethernet frame and drops the untagged Ethernet frame.
Untagged-only: LC (or NC) only forwards the untagged Ethernet frame and drops the tagged Ethernet frame.
It is noted that the value of configured Tagged mode and its Run-Time Status may be different. Please refer to Table 6-9 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.

Enter to the “**config lc**” sub-group directory to plan the line card slot.

```
CLI# config lc
CLI(config lc)#
```

Table 5-6 shows the commands to perform the planning of the line card slot. Example 50 shows the usage of these commands as well as their related parameters.

Table 5-6 Plan the Line Card Slot

Use this command to plan the line card type address in specific slot.
CLI(config lc)# set planned-type <*lc-range*> <card-*type*>
Use this command to define the RFC 2684 encapsulation method for specific line card.
CLI(config lc)# set rfc2684-encap <*lc-range*> <encap-*type*>
Use this command to define the Service Type Control function for specific line card.
CLI(config lc)# set service-type <*lc-range*> <*option*>
Use this command to modify the VLAN tag pass-through (VTP) that configured as enables or not. (per LC setting).
CLI(config lc)# set vlan-tag-pass <*lc-id*> <*option*>
Use this command to define the tagged mode in specific slot.
CLI(config lc)# set tagged-mode <*lc-id*> <*mode*>
Use this command to monitor the line card plug-in and planned status.
CLI(config lc)# show

Parameters	Task
<*lc-range*>	Specify the slot range of the system **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.
<*lc-id*>	Specify the specific slot identifier of NE. **Type:** Mandatory **Default values:** 1
<*card-type*>	Specify the planning line card type **Type:** Mandatory **Valid values:** none, adsl, shdsl
<*encap-type*>	Specify the RFC 2684 encapsulation method. **Type:** Mandatory **Valid values:** llc, vc-mux
<*option*>	Specify the VLAN tag pass-through status or Service Type Control, enable or disable. **Type:** Mandatory **Valid values:** enabled | disabled
<*mode*>	Specify the tagged mode is configured as either tagged or untagged mode. **Type:** Mandatory **Valid values:** tagged-only | untagged-only

Example 50 Display the line card type status

```
CLI(config lc)# set planned-type 1 adsl

LC 1. 1: OK

CLI(config lc)# set rfc2684-encap 1 vc-mux

LC1 will be reset. Are you sure? (Y/N) Y
OK

CLI(config lc)# set vlan-tag-pass 1 enabled

OK

CLI(config lc)# set tagged-mode 1 tagged-only
LC1 will be reset. Are you sure? (Y/N) Y
OK

CLI(config lc)# show
```

LC	planned type	current type	rfc2684 encap	vlan-tag pass	service type	configured tagged-mode
1	ADSL	ADSL	VC-MUX	enabled	disabled	tagged-only
2	n/a	n/p	LLC	disabled	disabled	untagged-only
3	n/a	n/p	LLC	disabled	disabled	untagged-only
4	n/a	n/p	LLC	disabled	disabled	untagged-only

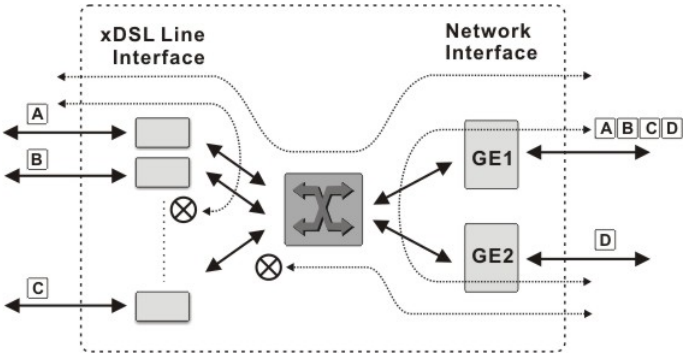
This page is leave in blank for note or memo use

Chapter 6 Managing the Network Interface

There are two GE network interfaces, GE1 and GE2, for NCT192 IP-DSLAM. By default, GE1 is stated as the uplink GE port. GE2 is stated as the subtended GE port, and it connects to other equipment and forward traffics to GE1 if none of LACP or RSTP is enabled.

Figure 6-1shows the packet forwarding diagram. As can be seen, the so-called “Port Isolation” indicates that all xDSL users can not communicate with each other. That is, all traffic from the xDSL line interface is forwarded to the GE1 interface. In the mean time, once the GE2 is configured as a subtended port, all the ingress traffic of GE2 is restricted to be forwarded to GE1.

Figure 6-1 GE Network Interface Packet Forwarding Illustrate



This chapter contains the following sections:

- Configuring the RSTP
- Configuring the Link Aggregation
- Configuring the CoS Traffic Mapping
- Network Interface Administrating
- Defining the NC Card Operation Mode
- Configuring the Subtending
- Configuring the Cascading

Configuring the RSTP

The 802.1D Spanning Tree Protocol (STP) standard was designed at a time when the recovery of connectivity after an outage within a minute or so was considered adequate performance. Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) can be seen as an evolution of the 802.1D standard more than a revolution. The 802.1D terminology remains primarily the same.

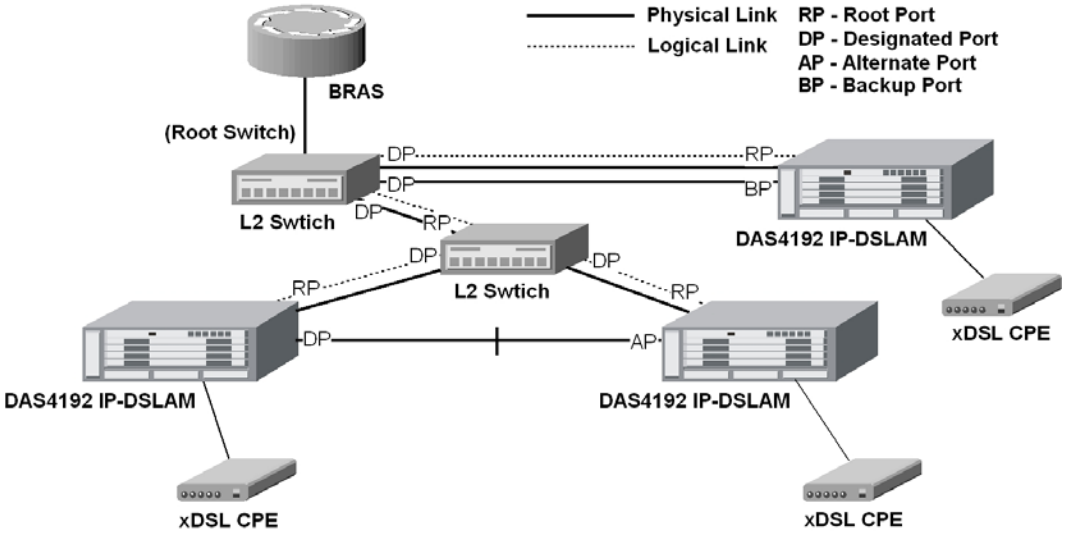
Port Roles and the RSTP Topology

The RSTP selects the bridge with the highest switch priority (lowest numerical priority value) as the root bridge. When the RSTP function of NCT192 IP-DSLAM is enabled, it assigns their network interface to play one of following port-roles. Figure 6-2 shows an example of Rapid Spanning Tree Topology when the RSTP converges.

- Root port – Provides the best path (lowest cost) when the switch forwards packets to the root switch.
- Designated port – Connects to the designated switch, which incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.

- Alternate port – An alternate port is a port blocked by receiving more BPDUs form another bridge.
- Backup port – A backup port is a port blocked by receiving more useful BPDUs from the same bridge which is on.

Figure 6-2 Rapid Spanning Tree Active Topology



The RSTP protocol smartly prevents the loop connection in your uplink networks. It improves the Spanning Tree Protocol (STP) by reducing the fail-over time whenever there is network topology change. The configuration of RSTP is divided into 2 parts. One is the system-wise configuration, which is described in the subsection “Bridge”. The other one is the port-specific configuration, which is described in the subsection “Port GE1/Port GE2”.

Configuring RSTP Bridge Parameters

Enter to the “**config rstp**” sub-group directory to set the RSTP bridge-related parameters.

```
CLI# config rstp
CLI(config rstp)#
```

Table 6-1 shows the commands to perform the configuration of RSTP switch. Example 51 shows the usage of these commands as well as their related parameters.

Table 6-1 RSTP Switch Configuration

The following command is to enable the RSTP function.
CLI(config rstp)# enable
The following command is to disable the RSTP function.
CLI(config rstp)# disable
The following command is to specify the version, RSTP or STP compatible.
CLI(config rstp)# set forceversion <*protocol*>
The following command is to configure the forwarding-delay for all RSTP instance.
CLI(config rstp)# set forwarddelay <*delay-sec*>
The following command is to configure the interval between the generations of configuration messages by the root switch to change the hello time.
CLI(config rstp)# set hellowtime <*hello-sec*>
The following command is to configure the maximum-aging time for all RSTP instance.
CLI(config rstp)# set maxage <*aging-sec*>
The following command is to configure the switch priority and make it more likely that the switch will be chosen as the root switch.
CLI(config rstp)# set priority <*priority-value*>
The following command is to configure the Tx hold count for all RSTP instance.
CLI(config rstp)# set txholdcount <*count*>
The following command is to view the RSTP bridge information.
CLI(config rstp)# show bridge

Parameters	Task
<*protocol*>	This specifies the Network interface to be acting in RSTP mode or STP-Compatible mode. **Valid values:** rstp, stp **Default:** rstp
<*delay-sec*>	This specifies the time value that controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in the Learning states, which precede the Forwarding state. This value is also used, when topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database. **Default:** 15 **Valid values:** 4 ~ 30 (Second)
<*hello-sec*>	The hello time is the interval between the generations of configuration messages by the root switch and specifies the amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so. **Default:** 2 **Valid values:** 1 ~ 10 (Second)
<*aging-sec*>	This specifies the maximum age time (in second) of STP/RSTP information learned from the network on any port before it is discarded. **Default:** 20 **Valid values:** 4 ~ 60 (Second)
<*priority-value*>	Configure the switch priority for an RSTP instance, the range is 0x0000 to 0xF000 in increments of 0x1000. The lower the number, the more likely the switch will be chosen as the root switch. **Default:** 0x8000 **Valid values:** 0x0000 ~ 0xF000 in steps of 0x1000.
<*count*>	This specifies the value used by the port Transmit state machine to limit the maximum transmission rate. **Default:** 3 **Valid values:** 0 ~ 10

It is noted that the following relationships have to be maintained.

2 x (<***delay-sec***> – 1 *second*) >= <***aging-sec***>
<***aging-sec***> ≥ 2 x (<***hello-sec***> + 1 *second*)

Example 51 RSTP switch configuration

```
CLI(config rstp)# set forceversion rstp
OK

CLI(config rstp)# set forwarddelay 10
OK

CLI(config rstp)# set hellotime 5
OK

CLI(config rstp)# set maxage 30
OK

CLI(config rstp)# set priority 0x1000
OK

CLI(config rstp)# set txholdcount 5
OK

CLI(config rstp)# show bridge

[bridge]
    admin status                    : disabled
    force version                   : RSTP
    bridge ID                       : 0x1000-00:60:64:dc:7a:17
    bridge priority                 : 4096
    bridge max age                  : 30 sec
    bridge hello time               : 5 sec
    bridge forward delay            : 10 sec
    bridge Tx hold count            : 5
    root bridge ID                  : 0x8000-00:60:64:dc:7a:17
    root port ID                    : N/A
    root path cost                  : 0
    root max age                    : 20 sec
    root hello time                 : 2 sec
    root forward delay              : 15 sec
    time since last topology change : 0 sec
    topology change count           : 0
```

Configuring RSTP Port GE1/Port GE2 parameters

Enter to the "**config rstp**" sub-group directory to set the RSTP port-related parameters. It is noted that the RSTP port-related parameters apply to the GE1/GE2 ports only, not to the xDSL subscriber ports.

```
CLI# config rstp
CLI(config rstp)#
```

Table 6-2 shows the commands to perform the configuration of RSTP port. Example 52 shows the usage of these commands as well as their related parameters.

Table 6-2 RSTP Port Configuration

The following command is to configure the path cost of port interface.
CLI(config rstp)# set uge cost <*uge-range*> <*cost-value*>
The following command is to disable the STP function of UGE port.
CLI(config rstp)# set uge disable <*uge-range*>
The following command is to configure the edge port instance.
CLI(config rstp)# set uge edge <*uge-range*> {*false* | *true*}
The following command is to enable the STP function of UGE port.
CLI(config rstp)# set uge enable<*uge-range*>
The following command is to migrate the operation of RSTP and STP swap ability.
CLI(config rstp)# set uge mcheck <*uge-range*> {*false* | *true*}
The following command is to configure the point-to-pint instance.
CLI(config rstp)# set uge p2p <*uge-range*> {*true* | *false* | *auto*}
The following command is to configure the port interface priority.
CLI(config rstp)# set uge priority <*uge-range*> <*port-priority*>
The following command is to view the RSTP information on GE Network interface.
CLI(config rstp)# show uge

Parameters	Task
<*uge-value*>	This specifies the Network interface number (UGE port). **Valid values:** 1 (UGE port 1), 2 (UGE port 2)
<*cost-value*>	It specifies the contribution of this port to the path cost of paths towards the spanning tree root bridge. A port of higher speed should be configured with lower numerical value. When set it to be “default”, its value follows the definition of IEEE 802.1d Table 17-3. You can assign lower cost values to interfaces that you want to select first and higher cost values that you want to select last. 0 means automatically calculated default Path Cost value. Default: 20000 Valid values: 0 ~ 200000000
set uge edge < *uge-range* > {*false* | *true*}	Check to let the port become edge port in spanning tree topology. An edge port on an RSTP switch will immediately transition to the forwarding state. However, the port will be a non-edge port if the NE receives RSTP BPDU on that port. And the port state and port role of the non-edge port will be determined by the RSTP hereafter. Default: false Valid values: false, true
set uge mcheck < *uge-range* >	Check to force this port to transmit RSTP BPDUs. **Default:** false
set uge p2p < *uge-range* > {*true* | *false* | *auto*}	This specifies the type of link the RSTP-enaabled port connects. *true:* Indicates to force this port always be treated as if it is connected to a point-to-point link. *false:* Indicates to let this port be treated as having a shared media connection. *auto*: Indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregately, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means. **Default:** auto **Valid values:** true, false, auto
<*port-priority*>	It specifies the port priority of a port. In the case that more than one ports form a loop in the NE, the RSTP/STP will block the ports of lower Port Priority (higher numerical value). Only the port of higher Port Priority (lower numerical value) is to be at the Forwarding state. **Default:** 128 **Valid values:** 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.

When set Path Cost to be “default”, its value follows the definition of IEEE 802.1d Table 17-3 as follows.

Link Speed	Recommended value	Recommended range	Range
<=100 Kb/s	200 000 000[a]	20 000 000–200 000 000	1–200 000 000
1 Mb/s	20 000 000[a]	2 000 000–200 000 000	1–200 000 000
10 Mb/s	2 000 000[a]	200 000–20 000 000	1–200 000 000
100 Mb/s	200 000[a]	20 000–2 000 000	1–200 000 000
1 Gb/s	20 000	2 000–200 000	1–200 000 000
10 Gb/s	2 000	200–20 000	1–200 000 000
100 Gb/s	200	20–2 000	1–200 000 000
1 Tb/s	20	2–200	1–200 000 000
10 Tb/s	2	1–20	1–200 000 000

Example 52 RSTP port Configuration

```
CLI(config rstp)# set uge cost 1 2000
OK

CLI(config rstp)# set uge edge 1 true
OK

CLI(config rstp)# set uge mcheck 1
OK

CLI(config rstp)# set uge priority 1 32
OK

CLI(config rstp)# show uge

[UGE 1]
    STP admin status                : enabled
    port ID                         : 0x2001
    port priority                   : 32
    STP state                       : broken
    admin path cost                 : 2000
    oper path cost                  : 2000
    admin edge port                 : true
    oper edge port                  : true
    admin P2P MAC                   : auto
    oper P2P MAC                    : true

[UGE 2]
    STP admin status                : enabled
    port ID                         : 0x8002
    port priority                   : 128
    STP state                       : broken
    admin path cost                 : 0 (default)
    oper path cost                  : 20000
    admin edge port                 : false
    oper edge port                  : false
    admin P2P MAC                   : auto
    oper P2P MAC                    : true
```

Configuring the Link Aggregation

Link aggregation (LA) is to aggregate the 2 GE ports to form a single logical GE-channel to provide higher uplink bandwidth. This NE supports both static link aggregation and LACP (IEEE802.3ad, Link Aggregation Control Protocol). Figure 6-3 shows a typical GE-channel configuration.

Static link aggregation

In this mode, the NE forces to bundle GE1 and GE2 ports to form a single logical GE-channel without negotiating with its peer L2/L3 switch/router.
For the traffic to be forwarded via the GE-channel as depicted in Figure 6-3, the NE will distribute the traffic on the GE1 and GE2 ports.

When the NE is configured to operate in the static LA mode, its peer L2/L3 switch/router needs to be configured in the same mode. Otherwise, the network may malfunction.

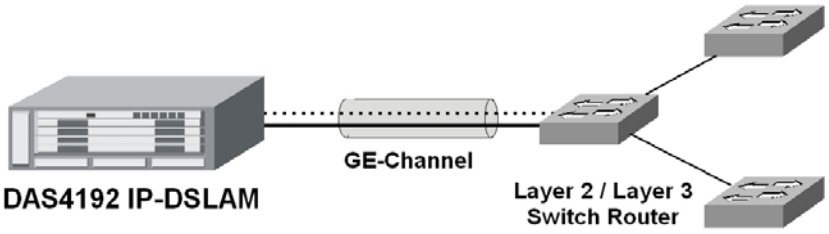
Dynamic link aggregation (LACP)

In this mode, the GE1 and GE2 ports are to form a single logical GE-channel by the LACP negotiating with its peer L2/L3 switch/router. By using the LACP, the NE learns the capability of its LACP peer. It then groups similarly configured ports into a single logical link (GE-channel). Once the GE-channel is built at the end of LACP negotiation, the NE will will forward traffic via the GE-channel by distributing the traffic on the "member port(s)" of GE-channel as depicted in Figure 6-3. Here, the "member port(s)" indicate GE1, GE2 or both GE ports of the NE.

In the LACP, two modes, active and passive modes, are defined for the LACP engine to decide to actively or passively negotiate with its LACP peer for the physical port in interest.

- **Active mode**
  In this mode, The NE is willing to initiate the LACP negotiation procedure on the specified group and sends out an LACP packet voluntarily. The aggregation link will be formed if the other end is running in LACP active or passive mode.
- **Passive mode**
  In this mode, The NE does not initiate LACP negotiation procedure on the specified group voluntarily, but waits for its LACP peer (in active state) initiates negotiation. The NE will form the aggregation link with its peer at the end of the negotiation procedure.

Figure 6-3 Typical GE-Channel Configuration



A LACP enabled switch/router needs to assign its "System ID". The "System ID" is of 8 bytes which consists of 2 parts:
SystemPriority: SystemMacAddress
During the LACP negotiation process, the LACP enabled device of lowest System ID has the previliage to determine the configuration of aggregated ports. Its peer will follow it.

Enter to the "**config la**" sub-group directory to manage the LACP function.

```
CLI# config la
CLI(config la)#
```

Table 6-3 shows the commands to perform the configuration of LACP. Example 53 shows the usage of these commands as well as their related parameters.

Table 6-3 LACP Configuration

The following command is to enable the static link aggregation or LACP.
CLI(config la)# enable <*option*>
The following command is to disable the static link aggregation or LACP.
CLI(config la)# disable
The following command is to configure the LACP group to be active or passive.
CLI(config la)# set group-activity <*group-id*> <*activity*>
The following command is to define the UGE port which the LACP group is.
CLI(config la)# set group-member <*uge-range*> <*group-id*>
The following command is to configure the timeout parameter of the LACP group.
CLI(config la)# set group-timeout <*group-id*> <*timeout*>
The following command is to configure the priority of UGE in LACP.
CLI(config la)# set port-priority <*uge-range*> <*priority*>
The following command is to configure the priority of the system in LACP.
CLI(config la)# set sys-priority <*priority*>
The following command is to view the LACP information.
CLI(config la)# show

Parameters	Task
<*option*>	Configure the aggregation mode to LACP or force to static link aggregation. **Valid values:** lacp | static
<*group-id*>	This indicates the LACP group ID. **Valid values:** 0 | 1
<*uge-range*>	This indicates the UGE port. **Valid values:** 1 | 2
<*timeout*>	It specifies the interval of periodical transmitting LACP BPDU by the peer NE. If the NE does not receive the LACP BPDU after 3 consecutive specified intervals, the NE will remove the port from the aggregation link. For a busy aggregation link, it is recommended to set a short timeout to ensure that a disabled port is removed as soon as possible. Configure the LACP timeout. Timeout = long means that BPDU is sent every 30 seconds. Timeout = short means that BPDU is sent every 1 second. **Valid values:** long | short
<*priority*>	This indicates the LACP port priority or LACP system priority. **Valid values:** 0 ~ 65535 or 0x0000 ~ 0xFFFF

Example 53 LACP Configuration

```
CLI(config la)# set group-activity 1 active
OK

CLI(config la)# set group-member 1 1
OK

CLI(config la)# set group-timeout 1 long
OK

CLI(config la)# set port-priority 1 0x0011
OK

CLI(config la)# show
```

```
Link aggregation state    : disabled
LACP system priority      : 0x8000

LACP group
    group-ID  activity  timeout
    --------  --------  -------
           1   passive     long
           2   passive     long

UGE port state
    UGE-port  LACP-priority  group-ID
    --------  -------------  --------
           1         0x0011         1
           2         0x8000         1
```

Configuring the CoS Traffic Mapping

In order for the NE to play the role of edge (boundary) node of a DiffServ domain, the NE supports the the configurable mapping among the following entities.

- IEEE 802.1p User Priority as configured in the VC-to-VLAN configuration.
- Queue (Traffic Class) on each uplink trunk GE port
- DiffServ Code Point (DSCP) of the IP frame to be forwarded via the uplink trunk GE port.

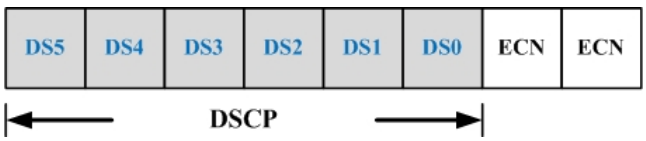
User priority: The IEEE 802.1p user priority is a label carried with the frame that communicates the requested priority to the next hop (bridge, router or end systems). Typically, the user priority is not modified in the intermediate hop. Thus, the user priority has end-to-end significance across bridged LANs.

Queue (traffic class): A bridge can be configured so that multiple queues are used to hold frames waiting to be transmitted on a given outbound port, in which case the traffic class is used to determine the relative priority of the queues. Whenever the bridge's physical port is configured as strict priority (SP), all waiting frames at a higher traffic class are transmitted before any waiting frames of a lower traffic class. As with access priority, traffic class is assigned by the bridge on the basis of incoming user priority.

Currently, the NE supports 8 traffic classes (queues) on its GE ports with the strict priority (SP) scheduling policy only.

Differentiated Service Code Point (DSCP): RFC 2474/2475 defines the DiffServ field, which replaces the Type of Service (ToS) field in the IPv4 header. It facilitates the network devices behind IP-DSLAM to fulfill the end-to-end QoS.
Figure 6-4 shows the DiffServ field.

Figure 6-4 DiffServ Field



The most significant six bits of DiffServ field are called DSCP. The network device classifies packets and marks them with appropriate DSCP value. According to these values, other network devices in the DiffServ domain can make decision for packets behavior and provide the Quality of Service properly.

A network device classify the priorities of traffic with 6 different levels, they are Express

Forwarding (EF), Assured Forwarding Class 4 (AF4), Assured Forwarding Class 3 (AF3), Assured Forwarding Class 2 (AF2), Assured Forwarding Class 1 (AF1) and Best Effort (BE). These forwarding classes are represented by the first 3 bits of DSCP as shown in Table 6-4. Moreover, the network device differentiates three drop precedence in AF4~AF1 respectively into last 3 bits of DSCP, they are Low Drop Precedence, Medium Drop Precedence and High Drop Precedence.

Table 6-4 DSCP: DS3~DS5 Bit Representation

Decimal representation of bits DS5, DS4 and DS3	Description
7	For link layer and routing protocol keep alive.
6	For using for IP routing protocols.
5	Express Forwarding (EF)
4	Assured Forwarding Class 4 (AF4)
3	Assured Forwarding Class 3 (AF3)
2	Assured Forwarding Class 2 (AF2)
1	Assured Forwarding Class 1 (AF1)
0	Best Effort (BF)

Expedited Forwarding: The code point of EF is 101110, the packets marked with EF is to be transmitted with highest priority, lowest drop probability.

Assured Forwarding: Assured Forwarding PHB is suggested for applications that require a better reliability than the best-effort service. There are 4 classes of AF. Within Each AF class, there are 3 drop precedences. In case of congestion, the drop precedence of a packet determines the relative importance of the packet within the AF class. Table 6-5 indicates the relationship of the 4 AF class.

Table 6-5 DSCP Class Relationship

	Class			
Drop	**AF1**	**AF2**	**AF3**	**AF4**
Low Drop Probability	001010 (AF11)	010010 (AF21)	011010 (AF31)	100010 (AF41)
Medium Drop Probability	001100 (AF12)	010100 (AF22)	011100 (AF32)	100100 (AF42)
High Drop Probability	001110 (AF13)	010110 (AF23)	011110 (AF33)	100110 (AF43)

The rest of this section depicts the setting of so called “per hop behavior (PHB)” defined in DiffServ. The setting of PHB is separated in two parts.

- Mapping the 802.1p value to the priority queue of GE port
- Mapping the 802.1p value to the DSCP value

In the definition of PHB defined in DiffServ, it implicates that the Hop (usually a router) needs to classify the received traffic and remark its DSCP accordingly. The classification here indicates either MFC (Multi-Field classification) or DSCP classification. When the NE is at the edge, it should adopt the MFC. Otherwise, it should adopt the DSCP classification.

Then if the physical link is Ethernet, it has to also reassign the 802.1p value to be consistent with the DSCP assignment.

However, as the NE can only support the PVC-based classification, and can only reassign the 802.1p value. We therefore adopt a way different to the formal DiffServ definition.

Mapping the 802.1p value to the priority queue of GE port

Enter to the "**config cos-queue**" sub-group directory to configure the CoS traffic mapping.

```
CLI# config cos-queue
CLI(config cos-queue)#
```

Table 6-6 shows the commands to configure the CoS traffic mapping of NE. 0 shows the usage of these commands as well as their related parameters.

Table 6-6 CoS Traffic Mapping

The following command is to configure the CoS queue mapping between 802.1p priority and system queue index.	
CLI(cos-queue)# mapping *<802_1p> <queue-index>*	
The following command is to viewing the CoS mapping information.	
CLI(cos-queue)# show	
Parameters	**Task**
<802_1p>	This indicates the 802.1p priority for VLAN traffic. **Type:** Mandatory **Valid values:** 0 ~ 7
<queue-index>	The system switch queue index, the higher the number, the higher the forwarding priority. **Type:** Mandatory **Valid values:** 1 ~ 8

Example 54 Set and display the CoS traffic mapping of NE

```
CLI(config cos-queue)# mapping 0 1
OK

CLI(config cos-queue)# show

    802.1p  queue-index
    ------  -----------
         0            1
         1            1
         2            2
         3            4
         4            5
         5            6
         6            7
         7            8
```

Mapping the 802.1p value to the DSCP value

Enter to the "**config diffserv**" sub-group directory to configure the DiffServ function.

```
CLI# config diffserv
CLI(config diffserv)#
```

Table 6-7 shows the commands to configure the differentiated service of NE. Example 55 shows the usage of these commands as well as their related parameters.

Table 6-7 Configuring the DiffServ

The following command is to enable diffserv function.
CLI(config diffserv)# enable
The following command is to disable diffserv function.
CLI(config diffserv)# disable
The following command is to configure the DiffServ action mapping between 802.1p priority and DSCP value.
CLI(config diffserv)# mapping *<802_1p> <dscp>*
The following command is to viewing the diffserv information.
CLI(config diffserv)# show

Parameters	Task
<802_1p>	This indicates the 802.1p priority for VLAN traffic. **Type:** Mandatory **Valid values:** 0 ~ 7
<dscp>	Defines the DSCP value mapping to 802.1p priority. **Type:** Mandatory **Valid values:** BE | AF11 | AF12 | AF13 | AF21 | AF22 | AF23 | AF31 | AF32 | AF33 | AF41 | AF42 | AF43 | EF

Example 55 Set and display the differentiated service of NE

```
CLI(config diffserv)# mapping 0 AF11
OK

CLI(config diffserv)# enable
OK

CLI(config diffserv)# show

DiffServ: enabled
DiffServ 802.1p and DSCP mapping:
    802.1p    :    0     1     2     3     4     5     6     7
      DSCP    : AF11  AF11  AF11  AF21  AF21  AF31  AF31    EF
```

Network Interface Administrating

Enter to the "**config nc**" sub-group directory to manege the GE network interface.

```
CLI# config nc
CLI(config nc)#
```

Table 6-8 shows the commands to perform the network services administration of NE. Example 56 shows the usage of these commands as well as their related parameters.

Table 6-8 Network Interface Administration

The following command is to activate the network service of specific UGE port.
CLI(config nc)# enable <*uge-id*>
The following command is to deactivate the network service of specific UGE port.
CLI(config nc)# disable <*uge-id*>
The following command is to display the UGE interface status.
CLI(config nc)# show

Parameters	Task
<*uge-id*>	This specifies the Network interface number (UGE port). **Valid values:** 1 (UGE port 1), 2 (UGE port 2)

Example 56 Network Services Administration of NE

```
CLI(config nc)# add subtend-vid 100
OK

CLI(config nc)# set planned-type 1 cpu
OK

CLI(config nc)# set autoneg 1 enabled
OK

CLI(config nc)# set tagged-mode untagged-only

This operation will save configuration and reboot system. Are you sure? (Y/N)
Y
Saving...
OK

CLI(config nc)# set subtend enabled
You will enable subtending. Set subtending port VLANs for passing packets.
And you should use IGMP proxy at remote NE. Make sure your IGMP usage.
Are you sure? (Y/N) y
OK

CLI(config nc)# enable 1
OK

CLI(config nc)# show
NC:
    planned-type  current-type   tagged-mode
    ------------  ------------  -------------
              CPU           CPU  untagged-only

UGE:
    UGE  oper-status  admin-status  auto negotiation  use-mode
    ---  -----------  ------------  -----------------  --------
      1         down       enabled            enabled    uplink
```

```
      2         down      disabled          enabled   subtend

Subtend VLAN ID:
     100
```

Defining the NC Card Operation Mode

The NE supports the IEEE 802.1Q VLAN forwarding function. The operator can set the xDSL subscriber ports as well as the GE ports to only forward either tagged traffic or untagged traffic. This section depicts the commands to set the IEEE 802.1Q VLAN forwarding function on GE ports. As to the setting on the xDSL subscriber ports, please refer to Section “Defining the Line Card Operation Mode” of Chapter 5 for the configuration of xDSL subscriber port to either only forward either tagged traffic or untagged traffic on a per-LC basis.

Table 6-9 depicts the NE behavior with the follwoing configurations.

- NC with various Tagged mode parameters.
- ADSL LC with various Tagged mode and VTP parameters.

It is noted that the run-time status of LC may be different to its corresponding configuration. In this case, the behavior of the NE is per the run-time status of NE instead of their configuration. To describe the NE behavior, the following notations are adopted in Table 6-9.

- Q_S represents the service VLAN-tag and its VLAN-ID value is provided by the NE.
- $Q_{S\ (CPE)}$ represents the service VLAN-tag and the notation $_{(CPE)}$ indicates that its VLAN-ID value is provided by the CPE (or the subscriber’s PC behind the CPE).
- $Q_{(CPE)}$ represents the 802.1Q VLAN-tag.
- $Q_{C\ (CPE)}$ represents the customer VLAN-tag and the notation $_{(CPE)}$ indicates that its VLAN-ID value is provided by the CPE (or the subscriber’s PC behind the CPE).

Please refer to Section “Verifying Current Software and Hardware Versions” of Chapter 3 for the run-time status of the tagged mode on NC and LC.

The ADSL LC needs to be reset to perform the expected system behavior as depicted in Table 6-9 whenever its run-time status changes.

The NC needs to be reset to perform the expected system behavior as depicted in Table 6-9 whenever its configured tagged mode changes.

Whenever the GE2 is set as subtended port and the NC is set as “tagged-only” mode, in order to make the NE forward the VLAN-specific traffic between GE1 and GE2, the operator needs to manually set GE1 and GE2 as the member ports of VLANs in interest. Please refer Table 6-9 for the “subtend-vid” related CLI commands.

Table 6-9 The NE behavior when configuring NC and ADSL LC with various Tagged modes and VTP parameters.

NC Setting	ADSL LC setting		ADSL LC Run-Time Status		Expected NE behavior			
					VLAN-tagging Status of Egress Traffic		Acceptable Ingress Traffic	
Tagged mode	Tagged mode	VTP	Tagged mode	VTP	On the GE port	On the ADSL line	On the GE port	On the ADSL line
Tagged	Tagged	Enabled	Tagged	Enabled	$Q_{S\ (CPE)}$	$Q_{(CPE)}$	Tagged	Tagged
		Disabled	Tagged	Disabled	$Q_S+Q_{C\ (CPE)}$	$Q_{(CPE)}$	Tagged	Tagged
	Untagged	Enabled	Untagged	***Disabled***	Q_S	Untagged	Tagged	Untagged
		Disabled	Untagged	Disabled	Q_S	Untagged	Tagged	Untagged
Untagged	Tagged	Enabled	***Untagged***	***Disabled***	Untagged	Untagged	Untagged	Untagged
		Disabled	***Untagged***	Disabled	Untagged	Untagged	Untagged	Untagged
	Untagged	Enabled	Untagged	***Disabled***	Untagged	Untagged	Untagged	Untagged
		Disabled	Untagged	Disabled	Untagged	Untagged	Untagged	Untagged

It is noted that the NE will drop the tagged Ethernet frames of VLAN-ID not configured by the VC-to-VLAN setting (see Table 6-9) in the following case.
NC tagged mode = Tagged
LC tagged mode Run-Time Status = Tagged
LC VTP Run-Time Status = Enabled

The tagged mode (run-time) indicates the operational status of tagged mode.
Tagged-only: LC (or NC) only forwards the tagged Ethernet frame and drops the untagged Ethernet frame.
Untagged-only: LC (or NC) only forwards the untagged Ethernet frame and drops the tagged Ethernet frame.
It is noted that the value of configured Tagged mode and its Run-Time Status may be different. Please refer to Table 6-9 for the NE behavior when configuring NC and ADSL LC with various Tagged mode and VTP parameters.

Enter to the "**config nc**" sub-group directory to manege the GE network interface.

```
CLI# config nc
CLI(config nc)#
```

Table 6-10 shows the commands to perform the network services administration of NE. Example 57 shows the usage of these commands as well as their related parameters.

Table 6-10 Defining the NC Card Operation Mode

Use this command to modify the planning NC card type.
CLI(config nc)# set planned-type <*nc-id*> {*none* | *cpu*}
Use this command to modify the negotiation mode of GE port.
CLI(config nc)# set autoneg <*uge-id*> {*off* | *on*}
Use this command to configure the both of the GE ports to operate either in the "*tagged-only*" or "*untagged-only*" mode.
CLI(config nc)# set tagged-mode { *tagged-only* | *untagged-only*}
Use this command to display the UGE interface status.
CLI(config nc)# show

Parameters	Task
<*nc-id*>	Identify the slot range of the NC card **Type:** Mandatory **Valid values:** 1 ~ 2 (value = 2 does not apply to NCT192)
{*none* | *cpu*}	Identify the NC type.
<*uge-id*>	This specifies the Network interface number (UGE port). **Valid values:** 1 (UGE port 1), 2 (UGE port 2)
{*off* | *on*}	Identify the auto negotiation mode of specified UGE port. **Type:** Mandatory **Valid values:** off | on
{ *tagged-only* | *untagged-only*}	This specifies both of the GE ports to operate either in the "*tagged-only*" or "*untagged-only*" mode. **Type:** Mandatory **Valid values:** tagged-only | untagged-only

The operator needs to add both of the GE ports as member-ports of vlan <*vid*> when the following cases hold.

- GE1 port and GE2 port on NC is configured as tagged-only mode.
- GE2 port is configured as a subtended port. (Section "Configuring the Subtending" of Chapter 6 for the configuration of GE ports to either only forward either tagged traffic or untagged traffic.)

Example 57 Network Services Administration of NE

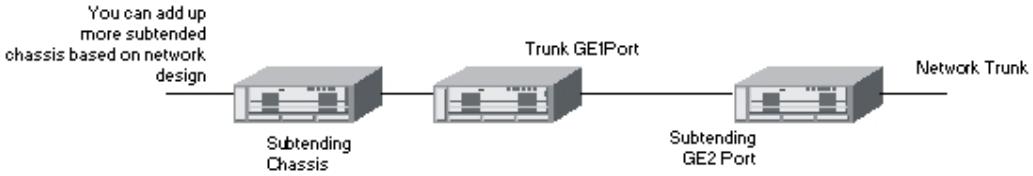
```
CLI(config nc)# add subtend-vid 100
OK

CLI(config nc)# set planned-type 1 cpu
OK

CLI(config nc)# set autoneg 1 enabled
OK

CLI(config nc)# set tagged-mode untagged-only

This operation will save configuration and reboot system. Are you sure? (Y/N)
Y
Saving...
OK

CLI(config nc)# set subtend enabled
You will enable subtending. Set subtending port VLANs for passing packets.
And you should use IGMP proxy at remote NE. Make sure your IGMP usage.
Are you sure? (Y/N) y
OK
```

```
CLI(config nc)# enable 1
OK

CLI(config nc)# show
NC:
    planned-type  current-type   tagged-mode
    ------------  ------------  -------------
             CPU           CPU  untagged-only

UGE:
    UGE  oper-status  admin-status  auto negotiation  use-mode
    ---  -----------  ------------  -----------------  --------
      1         down       enabled            enabled    uplink
      2         down      disabled            enabled   subtend

Subtend VLAN ID:
     100
```

Configuring the Subtending

In some network deployment environment, it is desired to connect several IP-DSLNCT192 to share a single uplink to the access network as shown in Figure 6-5. As can be seen in Figure 6-5, three NCT192 IP-DSLNCT192 are connected via their GE ports to each other in a Daisy-Chain topology. The left-most NE connects to the access network (where the Internet is behind) via its GE1 port (uplink GE port). It also connects to the middle NE via its GE2 port (subtending GE port).

Figure 6-5 Illustration of 3 NCT192 IP-DSLNCT192 are connected in a Daisy-Chain topology



This section depicts the manual VLAN-member port setting procedure of GE1 and GE2. The operator needs to choose the VLAN between 1 and 4094 to apply to GE ports when the following cases hold.

- GE1 port and GE2 port on NC is configured as tagged-only mode.
- GE2 port is configured as a subtended port

Enter to the "**config nc**" group directory to enable the subtending function.

```
CLI# config nc
CLI(config nc)#
```

Table 6-11 shows the commands to perform the configuration of subtending port. 0 shows the usage of these commands as well as their related parameters.

Table 6-11 Subtending Configuration

The following command is to enable, disable, or show the subtend status of system.
CLI(config nc)# set subtend <*option*>
The following command is to set GE2 as a subtendded port (by "*enable*") or an uplink port. (by "*disable*")
CLI(config nc)# set subtend { *disabled* | *enabled*}
The following command is to add both of the GE ports as member-ports of vlan <*vid*>. (See the note at the end of this section to learn the usage of this command.)
CLI(config nc)#add subtend-vid <*vid*>
The following command is to configure both of the GE ports to be not the member-ports of the VLAN specified by <*vid*>.
CLI(config nc)#del subtend-vid <*vid*>
The following command is to configure both of the GE ports to be not the member-ports of any VLAN.
CLI(config nc)#clear subtend-vid

Parameters	Task
{ *disabled* | *enabled*}	Specify the GE2 as either a subtendded port or an uplink port. Enable: GE2 works as a subtend port of the NC Disable: GE2 works as an uplink port of the NC. **Type:** Mandatory **Valid values:** disabled | enabled
<vid>	Identify the vlan id of the VLAN which the GE ports belong to. **Type:** Mandatory **Default value:** 1 **Valid values:** 1 ~ 4093
<*option*>	Configure the subtend function of system. **Valid values:** enable, disable

RSTP and LACP can not work when the subtending function is enabled.

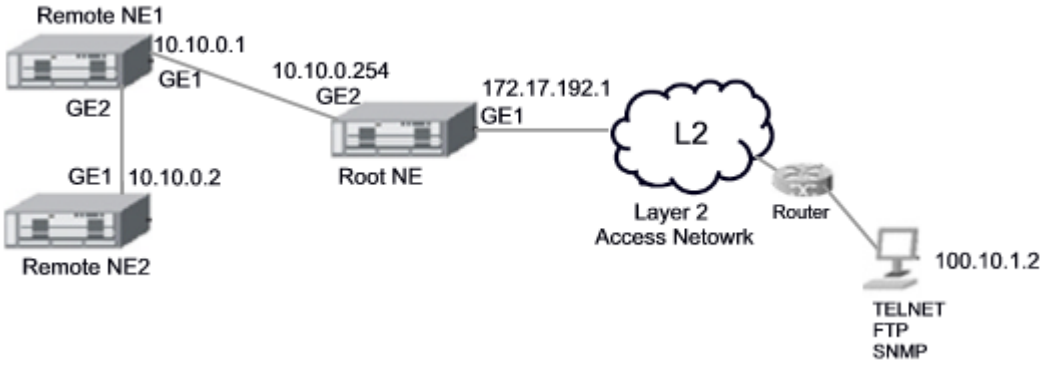
Example 58 The configuration of subtending port

```
CLI(config nc)# set subtend enabled
You will enable subtending.Set subtending port VLANs for passing packets.
And you should use IGMP proxy at remote NE. Make sure your IGMP usage.
Are you sure? (Y/N) y
OK

CLI(config nc)# show

NC:
    planned-type  current-type   tagged-mode
    ------------  ------------  -------------
             CPU           CPU    tagged-only

UGE:
    UGE  oper-status  admin-status  auto negotiation  use-mode
    ---  -----------  ------------  -----------------  --------
      1         down       enabled            enabled    uplink
      2         down      disabled            enabled   subtend

Subtend VLAN ID:
    n/a
```

Configuring the Cascading

In some network deployment environment, it is desired to cascade several IP-DSLNCT192 to share a single uplink as well as the same management IP address to the access network. Hereafter, the NE is said to be connected in a cascading topology when it is deployed in the aforementioned way. And the NE is said to run in the cascade mode. Figure 6-6 depicts a typical cascading topology.

Figure 6-6 Illustration of cascading topology



When the NEs are connected in a cascading topology, the NE plays either one of the following roles.

- Root-NE
  The Root-NE indicates the NE which is directly connected to the L2 access network as shown in Figure 6-6. The Root-NE possesses 2 IP addresses.
  - UGE IP: “UGE IP” is for the communication with the EMS server, LCT and Telnet hosts.
  - root IP: “root IP” is for the communication with the Remote-NE. It is invisible to the network operartor.
- Remote-NE
  The Remote-NE indicates the NE which is is not directly connected to the L2 access network as shown in Figure 6-6. The Remote-NE possesses only one IP address.
  - UGE IP: “UGE IP” is for the communication with the Root-NE.

The following 2 IPs should be the same otherwise, the Root-NE can not communicate with Remote-NE.

- “remote-ne-ip” of the Root-NE
- “UGE IP” of the Remote-NE

In order for the operator to manage the NEs in a cascading topology as shown in Figure 6-6, the operator needs to set them to run in the cascade mode. After appropriate configurations on the Root-NE and Remote-NEs, these NEs will work as a single NE which possesses several shelves via the EMS.

This section depicts the CLI commands to set the NE to run in the cascade mode. Once the Remote-NE is properly set, the operators can manage the remote NEs via the Root-NE by the “clogin” CLI command to login the remote NE.

Enter to the “**config mgt**” group directory to enable the cascade management function.

```
CLI# config mgt
CLI(config mgt)#
```

Table 6-11 shows the commands to perform the configuration of cascaded management. Example 59~Example 60 shows the usage of these commands as well as their related parameters.

Table 6-12 Cascaded Management Configuration

The following command is to enable the cascaded management (single IP management) of the NE.
CLI(config mgt)# cascade enable
The following command is to disable the cascaded management (single IP management) of the NE.
CLI(config mgt)# cascade disable
The following command is to set the role of the NE to be either “Root-NE” or “Remote-NE”
CLI(config mgt)# cascade set role {*root* | *remote*}
The following command is to add a NE into the “Remote-NE-list” of the Root-NE.
CLI(config mgt)# cascade add <*remote-ne-id*> <*remote-ne-ip*> [<*note*>]
The following command is to remove the remote NE from the “Remote-NE-list” of the Root-NE.
CLI(config mgt)# cascade del <*remote-ne-id*>
The following command is to set the user login account and password for the Root-NE to login the remote NE via Telent.
CLI(config mgt)# cascade set remote-account <*remote-ne-id*> <*login-user*> <*login -password*>
The following command is to set the community of the remote NE for the Root-NE to access the Remote-NE via SNMP.
CLI(config mgt)# cascade set remote-community <*remote-ne-id*> <*community-name*>
The following command is to enable/disable the Root-NE to be allowed to access the Remote-NE specified by <*remote-ne-id*>
CLI(config mgt)# cascade set remote-state <*remote-ne-id*> {*disabled* | *enabled*}
The following command is to set the IP address as well as the associated subnet for the Root-NE to communicate with the Remote-NE
CLI(config mgt)# cascade set root-ip <*root-ne-ip*> <*net-mask*>
The following command is to view the status of the cascaded management mode.
CLI(config mgt)# cascade show <*remote-ne-id*>
The following command is to view the status of the cascade connection.
CLI(status)# cascade show
The following command is to access the Remote-NE via Telnet.
CLI# clogin <*remote-ne-id*>

Parameters	Task
<*remote-ne-id*>	This specifies the identified number of remote NE **Type:** Mandatory **Valid values:** 1~2147483647
<*remote-ne-ip*>	This specifies the IP address of the NE to be added into the “Remote-NE-list” of the Root-NE **Type:** Mandatory **Valid values:** Any valid class A/B/C address

Table 6-12 Cascaded Management Configuration (Continued)

Parameters	Task
[<*note*>]	This specifies the note the operator takes for the NE to be added into the "Remote-NE-list" of the Root-NE. **Type:** Mandatory **Valid values:** none
<*login-user*>	This specifies the login user name for the Root-NE to login the remote NE via Telent. **Type:** Mandatory **Valid values:** String of up to 16 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_', '.', '@')
<*login -password*>	This specifies the login user password for the Root-NE to login the remote NE via Telent.. **Type:** Mandatory **Valid values:** String of up to 16 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_', '.', '@')
<*community-name*>	This specifies the community name for the Root-NE to access the remote NE via SNMP. **Type:** Mandatory **Valid values:** String of up to 16 characters ('A' – 'Z', 'a' – 'z', '0' – '9', '-', '_', '.', '@')
<*root-ne-ip*>	This specifies the IP address of the Root-NE for the Root-NE to communicate with the Remote-NE. **Type:** Mandatory **Valid values:** Any valid class A/B/C address
<*net-mask*>	This specifies the subnet mask associated with <*root-ne-ip*> to specifies a subnet where the Remote-NE to resides in **Type:** Mandatory **Valid values:** 255.0.0.0 ~ 255.255.255.255

Th following setting of the Root-NE and Remote-NEs are different.

- "Secured host" of Remote-NE: must be set to be Root-NE.
  "Secured host" of Root-NE: must be set to be LCT, EMS server and so on.
- "SNMP trap station" of Remote-NE: must be set to be Root-NE.
  "SNMP trap station" of Root-NE: must be set to be LCT, EMS server and so on.

Th following setting of the Root-NE and Remote-NEs must be the same.

- "SNMP community" of the read-write privileage.
- <*login-user*> and <*login -password*> of the read-write privileage.
- "tagged mode" of the UGE ports: Either "tagged" or "untagged".
- Management VLAN setting: when the the UGE ports of Root-NE and Remote-NEs are set to be in "tagged" mode.
- The software version of NC.

Whenever the operator establishes a telnet session to access the Root-NE, he/she can use the "clogin" command to establish a telnet session to access Remote-NE. In such situation, he/she has to use the "logout" CLI command to close the telnet session between the Root-NE and Remote-NE before he/she close the telnet session between the host PC and Root-NE. Otherwise, the operator can not "clogin" the Remote-NE anymore.

Hence the following rules should be followed strictly.

- "telnet time-out value between the Root-NE and host PC" should be set to longer than the "telnet time-out value between the Root-NE and Remote-NE".
- Be carefully not to disconnect the "telnet session between the Root-NE and host PC" before disconnect the "telnet session between the Root-NE and Remote-NE".

When deploying NEs to form a cascading topology as shown in Figure 6-7, the IP address of UGE ports of Remote-NE1and Remote-NE2 have to be setup up frist. As can be seen in Figure 6-7, they are set as UGE IP#1 and UGE IP#2, respectively.

On the Root-NE, suppose the operator sets <*remote-ne-ip*> corresponding to Remote-NE1and Remote-NE2 as Remote IP#1 and Remote IP#2, respectively.
In this situation, the operator has to let the following equations hold.

Remote IP#1 = UGE IP#1
Remote IP#2 = UGE IP#2

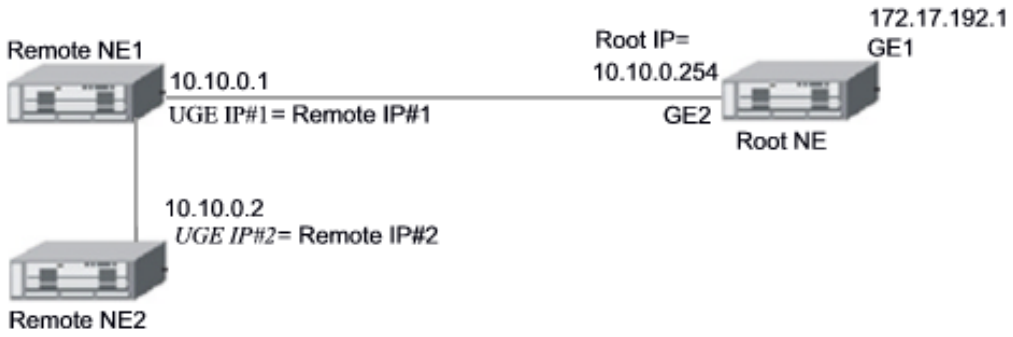
Moreover, the Root IP of Root NE, UGE IP#1 and UGE IP#2, have to be set in the same subnet.

The mini-GBIC and fiber have to be of the same type, either SM or MM.

The LCT does not support to manage the Remote-NE.

The operators can upgrade the firmware of Remote-NE via FTP. (Please refer to the Section “NE Firmware Upgrade in Cascade mode” of Chapter 3)

Figure 6-7 Illustration the IP configuration of NEs in a cascading topology



Example 59 Configuration of NE to play the role of “Root-NE”

```
CLI(config mgt)# cascade set role root
OK.

CLI(config mgt)# cascade set root-ip 10.10.0.254 255.255.255.0
OK

CLI(config mgt)# cascade add 1 10.10.0.1 Remote_NE1
OK

CLI(config mgt)# cascade set remote-account 1 admin admin
OK

CLI(config mgt)# cascade set remote-community 1 netman
OK

CLI(config mgt)# cascade set remote-state 1 enabled
OK

CLI(config mgt)# cascade enable
OK
```

```
CLI(config mgt)# cascade show

[Cascaded management]
    control status            : enabled
    current role              : root
    cascaded root IP          : 10.10.0.254
    cascaded root net mask    : 255.255.255.0

[Remote NE ID: 1]
    IP                : 10.10.0.1
    community         : netman
    account           : admin
    password          : ************
    admin status      : enabled
    note              : Remote_NE1

CLI# config ip show

UGE
    IP address     : 100.168.100.100
    subnet mask    : 255.255.0.0
    MAC address    : 00:60:64:dc:7a:17
    UGE VLAN ID    : 4092

NME
    IP address     : 10.12.3.63
    subnet mask    : 255.255.0.0
    MAC address    : 00:60:64:dc:7a:16

Gateway
    IP address     : 10.12.1.252
```

Example 60 Configuration of NE to play the role of “Remote-NE”

```
CLI# clogin 1

CLI#
       Please type "@.<cr>" to locally close connection
Login:admin
Password:

CLI# config mgt
CLI(config mgt)# cascade set role remote
OK

CLI(config mgt)# cascade enable
OK

CLI(config mgt)# cascade show

[Cascaded management]
    control status            : enabled
    current role              : remote
    cascaded root IP          :
    cascaded root net mask    : 255.255.255.0

CLI# config ip show

UGE
    IP address     : 10.10.0.1
    subnet mask    : 255.255.0.0
    MAC address    : 00:01:03:05:07:09
    UGE VLAN ID    : 4092

NME
```

```
    IP address      : 10.12.3.125
    subnet mask     : 255.255.0.0
    MAC address     : 00:01:55:66:11:22

Gateway
    IP address      : 10.12.1.252
```

Example 61 Monitoring the Cascade Connection Status on the Root-NE

```
CLI(status)# cascade show

[Cascaded management]
    control status            : enabled
    current role              : root
    cascaded root IP          : 10.10.0.254
    cascaded root net mask    : 255.255.255.0

                              admin       oper
remote ID      remote IP      status      status              note
----------  ---------------  --------  -------------  ----------------------------
         1        10.10.0.1   enabled     connected                    Remote_NE1
```

Example 62 Monitoring the Cascade Connection Status on the Remote-NE

```
CLI# clogin 1

CLI#
       Please type "@.<cr>" to locally close connection
Login:admin
Password:

CLI# status cascade show

[Cascaded management]
    control status            : disabled
    current role              : root
    cascaded root IP          : 172.16.1.1
    cascaded root net mask    : 255.255.255.0

CLI# config mgt cascade
CLI(config mgt cascade)# set role remote

OK

CLI(config mgt cascade)# exit
CLI# status cascade show

INFO: This NE is not cascaded root.
```

Chapter 7 Managing the Connection Services

This chapter describes how to manage the system connection services and contains the following sections:

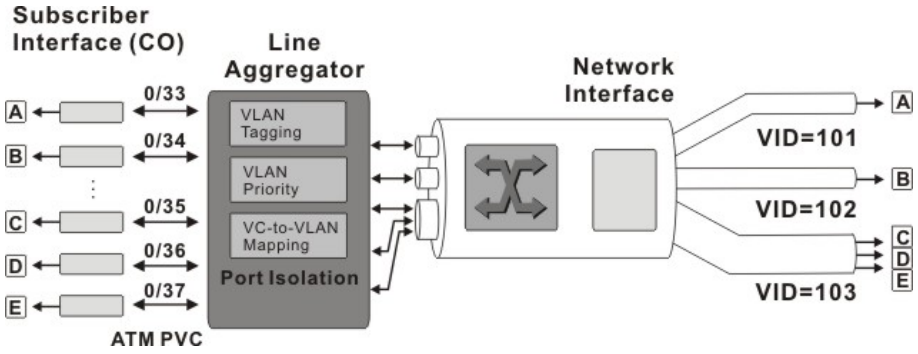
- VC-to-VLAN Connection Management
- Multicast Service Management
- Managing the Subscriber Access Services
- Configuring the Access Control List
- Configuring the System Services

VC-to-VLAN Connection Management

The VC-to-VLAN setting can easily define the multiple to one or one to one mapping; you can group different PVCs to a single VLAN ID as well as single PVC to one VLAN mapping. Figure 7-1 illustrates the basic principle for VLAN assignment in the NCT192 IP-DSLAM. As shown in Figure 7-1, the NE forwards five data flows, A~E, which may be either owned by the same subscriber or by different subscribers. It is noted that these data flows are conveyed in five individual ATM PVCs, and they are grouped into 3 individual VLANs.

NOTE
The NE supports up to 8 PVCs per xDSL port.
The NE supports up to 4094 VLANs per system.

Figure 7-1 VC-to-VLAN Mapping Illustration



According to IETF RFC2684, an IP packet is encapsulated in either bridged mode or routed mode. The VC-to-VLAN settings are similar but not the same in these two encapsulation modes. This section depicts their configuration separately.

NOTE
The VC-to-VLAN configuration procedures are the same to both the ADSL port and SHDSL port.

NOTE
More than one PVCs can be configured in a xDSL port. Each PVC can be configured with different RFC 2684 mode (either RFC 2684 routed mode or RFC 2684 bridged mode). However, the NE supports only one RFC 2684 mode to be enabled for the PVCs in a xDSL port.
Different xDSL ports are allowed to have their PVCs to run with distinct RFC 2684 mode.

Configuring a VC-to-VLAN Connection for the VC of RFC2684 Bridged Mode

In the RFC 2684 bridged mode, the NE needs to perform the following functions for the xDSL subscriber to access the Internet.

- For the upstream traffic
  1. Performs the ATM SAR (Segmentation and Reassembly) function to reassemble the ATM cells to get an ATM AAL5 frame.
  2. Strip off the ATM AAL5 tailer to get the RFC2684-encapsulated Ethernet frame.
  3. Strip off the RFC2684 header to get the Ethernet frame.
  4. Add a VLAN tag (Q_S) to the Ethernet frame if required. (see the definition of "Q_S" in the description of Table 6-9)
  5. Forward the Ethernet frame from the xDSL subscriber to ISP.
- For the downstream traffic
  1. Strip off the VLAN tag (Q_S) from the Ethernet frame if required. (see the definition of "Q_S" in the description of Table 6-9)
  2. Encapsulate the downstream Ethernet frame with RFC2684 header
  3. Append the ATM AAL5 tailer to the RFC2684-encapsulated Ethernet frame to get an ATM AAL5 frame.
  4. Performs the ATM SAR (Segmentation and Reassembly) function to segment the ATM AAL5 frame to get ATM cells.
  5. Forward the Ethernet frame from the ISP to the xDSL subscriber.

Enter to the "**config ucast**" sub-group directory to configure the bridged services of unicast connections.

```
CLI# config ucast
CLI(config ucast)#
```

Table 7-1 shows the commands to perform the configuration of bridged services.Example 63~Example 65 shows the usage of these commands as well as their related parameters.

Table 7-1 Bridged Services Configuration

The following command is to create a new VC-to-VLAN connection on specific of xDSL line port.
CLI(config ucast)# add vcvlan <*port-range*> <*vpi*> <*vci*>
The following command is to remove the VC-to-VLAN connection on specific of xDSL line port.
CLI(config ucast)# del vcvlan <*port-range*> <*vpi*> <*vci*>
The following command is to set the bridged VC-to-VLAN parameters on specific of xDSL line port.
CLI(config ucast)# set vcvlan <*port-range*> <*vpi*> <*vci*> <*802_1p*> <*iptraffic-profile*> **bridged** <*vid*>
The following command is to activate the VC-to-VLAN service on specific of xDSL line port.
CLI(config ucast)# enable vcvlan <*port-range*> <*vpi*> <*vci*>
The following command is to deactivate the VC-to-VLAN service on specific of xDSL line port.
CLI(config ucast)# disable vcvlan <*port-range*> <*vpi*> <*vci*>
The following command is to set the FDB (filtering Database) non-aged mode on specific PVCs.
CLI(config ucast)# set fdb-non-aged <*port-range*> <*vpi*> <*vci*> <*option*>

Table 7-1 Bridged Services Configuration (continued)

The following command is to display the FDB (filtering Database) non-aged mode on specific PVCs.
CLI(config ucast)# show fdb-non-aged [<*port-range*>]
The following command is to change the MAC limit on specific of xDSL line ports.
CLI(config ucast)# set mac-limit <*port-range*> <*vpi*> <*vci*> <*pvc-mac-limit*>
The following command is to display the MAC limit on specific of xDSL line ports.
CLI(config ucast)# show mac-limit [<*port-range*>]
The following command is to display the VC-VLAN connection on specific of xDSL line ports.
CLI(config ucast)# show vcvlan [<*port-range*>]

Parameters	Task
<*port-range*>	Identify the port range of the system wish to configure in bridged services. **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.
<*vpi*>	Defines the VPI (Virtual Path Identifier) value. **Type:** Mandatory **Valid values:** 0 ~ 255
<*vci*>	Defines the VCI (Virtual Channel Identifier) value. **Type:** Mandatory **Valid values:** 1 ~ 65535 (1 ~ 31 are reserved)
<*802_1p*>	Defines the tagging of VLAN 802.1p priority of egress switch fabric on specific of VC-to-VLAN connection. **Type:** Mandatory **Default value:** 0 **Valid values:** 0 ~ 7 (low ~ high)
<*iptraffic-profile*>	Defines the IP traffic profile name. (See the Section “Configuring the IP Traffic Profile” of Chapter 4) **Type:** Mandatory **Valid values:** The name of “ip traffic profile”
<*vid*>	Defines the VLAN ID to be assign on specific of VC-to-VLAN connection. **Type:** Mandatory **Default value:** 1 **Valid values:** 1 ~ 4093
<*pvc-mac-limit*>	Defines the limit of MAC address learning from specific bridged service per xDSL line port. Each xDSL line port allow maximum of 8 MAC address learning in total of VC-to-VLAN usage. **Type:** Mandatory **Default value:** 1 **Valid values:** 1 ~ 8
<*option*>	Enable or disable the FDB (filtering Database) non-aged mode on specific PVCs. **Valid values:** enable: to let the MAC entries dynamically learned from the specific PVCs never be aged. disable:to let the MAC entries learned from the specific PVCs be aged as in normally FDB aging process.

Example 63 Bridged Services Configuration of NE

```
CLI(config ucast)# add vcvlan 1.6 8 35
OK

CLI(config ucast)# set vcvlan 1.6 8 35 0 ADSL_TRAF bridged 100
OK

CLI(config ucast)# enable vcvlan 1.6 8 35
OK

CLI(config ucast)# show vcvlan 1.6
```

```
port ID  VPI/VCI     IP-traffic    VLAN 1p MAC RFC2684  next-hop   admin   oper
-------- --------- ---------------- ---- -- --- -------- ---------- --------- -----
   1. 6   8/   35        ADSL_TRAF  100  0   1 bridged             enabled   up
```

Example 64 Bridged FDB Non-Aged Mode Configuration of NE

```
CLI(config ucast)# set fdb-non-aged 1.6 8 35  enabled
OK

CLI(config ucast)# show fdb-non-aged 1.6
port ID   VPI/VCI   non-aged
--------  ---------  ---------
   1. 6    8/   35   enabled
```

Example 65 Bridged MAC Limit Configuration of NE

```
CLI(config ucast)# set mac-limit 1.6 8 35 8
OK

CLI(config ucast)# show mac-limit 1.6

port ID   VPI/VCI   mac-limit
--------  ---------  ----------
   1. 6    8/   35          8
```

In the RFC 2684 bridged mode, the NE supports to IP counts <= MAC limit per PVC of xDSL port.

Configuring a VC-to-VLAN Connection for the VC of RFC2684 Routed Mode

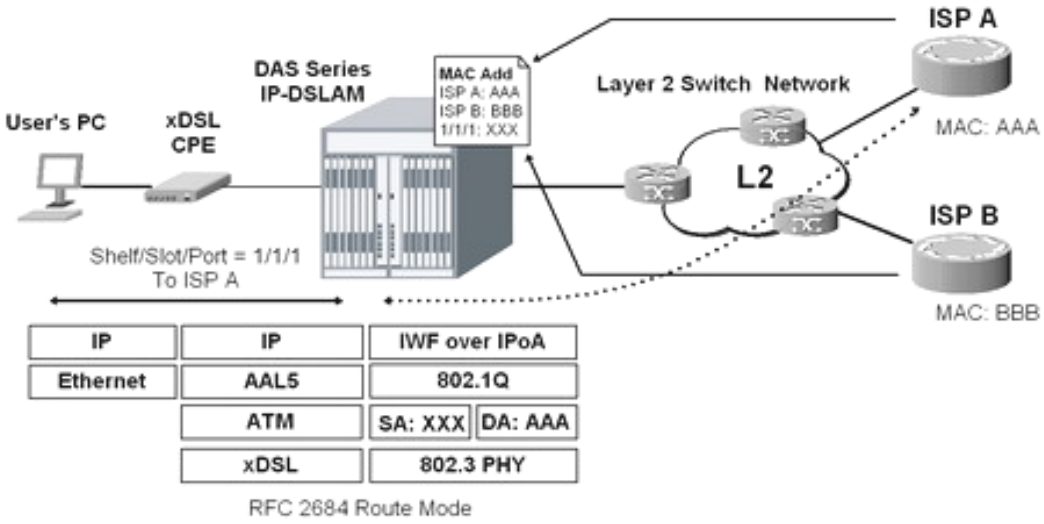
In the RFC 2684 routed mode, the NE needs to perform the following functions for the xDSL subscriber to access the Internet.

- For the upstream traffic
  1. Performs the ATM SAR (Segmentation and Reassembly) function to reassemble the ATM cells to get an ATM AAL5 frame.
  2. Strip off the ATM AAL5 tailer to get the RFC2684-encapsulated IP packet.
  3. Strip off the RFC2684 header to get the IP packet.
  4. Prefix an Ethernet header to the IP packet. The prefixed Ethernet header is of the following setting.
     Destination MAC = the MAC of Next-hop router toward the ISP's router.
     Source MAC = an unique MAC generated by the NE.
  5. Add a VLAN tag (Q_S) to the Ethernet frame if required. (see the definition of "Q_S" in the description of Table 6-9)
  6. Forward the Ethernet frame from the xDSL subscriber to ISP.
- For the downstream traffic
  1. Strip off the VLAN tag (Q_S) from the Ethernet frame if required. (see the definition of "Q_S" in the description of Table 6-9)
  2. Strip off the Ethernet header from the IP packet.
  3. Encapsulate the downstream IP packet with RFC2684 header
  4. Append the ATM AAL5 tailer to the RFC2684-encapsulated Ethernet frame to get an ATM AAL5 frame.
  5. Performs the ATM SAR (Segmentation and Reassembly) function to segment the ATM AAL5 frame to get ATM cells.
  6. Forward the Ethernet frame from the ISP to the xDSL subscriber.

In the RFC 2684 routed mode, IP packets are directly encapsulated, i.e., no MAC layer is presented. Through the IWF (Inter-Work Function) of IPoA of IP-DSLAM, it needs to prefix the Ethernet MAC layer for particular subscriber interface. The source MAC address is specially generated by IP-DSLAM, and the destination MAC address is the next-hop router toward the ISP's router. The NE determines the MAC address of next-hop router by the (Address Resolution Protocol (ARP).

Figure 7-2 illustrates an example of the IWF in the case of RFC 2684 routed mode.

Figure 7-2 RFC 2684 Route Mode Connection Method



When you set the IP of "Next Hop", the NE will send ARP to query the MAC of the "Next Hop". When the MAC you observe is 00:00:00:00:00:00, it indicates something wrong such that the NE can not get the MAC of the Next-Hop router via ARP.

Enter to the "**config ucast**" sub-group directory to configure the routed services of unicast connection.

```
CLI# config unast
CLI(config ucast)#
```

Table 7-2 shows the commands to perform the configuration of routed services. Example 66 shows the usage of these commands as well as their related parameters.

Table 7-2 Routed Services Configuration

The following command is to create a new VC-to-VLAN connection on specific of xDSL line port.
CLI(config ucast)# add vcvlan <*port-range*> <*vpi*> <*vci*>
The following command is to create a new ISP (Internet Service Provider) connection.
CLI(config ucast)# add nexthop <*ispname*> <*ip-addr*><*vid*>
The following command is to remove the VC-to-VLAN connection on specific of xDSL line port.
CLI(config ucast)# del vcvlan <*port-range*> <*vpi*> <*vci*>
The following command is to remove the ISP connection.
CLI(config ucast)# del nexthop <*ispname*>
The following command is to activate the VC-to-VLAN service on specific of xDSL line port.
CLI(config ucast)# enable vcvlan <*port-range*> <*vpi*> <*vci*>
The following command is to deactivate the VC-to-VLAN service on specific of xDSL line port.
CLI(config ucast)# disable vcvlan <*port-range*> <*vpi*> <*vci*>
The following command is to change the routed VC-to-VLAN parameters on specific of xDSL line port.
CLI(config ucast)# set vcvlan <*port-range*> <*vpi*> <*vci*> <*802_1p*> <*iptraffic-profile*> **routed** <*ispname*>

Parameters	Task
<*port-range*>	Identify the port range of the system wish to configure in routed services. **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.
<*vpi*>	Defines the VPI (Virtual Path Identifier) value. **Type:** Mandatory **Valid values:** 0 ~ 255
<*vci*>	Defines the VCI (Virtual Channel Identifier) value. **Type:** Mandatory **Valid values:** 1 ~ 65535 (1 ~ 31 are reserved when VPI equal 0)
<*ispname*>	Defines the ISP name for routed service. **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
<*ip-addr*>	Defines IP address of the ISP server. **Type:** Mandatory **Valid values:** 0.0.0.0 ~ 255.255.255.255
<*vid*>	Defines the VLAN ID to be assign on specific of VC-to-VLAN connection. **Type:** Mandatory **Default value:** 1 **Valid values:** 1 ~ 4093
<*802_1p*>	Defines the tagging of VLAN 802.1p priority of egress switch fabric on specific of VC-to-VLAN connection. **Type:** Mandatory **Default value:** 0 **Valid values:** 0 ~ 7 (low ~ high)
<*iptraffic-profile*>	Defines the created IP traffic profile name. **Type:** Mandatory **Valid values:** The name of “ip traffic profile”

Example 66 Configure the routed services of NE (Jack_Changed->Revision)

```
CLI(config ucast)# add nexthop PC1 192.168.192.63 100
OK

CLI(config ucast)# add vcvlan 1.37 8 35
OK
```

```
CLI(config ucast)# set vcvlan 1.37 8 35 0 ADSL_TRAF routed PC1
OK

CLI(config ucast)# enable vcvlan  1.37 8 35
OK

CLI(config ucast)# show vcvlan 1.37

port ID  VPI/VCI     IP-traffic    VLAN 1p MAC RFC2684  next-hop   admin   oper
------- --------- ---------------- ---- -- --- -------- ---------- --------- -----
 1   37   8   35       ADSL_TRAF   100  0   1 bridged        PC1  enabled   up
```

Monitoring the VC-to-VLAN Connection Status

Enter to the "**config ucast**" sub-group directory to monitoring the unicast connection status.

```
CLI# config ucast
CLI(config ucast)#
```

Table 7-3 shows the commands to perform the unicast connection status of NE. Example 67 shows the usage of these commands as well as their related parameters.

Table 7-3 Unicast Connection Status Monitor

The following command is to view the VC-to-VLAN connection of specific xDSL line port.
CLI(config ucast)# show vcvlan [<*port-range*>]
The following command is to view the status of ISP server use for routed services.
CLI(config ucast)# show nexthop
The following command is to view the launched service type of specific xDSL line port.
CLI(config ucast)# show servicetype [<*port-range*>]
The following command is to view the various error code to identify the PVC errors.
CLI(config ucast)# show error-code <*code-value*>

Parameters	Task
<*port-range*>	Identify the port range of the system wish to view the VC-to-VLAN connection. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*code-value*>	Identify the PVC error code to form with '0xNNNNNNNN' where N is the hex between 0 to f. **Type:** Mandatory **Valid values:** 0x00000000-0xffffffff.

Example 67 Displaying the unicast connection status

```
CLI(config ucast)# show vcvlan 1.6

port ID  VPI/VCI     IP-traffic    VLAN 1p MAC RFC2684  next-hop   admin   oper
------- --------- ---------------- ---- -- --- -------- ---------- --------- -----
   1. 6   8/   35        ADSL_TRAF  100  0   1 bridged              enabled   up

CLI(config ucast)# show nexthop

         next-hop name              next-hop IP          MAC         VLAN  status
-------------------------------- ---------------- ----------------- ---- ---------
                             PC1  192.168.63.100 00:18:f3:91:99:50  100 inactive

CLI(config ucast)# show servicetype 1.6
```

```
 port           RFC2684   STC      runtime     configured       base        IP
  ID   VPI/VCI    mode   status  service-type service-type   IP address    count
----- --------- ------- -------- ------------ ------------ --------------- -----
 1. 6   8/   35 bridged disabled  pure-bridge         DHCP         0.0.0.0     1
```

Example 68 Displaying the various error code to identify the PVC errors

```
CLI(config ucast)# show error-code  0x000000F

Bit 0: PVC is nonexistent.
Bit 1: PVC has enabled.
Bit 2: PVC values are not changed.

CLI(config ucast)# show error-code  0x0000EEE

Bit 1: PVC has enabled.
Bit 2: PVC values are not changed.
Bit 4: Number of enabled VPI/VCI pair variety on this LC is maximum(32).
Bit 5: PVC amount on this port has reached maximum(8).
Bit 6: Sum of enabled PVC and MCAU on port has reached maximum(8).
Bit 8: No IP traffic profile is assigned on this PVC.
Bit 9: On this bridged PVC, service type IP amount is greater than MAC limit.
Bit10: On this routed PVC, service type IP amount is greater than 8.
```

Multicast Service Management

Whenever the subscriber clicks his remote controller to watch a TV channel transmitted via the ADSL line, the set-top-box sends the corresponding IGMP report packet. The NE will forward IGMP packet if its multicast IP hits the associated multicast service profile. Otherwise, the NE drops the IGMP packet. As a result, the subscriber is restricted to watch the TV progrNCT192 that he booked.

To provide multicast service, the operator needs to properly configure the multicast channel and IGMP snooping /IGMP proxy. This section contains the following two subsections.

- Configuring Multicast Channel
- IGMP Snooping/Proxy Setting

Configuring Multicast Channel

The NE supports to prevent the subscriber to receive un-booked TV channel (multicast channel) by checking the received “IGMP join” packet with a preconfigured Multicast Service Profile. (A Multicast Service Profile consists of a number of Multicast Channel Profiles.) The subscriber is restriced to receive the TV channels (recorded in the Multicast Channel Profile).

This sub-section depicts the CLI commands to associate the ADSL subscriber with the created Multicast Service Profiles.

Refer for the CLI commands to create Multicast Channel Profiles and Multicast Service Profiles in Section “Configuring the Multicast Service Related Profile” of Chapter 4.

Enter to the “**config mcau**” sub-group directory to configure the multicast connection.

```
CLI# config mcau
CLI(config mcau)#
```

Table 7-4 shows the commands to perform the multicast connection status of NE. Example 69 shows the usage of these commands as well as their related parameters.

Table 7-4 Multicast Services Configuration

The following command is to remove the multicast service on specific of xDSL line port.
CLI(config mcau)# del <*port-range*>
The following command is to activate the multicast service on specific of xDSL line port.
CLI(config mcau)# enable <*port-range*>
The following command is to deactivate the multicast service on specific of xDSL line port.
CLI(config mcau)# disable <*port-range*>
The following command is to change the multicast service with desired parameters on specific of xDSL line port.
CLI(config mcau)# set <*port-range*> <*vpi*> <*vci*> <*vlan-id*> <*channel-limit*> <*mservice-name*>
The following command is to show the multicast service with desired parameters on specific of xDSL line port.
CLI(config mcau)# show [<*port-range*>]

Parameters	Task
<*port-range*>	Identify the port range of the system wish to configure in multicast services. **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.
<*vpi*>	Defines the VPI (Virtual Path Identifier) value. **Type:** Mandatory **Default value:** 8 **Valid values:** 0 ~ 255
<*vci*>	Defines the VCI (Virtual Channel Identifier) value. **Type:** Mandatory **Default value:** 35 **Valid values:** 1 ~ 65535 (1 ~ 31 are reserved)
<*channel-limit*>	Defines the limit of concurrent multicast channel transmission on specific of VC-to-VLAN connection. **Type:** Mandatory **Default value:** 1 **Valid values:** 1 ~ 5
<*vlan-id*>	Defines the VLAN ID to be assign to a multicast VLAN **Type:** Mandatory **Default value:** 1 **Valid values:** 1 ~ 4093
<*mservice-name*>	This specifies the multicast service profile name **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').

Example 69 Display the multicast connection status

```
CLI(config mcau)# set 1.6 8 35 100 1 program_1
OK

CLI(config mcau)# enable 1.6
OK

CLI(config mcau)# show 1.6

                          channel
port ID   VPI/VCI   VLAN  limit          service-profile            status
-------  ---------  ----  -----  ---------------------------------  --------
   1. 6    8/   35   100      1                          program_1   enabled
```

IGMP Snooping/Proxy Setting

The NE supports IGMP snooping and IGMP proxy as follows.

- IGMP snooping:
  When the IGMP snooping function is enabled,
  1. The NE starts to "listen in" IGMP conversations between hosts and routers.
  2. Once the NE hears an "IGMP join" message on an xDSL interface, it checks the associated Multicast Service Profile to prevent the subscriber to receive un-booked TV channels (multicast channel).
  3. If the multicast group IP of the received "IGMP join" message "hits" the Multicast Service Profile, the NE adds that xDSL interface to the corresponding multicast forwarding table and forwards this "IGMP join" message out of the GE port.
     Otherwise, the NE drops the "IGMP join" message.
  4. As the NE hears an "IGMP leave" message or the 'snooping aging-time' expires, the NE will remove that xDSL interface from the corresponding multicast forwarding table.
- IGMP proxy:
  When the IGMP proxy function is enabled,
  1. The NE starts to "listen in" IGMP conversations between hosts and routers.
  2. Once it recieves an "IGMP join" message from the subscribers, it checks the associated Multicast Service Profile to prevent the subscriber to receive un-booked TV channels (multicast channel).
  3. If the multicast group IP of the received "IGMP join" message "hits" the Multicast Service Profile, the NE adds that xDSL interface to the corresponding multicast forwarding table. And the NE further checks if it already forwards the TV channel requested by this "IGMP join" message. If the answer is YES, the NE drops this "IGMP join" message. Otherwise, the NE sends an "IGMP join" message to request that TV channel via the GE port.
     If the multicast group IP of the received "IGMP join" message "misses" the Multicast Service Profile, the NE drops the "IGMP join" message.
  4. As the NE receives an "IGMP leave" message or the 'response-time' expires, the NE will remove that xDSL interface from the corresponding multicast forwarding table.

Follow the commands to configure the IGMP snooping or proxy function.

Enter to the "**config igmp**" sub-group directory to configure the related parameters.

```
CLI# config igmp
CLI(config igmp)#
```

Table 7-5 shows the commands to set the IGMP snooping and proxy functions of NE. Example 70 shows the usage of these commands as well as their related parameters.

Table 7-5 IGMP Snooping/Proxy Setting

The following command is to activate the IGMP snooping or proxy function for multicast services.
CLI(config igmp)# enable <*igmp-mode*>
The following command is to deactivate both the IGMP snooping and proxy function for multicast services.
CLI(config igmp)# disable
The following command is to enable the IGMP proxy to perform “immediated-leave” function or not. (see the note below)
CLI(config igmp)# proxy set immediated-leave <*option*>
The following command is to configure the IGMP proxy response time against the subscriber link.
CLI(config igmp)# proxy set response-interval <*interval*>
The following command is to configure the IGMP proxy retry counter.
CLI(config igmp)# proxy set retries <*times*>
The following command is to enable the IGMP snooping to perform “immediated-leave” function or not. (see the note below)
CLI(config igmp)# snooping set immediated-leave <*option*>
The following command is to configure the IGMP snooping response time against the subscriber link.
CLI(config igmp)# snooping set response-interval <*interval*>
The following command is to configure the IGMP snooping retry counter.
CLI(config igmp)# snooping set retries <*times*>
The following command is to configure the aging time of IGMP Snooping.
CLI(config igmp)# snooping set aging-time <*sec*>
The following command is to configure the stateful mode of IGMP packets.
CLI(config igmp)# set stateful <*level*>
The following command is to viewing the IGMP status.
CLI(config igmp)# show
The following command is to set the IGMP version for query.
CLI(config igmp)# version query <*version-type*>
The following command is to set the IGMP version for report and leave.
CLI(config igmp)# version report-leavel < *version-type* >

Table 7-5 IGMP Snooping/Proxy Setting (Continued)

Parameters	Task
<igmp-mode>	Define the IGMP mode for multicast services **Type:** Mandatory **Valid values:** proxy | snooping
<option>	Enable the IGMP snooping or proxy to perform "immediated-leave" function or not **Type:** Mandatory **Valid values:** disabled | enabled
<sec>	Defines the IGMP snooping aging time in second. **Type:** Mandatory **Valid values:** 30 ~ 3600 (sec.) **Default value:** 300 (sec.)
<interval>	Defines the time period waiting for subscriber response the IGMP message. **Type:** Mandatory **Valid values:** 1 ~ 30 (sec.) **Default value:** 30 (sec.)
<times>	Defines the retry counting for STB response the IGMP message, if the system did not receive IGMP message from subscriber edge, system will treat as 'leave' hence will stop the multicast stream to the particular link. **Type:** Mandatory **Valid values:** 1 ~ 5 **Default value:** 3 (count.)
<level>	Define the print out mode when system receives IGMP packets. **Type:** Mandatory **Valid values:** none | flow | msg None – show nothing Flow – show flow state only Msg – show packet flag and error message
< version-type >	Define the IGMP version type for the NE to launch/relay the IGMP query, report and leave message. **Type:** Mandatory **Valid values:** v2 | v3 | auto v2 – Indicate to force the NE to launch the IGMP packets of version 2 no matter what version of IGMP packet it receives v3 –Indicate to force the NE to launch the IGMP packets of version 3 no matter what version of IGMP packet it receives auto –Indicate to launch/relay the IGMP packets of version the same as the version of IGMP packet it receives.

- If "Immediate Leave" is enabled:
  The NE will stop forwarding the multicast stream once it receives the corresponding IGMP "leave" packet. That is, the TV image should be "freezed" immediately
- If " Immediate Leave" is disabled:
  The NE will react on the received IGMP "leave" packet and start the "leave" process as follows.
  1. The NE will re-send the "IGMP query" packet 'Robustness (Query Retry)' times if it does not receive "IGMP join".
  2. The time interval between 2 consecutive "IGMP query" packets is 'Query Response Interval' seconds.
  3. During the of "leave" process, if the NE receives the corresponding "IGMP join" packet, it continues to forward the multicast stream and stops the "leave" process.
  4. At the end of "leave" process, the NE will stop forwarding the multicast stream if it does not receive any "IGMP join" packet.

Example 70 Configure the IGMP proxy and display its status

```
CLI(config igmp)# proxy set immediate-leave enabled
OK

CLI(config igmp)# proxy set response-interval 300
```

```
OK

CLI(config igmp)# proxy set retrials 3
OK

CLI(config igmp)# enable proxy
OK

CLI(config igmp)# show

IGMP proxy
    status                  : enabled
    immediate leave         : enabled
    retrials                : 3
    response interval       : 300   in 1/10 sec

IGMP snooping
    status                  : disabled
    immediate leave         : enabled
    aging time              : 30   sec
    retrials                : 2
    response interval       : 100   in 1/10 sec

IGMP version
    query version           : v2
    report/leave version    : auto

Stateful
    level                   : none - show nothing
```

Example 71 Configure the IGMP snooping and display its status

```
CLI(config igmp)# snooping set immediate-leave enabled
OK

CLI(config igmp)# snooping set response-interval 300
OK

CLI(config igmp)# snooping set retrials 3
OK

CLI(config igmp)# snooping set aging-time 30
OK

CLI(config igmp)# set stateful flow
OK

CLI(config igmp)# enable snooping
OK

CLI(config igmp)# show

IGMP proxy
    status                  : disabled
    immediate leave         : enabled
    retrials                : 3
    response interval       : 300   in 1/10 sec

IGMP snooping
    status                  : enabled
    immediate leave         : enabled
    aging time              : 30   sec
    retrials                : 3
    response interval       : 300   in 1/10 sec

IGMP version
    query version           : v2
```

```
    report/leave version    : auto

Stateful
    level                   : flow - show flow state only
```

Example 72 Configure the IGMP version for query, report and leave

```
CLI(config igmp)# version query v2
OK

CLI(config igmp)# version report-leave v3
OK

CLI(config igmp)# show
IGMP proxy
    status                  : disabled
    immediate leave         : disabled
    retrials                : 3
    response interval       : 30   in 1/10 sec

IGMP snooping
    status                  : enabled
    immediate leave         : enabled
    aging time              : 30   sec
    retrials                : 2
    response interval       : 100   in 1/10 sec

IGMP version
    query version           : v2
    report/leave version    : v3

Stateful
    level                   : none - show nothing
```

Monitoring the IGMP Snoopy/Proxy Information

Enter to the "**status igmp**" sub-group directory to display the IGMP snoop and proxy information with associated xDSL line port.

```
CLI# status igmp
CLI(status igmp)#
```

Table 7-6 shows the commands to set the IGMP snooping and proxy information of NE. Example 73 shows the usage of these commands as well as their related parameters.

Table 7-6 Viewing IGMP Proxy Information

The following command is to view the IGMP group (IP) with associated xDSL line port.	
CLI(status igmp)# group show [*<group-ip>*]	
The following command is to show IGMP member information on this port.	
CLI(status igmp)# member show *<port-id>*	
Parameters	**Task**
<group-ip>	Defines class D IP addressing for multicast channel **Type:** Mandatory **Valid values:** 224.0.1.0 ~ 239.255.255.255
<port-id>	Identify the port ID of the system line card **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.

Example 73 Display the IGMP snooping/proxy information

```
CLI(status igmp)# group show

Current IGMP: IGMP Snooping

Group IP [234.5.1.1]
    group MAC         : 01:00:5e:05:01:01
    last reporter     : 10.10.10.10
    up time           : 00:00:00:50
    last port         : 1.37
    member counter    : 1
    member port       :

        slot [ 1]: 37
        slot [ 2]: none
        slot [ 3]: none
        slot [ 4]: none
        uge      : none


CLI(status igmp)# member show 1.37

Current IGMP: IGMP Snooping
    port-ID     group-IP      state
    -------  ---------------  ------
       1.37        234.5.1.1  active
```

Managing the Subscriber Access Services

The system supports the so-called “service type control” function to restrict the type of traffic to be forwarded on the PVC of individual subscriber.

- In RFC2684 routed mode, the following service type is supported.
  - Static IP
- In RFC2684 bridged mode, the following three service types are supported.
  - PPPoE
  - DHCP
  - Static IP

Enter to the “**config ucast**” sub-group directory to manage the access service control.

```
CLI# config ucast
CLI(config ucast)#
```

Table 7-7 shows the commands to perform the access services configuration of NE. Example 74 shows the usage of these commands as well as their related parameters.

Table 7-7 Access Services Configuration

The following command is to define the access service of particular PVC.
CLI(config ucast)# set servicetype *<port-range> <vpi> <vci> <mode>*
The following command is to define the authentic IP in static IP access mode.
CLI(config ucast)# set servicetypestaticip *<port-range> <vpi> <vci> <staticipbase> <iplimit>*
The following command is to view the access service status in specific Subscriber port interface.
CLI(config ucast)# show servicetype *<port-range>*

Parameters	Task
<port-range>	Identify the port range of the system line card **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<vpi>	Defines the VPI (Virtual Path Identifier) value. **Type:** Mandatory **Valid values:** 0 ~ 255
<vci>	Defines the VCI (Virtual Channel Identifier) value. **Type:** Mandatory **Valid values:** 1 ~ 65535 (1 ~ 31 are reserved)
<staticipbase>	This specifies the base of the IP address if the service type is Static IP **Type:** Mandatory **Valid values:** Any valid class A/B/C address **Default value:** None
<iplimit>	This specifies the maximum IP counter when the service type is either "DHCP" or "Static IP". **Type:** Mandatory **Valid values:** 1 ~ 8
<mode>	This specifies the authentic of access service mode in particular PVC. **Type:** Mandatory **Valid values:** pppoe, dhcp, static ip

Example 74 Configure the static IP access service

```
CLI(config ucast)# set servicetypestaticip 1.6 8 35 192.168.1.1 1
OK

CLI(config ucast)# set servicetype 1.6 8 35 staticip
OK

CLI(config ucast)# show servicetype 1.6

 port           RFC2684   STC      runtime     configured       base         IP
  ID   VPI/VCI    mode   status  service-type service-type   IP address    count
----- --------- ------- -------- ------------ ------------ ---------------- -----
 1. 6   8/   35 bridged disabled  pure-bridge    static-IP     192.168.1.1     1
```

The CLI commands in this section take effect only when the **service-type** setting of ADSL LC is enabled. Please refer to Table 5-6 for the related commands.

Enabling the Service Type Control makes the NE to provide the IP/MAC anti spoofing function.

- **In the case that the subscriber acquires his IP address dynamically via PPPoE**
  The NE will block the subscriber's traffic before a valid IP address assignment. Once the subscriber possesses a valid dynamic IP, the NE will just forward the packet of valid source MAC addresses. In other words, the NE drops the subscriber's traffic of invalid source MAC addresses
- **In the case that the subscriber acquires his IP address dynamically via DHCP**
  The NE will block the subscriber's traffic before a valid IP address assignment. Once the subscriber possesses a valid dynamic IP, the NE will just forward the packet of valid source IP/MAC addresses. In other words, the NE drops the subscriber's traffic of invalid source IP/MAC addresses.
- **In the case that the subscriber possesses static IP address**
  The NE will just forward the packet of valid source IP/MAC addresses. In other words, the NE drops the subscriber's traffic of invalid source IP/MAC addresses.

Configuring the Access Control List

This section describes the configurations of the following 2 kinds of Access Control List (ACL).

- Source MAC Access Control List
- Filtering the NetBIOS and NetBEUI

Source MAC Access Control List

The NE supports the VC-to-VLAN ACL function is to provide the operator a tool to manually deny/permit the ADSL subscriber's upstream Ethernet frame according to their source MAC addresses.

For example, if there are duplicate MAC addresses from two or more individual xDSL subscriber ports, the operator should deny the hacker's traffic and permit the good guy's traffic. With the VC-to-VLAN ACL function, the operator can manually set to permit (forward) one of them and deny the rest traffic. (or via the CLI commands depicts in Section "Filtering the Upstream Traffic of Spoofed MAC" of Chapter 7)

The VC-to-VLAN ACL function is to apply to the specified PVC on the ADSL line only.

The roles of access control function, Deny and Permit, are repulsive, i.e. a "deny" role will be replaced while a new role "permit" is be configured.

Enter to the "**config fdb**" sub-group directory to manage the ACL statement.

```
CLI# config fdb
CLI(config fdb)#
```

Table 7-8 shows the commands to configure the access control list of NE. Example 75 shows the usage of these commands as well as their related parameters.

Table 7-8 Access Control List Configuration

The following command is to add the ACL permission of the specified MAC addresses on specified xDSL line port.
CLI(config fdb)# add acl <*port-id*> <*vpi*> <*vci*> <*mac-addr*> <*mode*>
The following command is to remove the specified MAC addresses of specified xDSL line port.
CLI(config fdb)# del <*port-id*> <*vpi*> <*vci*> <*mac-addr*>
The following command is to display the FDB entries on specified xDSL line ports
CLI(config fdb)# show [<*port-range*>]

Parameters	Task
<*port-range*>	Identify the port range of the system wish to configure in bridged services. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*port-id*>	Identify the port id of the system wish to display current list of learning MAC addresses from their remote network. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*vpi*>	Defines the VPI (Virtual Path Identifier) value. **Type:** Mandatory **Valid values:** 0 ~ 255
<*vci*>	Defines the VCI (Virtual Channel Identifier) value. **Type:** Mandatory **Valid values:** 1 ~ 65535 (1 ~ 31 are reserved)
<*mac-addr*>	Indicate the target MAC address. **Type:** Mandatory **Valid values:** Valid MAC addresses form. (for example: 00:1F:AA:19:78:03)
<*mode*>	Defines the ACL action of specific MAC address in the PVC connection. Permit or deny the specific MAC addresses of xDSL line port where addresses are learned. **Type:** Mandatory **Valid values:** permit, deny

Example 75 Configure the access control list

```
CLI(config fdb)# add acl 1.6 8 35 00:60:64:dc:7a:15 permit
OK

CLI(config fdb)# show 1.6

port ID   VPI/VCI      MAC address     VLAN  type
-------  ---------  ------------------  ----  ----
   1. 6    8/   35  00:60:64:dc:7a:15   100    AP
```

Filtering the NetBIOS and NetBEUI

The NE allows the operator to configure to forward or drop the name server protocol (NetBIOS and NetBEUI) traffics received on the subscriber interfaces and network interfaces.

Enter to the "**config filter**" sub-group directory to define the NetBIOS and NetBEUI filtering function.

```
CLI# config filter
CLI(config filter)#
```

Table 7-9 shows the commands to filter the NetBIOS and NetBEUI packets. Example 76 shows the usage of these commands as well as their related parameters.

Table 7-9 NetBIOS and NetBEUI Filter

The following command is to define the action NetBIOS and NetBEUI filtering.	
CLI(config filter)# netbios *<netbios-action>*	
The following command is to display current setting of NetBIOS and NetBRUI filtering.	
CLI(config filter)# show	
Parameters	**Task**
<netbios-action>	Identify the NetBIOS and NetBEUI filtering action. **Type:** Mandatory **Valid values:** drop, forward

Example 76 NetBIOS and NetBEUI Filtering

```
CLI(config filter)# netbios drop
OK

CLI(config filter)# show

NetBIOS filter action: drop
```

Configuring the System Services

This section describes the configurations of the following System Services.

- DHCP Broadcast Control
- DHCP Relay Setting
- DHCP Relay Option 82 Setting
- Configuring the PPPoE Suboption
- Configuring the VLAN MAC Limitation
- Configuring MAC Aging for Bridged Services
- Monitoring the VLAN Member Set
- Filtering the Upstream Traffic of Spoofed MAC
- Monitoring the Subscriber MAC

DHCP Broadcast Control

Users can set the DHCP broadcast packet rate limit and set the action to be applied to the out-of-profile traffic on a per-NE basis.

Enter to the "**config dhcp**" sub-group directory to configure the DHCP broadcast control.

```
CLI# config dhcp
CLI(config dhcp)#
```

Table 7-10 shows the commands to perform the DHCP broadcast control. Example 77 shows the usage of these commands as well as their related parameters.

Table 7-10 DHCP Broadcast Control

The following command is to define the action to the DHCP packets which exceed the specified <*rate-limit*>.
CLI(config dhcp)# set bc <*rate-limit*> <*action*>
The following command is to disable the DHCP broadcast control
CLI(config dhcp)# disable bc
The following command is to enable the DHCP broadcast control
CLI(config dhcp)# enable bc
The following command is to display the DHCP broadcast control information
CLI(config dhcp)# show

Parameters	Task
<*action*>	Defines the action to be applied to the DHCP broadcast packets which exceed the specified <*rate-limit*>. **Type:** Mandatory **Valid values:** none, drop, alarm, both none – do nothing drop – drop DHCP broadcast packets alarm – send alarm to the configured trap host (NCT192 LCT or NCT192 EMS Server) both– drop DHCP broadcast packets and send alarm **Default value:** none
<rate-*limit*>	Defines the rate limit of DHCP broadcast packets **Type:** Mandatory **Valid values:** 1 ~ 100000 (pkts/sec.) **Default value:** 100 (pkts/sec.)

When the action is set to be either “alarm” and “Drop packet and send alarm”, the NE will launch SNMP traps to the SNMP trap managers as specified in the Section “Configuring the IP Address of SNMP Trap Station” of Chapter 3.

Example 77 Configure the DHCP broadcast control

```
CLI(config dhcp)# set bc 1000 both
OK

CLI(config dhcp)# enable bc
OK

CLI(config dhcp)# show

    DHCP option82                : disabled
    broadcast control            : enabled
        rate limit               : 1000 pkts/sec
        action over rate limit   : both (drop & alarm)
    stateful level               : none - show nothing
    DHCP relay                   : disabled
    relay server                 : no server exists
```

DHCP Relay Setting

The DHCP relay intercepts the DHCP request packets from subscriber interface and forwards them to the specified DHCP server. In the opposite direction, the DHCP relay transfers the DHCP reply packets from DHCP server to the specified xDSL subscriber.

Enter to the “**config dhcp**” sub-group directory to configure the DHCP relay.

```
CLI# config dhcp
CLI(config dhcp)#
```

Table 7-11 shows the commands to perform the DHCP relay server configuration. Example 78 shows the usage of these commands as well as their related parameters.

Table 7-11 DHCP Relay Setting

The following command is to define the DHCP relay server and its correspondent VLAN ID.
CLI(config dhcp)# add relay-server <*server-ip*>
The following command is to remove the DHCP relay server IP
CLI(config dhcp)# del relay-server <*server-ip*>
The following command is to enable the DHCP relay functionality.
CLI(config dhcp)# enable relay
The following command is to disable the DHCP relay functionality.
CLI(config dhcp)# disable relay
The following command is to configure the stateful mode of DHCP packets.
CLI(config dhcp)# set stateful <*level*>
The following command is to view the DHCP relay status.
CLI(config dhcp)# show

Parameters	Task
<*server-ip*>	This specifies the IP address of DHCP server. **Type:** Mandatory **Valid values:** Any valid class A/B/C address **Default value:** None
<*level* >	Define the print out mode when system receives DHCP packets. **Type:** Mandatory **Valid values:** none | flow | pf | all None – show nothing Flow – show flow state only Pf – show packet content and flow state All – all content with hexadecimal data

Example 78 Set the DHCP relay server

```
CLI(config dhcp)# add relay-server 192.168.192.1
OK

CLI(config dhcp)# enable relay
OK

CLI(config dhcp)# set stateful flow
OK

CLI(config dhcp)# show

option82                    : disabled
broadcast control           : enabled
broadcast rate limit        : 1000 pkts/sec
broadcast action            : both (drop & alarm)
stateful level              : flow - show flow state only
relay                       : enabled
relay server 1              : 192.168.192.56
relay server 2              : 192.168.192.1
```

DHCP Relay Option 82 Setting

Enter to the "**config dhcp**" sub-group directory to configure the DHCP relay option 82.

```
CLI# config dhcp
CLI(config dhcp)#
```

Table 7-12 shows the commands to perform the DHCP Relay Option 82 configuration. Example 79 shows the usage of these commands as well as their related parameters.

Table 7-12 DHCP Relay Option 82 Setting

The following command is to enable the DHCP relay option 82 functionality.
CLI(config dhcp)# enable op82
The following command is to disable the DHCP relay option 82 functionality.
CLI(config dhcp)# disable op82

Example 79 Configure the DHCP Relay Option 82

```
CLI(config dhcp)# enable op82

OK

CLI(config dhcp)# show

option82                    : enabled
broadcast control           : disabled
broadcast rate limit        : 100 pkts/sec
broadcast action            : both (drop & alarm)
stateful level              : none - show nothing
relay                       : disabled
relay server                : no server exists
```

The setting of DHCP option 82 contents is performed by configuring the xDSL Port Agent ID. (See the Section "Configuring the ADSL Line Port" of Chapter 5)

Configuring the PPPoE Suboption

PPPoE sub-option has similar mechanism as DHCP option 82. The NE can insert Circuit ID and Remote ID in all upstream PPPoE packets in the PPPoE discovery stage, i.e. the PADI, PADR and upstream PADT packets.

The setting of PPPoE sub-option contents is performed by configuring the xDSL Port Agent ID

Enter to the "**config pppoe**" sub-group directory to configure the PPPoE suboption.

```
CLI# config pppoe
CLI(config pppoe)#
```

Table 7-13 shows the commands to perform the PPPoE suboption configuration. Example 80 shows the usage of these commands as well as their related parameters.

Table 7-13 PPPoE Suboption Setting

The following command is to enable the PPPoE suboption function.
CLI(config pppoe)# enable suboption
The following command is to disable the PPPoE suboption function.
CLI(config pppoe)# disable suboption
The following command is to configure the stateful mode of PPPoE packets.
CLI(config pppoe)# set stateful *<level>*
The following command is to display the PPPoE suboption and stateful information.
CLI(config pppoe)# show

Parameters	Task
<level>	Define the print out mode when system receives PPPoE packets. **Type:** Mandatory **Valid values:** none | flow | msg none – show nothing flow – show flow state only msg – show flow message

Example 80 Configure the PPPoE suboption

```
CLI(config pppoe)# set stateful flow
OK

CLI(config pppoe)# enable suboption
OK

CLI(config pppoe)# show

suboption         : enabled
stateful level    : flow
```

Configuring the VLAN MAC Limitation

To limit the number of source MAC address learned in a specific VLAN, the users can enable the MAC limiting function and configure the upper limit of allowed MAC for a specific VLAN.

Enter to the "**config vlan-mac-limit**" sub-group directory to manage the VLAN MAC limitation.

```
CLI# config vlan-mac-limit
CLI(config vlan-mac-limit)#
```

Table 7-14 shows the commands to perform the VLAN MAC limiting configuration. Example 81 shows the usage of these commands as well as their related parameters.

Table 7-14 VLAN MAC Limiting Configuration

The following command is to enable or disable the MAC limiting of specific VLAN ID.
CLI(config vlan-mac-limit)# set <*vid*> <*option*>
The following command is to define the MAC number of specific VLAN ID.
CLI(config vlan-mac-limit)# set <*vid*> <*maclimit*>
The following command is to display the status of VLAN MAC limiting.
CLI(config vlan-mac-limit)# show <*vid*>

Parameters	Task
<*vid*>	This specifies the VLAN ID of system. **Type:** Mandatory **Valid values:** 1 ~ 4094
<*option*>	This enable/disable the VLAN MAC limiting function of specific VLAN ID. **Type:** Mandatory **Valid values:** enabled | disabled
<*maclimit*>	This defines the MAC number of specific VLAN ID to be accept **Type:** Mandatory **Valid values:** 1 ~ 1536 **Default values:** 1536

Example 81 Configure the VLAN MAC limiting

```
CLI(config vlan-mac-limit)# set 100 43
OK

CLI(config vlan-mac-limit)# set 100 on
OK

CLI(config vlan-mac-limit)# show 100

    VID [ 100]
        MAC Limit : 43
        MAC Limit Control: enabled
```

Configuring MAC Aging for Bridged Services

The MAC aging time sets the lifetime for the learned MAC address. A specific MAC address will be dropped when aging out until it is learned by the NE again.

Enter to the "**config bridge**" sub-group directory to configure the system bridging and monitor its status.

```
CLI# config bridge
CLI(config bridge)#
```

Table 7-15 shows the commands to perform the MAC aging for bridged services. Example 82 shows the usage of these commands as well as their related parameters.

Table 7-15 Bridged Services Setting

The following command is to configure the bridging service aging time.
CLI(config bridge)# set aging-time <*sec*>
The following command is to view the bridging aging time status.
CLI(config bridge)# show

Parameters	Task
<*sec*>	Defines the bridging aging time in second. **Type:** Mandatory **Valid values:** 10 ~ 1000 (sec.) **Default value:** 300 (sec.)

Example 82 Display the bridging status

```
CLI(config bridge)# set aging-time 300
OK

CLI(config bridge)# show
MAC aging time: 5 min 0 sec (300 sec)
```

Monitoring the VLAN Member Set

Enter to the "**status vlan**" sub-group directory to display
- the VLAN member set of a specified VLAN.
- the VLANs which the GE port is a member port of.

```
CLI# status vlan
CLI(status vlan)#
```

Table 7-16 shows the commands to show the Subscriber VLAN Group configuration. Example 83 shows the usage of these commands as well as their related parameters.

Table 7-16 Viewing Subscriber VLAN Group

Use this command to viewing the xDSL line ports which are the VLAN member ports of a specified VLAN
CLI(status vlan)# show vlan-id <*vid*>
Use this command to view VLANs which the GE port is a member port of
CLI(status vlan)# show uge <*uge-id*>

Parameters	Task
<*vid*>	This specifies the VLAN ID of correspond xDSL line port. **Type:** Mandatory **Valid values:** 1~ 4094
<*uge-id*>	This specifies the uge id of correspond xDSL line port. **Type:** Mandatory **Valid values:** 1~2

Example 83 Display the subscriber VLAN group

```
CLI(status vlan)# show vlan-id 100

VLAN [100] egress ports

    LC 1: 6,21
```

```
    LC 2:
    LC 3:
    LC 4:
    UGE : 1, 2

CLI(status vlan)# show uge 1
Use mode: uplink

VLAN ID:
     100, 4092
```

Configuring Static MAC

The NE supports the operator to add the “static” MAC addresses to specified xDSL line port manually. In comparison with the the MAC addresses learned from the associate ATM VC, the manually added “static” MAC addresses are never aged out.

Enter to the “**config fdb**” sub-group directory to add the static MAC entry to the FDB associated with the specified ATM PVC (i.e., the so-called “PVC_FDB”).

```
CLI# config fdb
CLI(config fdb)#
```

Table 7-17 shows the commands to add the static MAC entry to the PVC_FDB. Example 84 shows the usage of these commands as well as their related parameters.

Table 7-17 Configuring a static MAC entry in PVC_FDB

The following command is to add the static MAC addresses of specified ATM PVC of an xDSL line port.	
CLI(config fdb)# add static <*port-id*> <*vpi*> <*vci*> <*mac-addr*>	
The following command is to remove the static MAC addresses of specified ATM PVC of an xDSL line port.	
CLI(config fdb)# del <*port-id*> <*vpi*> <*vci*> <*mac-addr*>	
The following command is to display the FDB entries on specified xDSL line ports	
CLI(config fdb)# show [<*port-range*>]	
Parameters	**Task**
<*port-range*>	Identify the xDSL port range of FDB to show. **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.
<*port-id*>	Identify the xDSL port id of the system to add/delete static MAC to **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.
<*vpi*>	Defines the VPI (Virtual Path Identifier) value. **Type:** Mandatory **Valid values:** 0 ~ 255
<*vci*>	Defines the VCI (Virtual Channel Identifier) value. **Type:** Mandatory **Valid values:** 1 ~ 65535 (1 ~ 31 are reserved)
<*mac-addr*>	Indicate the static MAC address to be added. **Type:** Mandatory **Valid values:** Valid MAC addresses form. (for example: 00:1F:AA:19:78:03)

Example 84 Adding a static MAC addresses to specified ATM PVC of an xDSL line port.

```
CLI(config fdb)# add static 1.6 8 35 00:00:00:00:00:11
```

```
OK

CLI(config fdb)# show

port ID   VPI/VCI      MAC address     VLAN  type
-------  ---------  ------------------  ----  ----
   1. 6    8/   35  00:00:00:00:00:11   100     S
```

Filtering the Upstream Traffic of Spoofed MAC

The FDB (filtering Database) of NCT192 system stored the MAC addresses learning from the associate ATM VC at bridged mode. The NE supports to prevent forwarding the upstream traffic of duplicated MAC address from xDSL subscribers as they may be maybe opportunist or hacker

When the NE learns two or more duplicated MAC addresses from xDSL subscribers's side learned at the same time, the NE's default action is to **allow the first MAC address and block all the others.** However, the illegal user's MAC address may be learned firstly. To provide the operator a tool to cure the aforementioned situation, the NE supports to manually change the default action.

Enter to the "**config fdb**" sub-group directory to configure learning MAC addresses from the associate ATM VC.

```
CLI# config fdb
CLI(config fdb)#
```

Table 7-24 shows the commands to configure the VC MAC Learning Table. Example 85~Example 86 shows the usage of these commands as well as their related parameters.

Table 7-18 Configuring the action to the upstream traffic of spoofed MAC

The following command is to permit the upstream traffic of spoofed MAC address on the specified xDSL port.	
CLI(config fdb)# set spoofed <*port-id*> <*mac-addr*> permit	
The following command is to drop all the upstream traffic of spoofed MAC addresses.	
CLI(config fdb)# set spoofed <*mac-addr*> deny-all	
The following command is to display the FDB entries on specified xDSL line ports	
CLI(config fdb)# show [<*port-range*>]	
Parameters	**Task**
<*port-range*>	Identify the xDSL port range of FDB to show. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*port-id*>	Identify the xDSL port id of the system to set the action to the upstream traffic of spoofed MAC address **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*mac-addr*>	Indicate the spoofed MAC address. **Type:** Mandatory **Valid values:** Valid MAC addresses form. (for example: 00:1F:AA:19:78:03)

Example 85 Permitting the upstream traffic of spoofed MAC address on the specified xDSL port.

```
CLI(status fdb)# show spoofed

   MAC address      port     VPI/VCI   VLAN  status
------------------  -------  ---------  ----  ------
```

```
00:00:00:00:00:11     1. 6    8/   35     0     LSA
                      1.23    8/   35     0     LSI

CLI(config fdb)# set spoofed 1.23 00:00:00:00:00:11 permit
OK

CLI(config fdb)# show

port ID   VPI/VCI      MAC address     VLAN  type
-------  ---------  ------------------  ----  ----
   1.6    8/   35  00:00:00:00:00:11     0    AD
```

Example 86 Denying all the upstream traffic of spoofed MAC addresses

```
CLI(status fdb)# show spoofed

   MAC address      port     VPI/VCI   VLAN  status
------------------  -------  ---------  ----  ------
00:00:00:00:00:11     1. 6    8/   35     0     LSA
                      1.23    8/   35     0     LSI


CLI(config fdb)# set spoofed 00:00:00:00:00:11 deny-all
OK

CLI(config fdb)# show

port ID   VPI/VCI      MAC address     VLAN  type
-------  ---------  ------------------  ----  ----
   1. 6    8/   35  00:00:00:00:00:11     0    AD
   1.23    8/   35  00:00:00:00:00:11     0    AD
```

Example 87 Denying all the upstream traffic of spoofed MAC addresses and then trying to permit one on the specified xDSL port.

```
CLI(status fdb)#show spoofed

   MAC address      port     VPI/VCI   VLAN  status
------------------  -------  ---------  ----  ------
00:00:00:00:00:11     1. 6    8/   35     0     LSI
                      1.23    8/   35     0     LSA

CLI(config fdb)# set spoofed 00:00:00:00:00:11 deny-all
OK

CLI(config fdb)# show

port ID   VPI/VCI      MAC address     VLAN  type
-------  ---------  ------------------  ----  ----
   1. 6    8/   35  00:00:00:00:00:11     0    AD
   1.23    8/   35  00:00:00:00:00:11     0    AD

CLI(config fdb)# set spoofed 1.6 00:00:00:00:00:11 permit

ERROR: MAC address is not spoofed.
```

Example 88 Permitting one spoofed MAC address and then trying to denying all the upstream traffic of spoofed MAC addresses on the specified xDSL port.

```
CLI(status fdb)# show spoofed

   MAC address      port     VPI/VCI   VLAN  status
------------------  -------  ---------  ----  ------
00:00:00:00:00:11     1. 6    8/   35     0     LSA
```

```
                    1.23    8/   35     0     LSI

CLI(status fdb)# exit

CLI# config fdb

CLI(config fdb)# set spoofed 1.23 00:00:00:00:00:11 permit
OK

CLI(config fdb)# show

port ID   VPI/VCI      MAC address     VLAN  type
-------  ---------  ------------------  ----  ----
   1. 6    8/   35  00:00:00:00:00:11     0    AD

CLI(config fdb)# set spoofed 00:00:00:00:00:11 deny-all

ERROR: MAC address is not spoofed.
```

Monitoring the Subscriber MAC

The FDB (filtering Database) of NCT192 system stores the following MAC entries

- the manually configured MAC addresses on an ATM VC of xDSL port.
- the MAC addresses learned from the associate ATM VC of xDSL port.

According to the nature of stored MAC entry, each entry possesses “status” field. The definitions of “status” field are as follows.

- “**AD**” : the abbreviation of “ACL Deny”,
  It means the NE is to drop the upstream traffic of the indicated source MAC and forward the upstream traffic of other source MAC from the indicated xDSL port.
- “**AP**” : the abbreviation of “ACL Permit”,
  It means the NE is to forward the upstream traffic of this indicated source MAC and drops the upstream traffic of other source MAC from the indicated xDSL port.
- “**S**”: the abbreviation of “Static”,
  It means this MAC entry is configured manually in FDB.
- “**LU**”: the abbreviation of “Learned Unique”,
  It means this MAC is learned on the indicated xDSL port dynamically with setting aged time and is a unique one.
- “**LUN**”: the abbreviation of “Learned Unique, non-aged”,
  It means this MAC is learned on the indicated xDSL port dynamically with setting non-aged time and is a unique one.
- “**LR**” : the abbreviation of “Learned Routed”,
  It means this MAC is inserted by the xDSL LC in the case that the indicated xDSL port is in the RFC2684 routed mode.
- “**LSI**”: the abbreviation of “Learned Spoofed Inactive”,
  It means the following identities.
  - This MAC is learned on the indicated xDSL port.
  - The NE learns the same MAC on the xDSL ports other than the indicated xDSL port. That is, this MAC is spoofed.
  - This spoofed MAC is at the “inactive” state. That is the NE is to drop the upstream traffic of the spoofed MAC from the the indicated xDSL port.
- “**LSA**” : the abbreviation of “Learned Spoofed Active”,
  It means the following identities.
  - This MAC is learned on the indicated xDSL port.
  - The NE also learns the same MAC on the xDSL ports other than the indicated xDSL port. That is, this MAC is spoofed.
  - This spoofed MAC is at the “active” state. That is the NE is to forward the upstream traffic of the spoofed MAC from the the indicated xDSL port.

Table 7-19 shows how the NE treats the upstream Ethernet frame whenever its source MAC hits the PVC_FDB. Here, the “PVC_FDB” indicates the the FDB associated with the specified ATM

PVC.

Table 7-20 shows the conditions the NE will not learn the source MAC of upstream traffic.

- When the status of existent MAC entry in PVC_FDB is "**AP**".

Table 7-19 The treatment of an upstream Ethernet frame of source MAC hitting the PVC_FDB

Status of hitted MAC entry in PVC_FDB	S	AD	AP	LU	LUN	LR	LSA	LSI
Forward (F) /Drop (D) packets of the same source MAC	F	D	F	F	F	F	F	D

Table 7-20 The conditions the NE does not learn additional source MAC of upstream traffic

Status of existent MAC entry in PVC_FDB	S	AD	AP	LU	LUN	LR	LSA	LSI
Allow (Y) /Deny (N) learning any additional MAC	Y	Y	N	Y	Y	NA	Y	Y

The NE may add a MAC entry to FDB due to either one of the following cases.

- The operator intends to manually add a MAC ACL entry.
- The operator intends to manually add a static MAC entry.
- The NE executes the basic "learning process of a bridge".

Depending on the status of existent MAC entries in FDB, the NE may take some or all of the following actions when it is to add a MAC entry to FDB

- Change the status of existent MAC entries of the same MAC.
- Reject to add this new MAC entry.
- Allow to add this new MAC entry but assign it some different status.

Table 7-21~Table 7-23 depicts the expected status of hitted MAC entry as well as the status of new added MAC entry in the aforementioned cases with the follwoing notations.

- Dif_Port_FDB = The MAC entries of FDB associated with different port
- Dif_PVC_FDB = The MAC entries of FDB associated with the same port but different PVC
- PVC_FDB = The MAC entries of FDB associated with the same port and the same PVC
- o : Permit x : Reject # : Clear LU/LUN Entry
- c : Clear AP Entry & : Clear non-AP Entry r : Replacement

Table 7-21 The expected status of hitted MAC entry as well as the status of new added MAC entry in the case that the MAC entry to be added hits the entry of Dif_Port_FDB

The reason to add a MACentry / Status of matched MAC entry of Dif_Port_FDB	Manual addition			Dynamicaly learning on ATM PVC of		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC	RFC2684 routed mode	"aged" RFC2684 bridged mode	"non-aged" RFC2684 bridged mode
S	x / S	x / S	0 / S	NA	LSI / S	LSI / S
AP	x / AP	x / AP	0 / AP	NA	LSI / AP	LSI / AP
AD	0 / AD	0 / AD	0 / AD	NA	LU / AD	LUN / AD
LR	x / LR	x / LR	x / LR	NA	LSI / LR	LSI / LR
LU	x / LU	x / LU	0 / LU	NA	LSI / LSA	LSI / LSA
LUN	x / LUN	x / LUN	0 / LUN	NA	LSI / LUN	LSI / LUN
LSA	x / LSA	x / LSA	0 / LSA	NA	LSI / LSA	LSI / LSA
LSI	x / LSI	x / LSI	0 / LSI	0 / NA	LSI / LSI	LSI / LSI

NOTE

NA indicates "Not Applicable". As the NE reserves MACs for routed PVC. It's not possible for NE to dynamicaly learn such a MAC address on an ATM PVC of RFC2684 routed mode.

NOTE

Whenever the following 3 cases hold simultaneously.

- NE learns a new MAC entry on a ATM PVC of "non-aged"/"aged" RFC2684 bridged mode,
- This new MAC is the same as the one of FDB associated with different port
- The status of the MAC entry associated with different port is "LUN".

The NE will keep the status of the MAC entry associated with different port as "LUN".

Table 7-22 The expected status of hitted MAC entry as well as the status of new added MAC entry in the case that the MAC entry to be added hits the entry of Dif_PVC_FDB

The reason to add a MACentry / Status of matched MAC entry of Dif_PVC_FDB	Manual addition			Dynamicaly learning on ATM PVC of		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC	RFC2684 routed mode	"aged" RFC2684 bridged mode	"non-aged" RFC2684 bridged mode
S	o / S	o / S	o / S	NA	LU / S	LUN / S
AP	o / AP	o / AP	o / AP	NA	LU / AP	LUN / AP
AD	o / AD	o / AD	o / AD	NA	LU / AD	LUN / AD
LR	x / LR	x / LR	x / LR	NA	NA	NA
LU	o / LU	o / LU	o / LU	NA	x / LU	x / LU
LUN	o / LUN	o / LUN	o / LUN	NA	x / LUN	x / LUN
LSA	x / LSA	x / LSA	x / LSA	NA	x / LSA	x / LSA
LSI	x / LSI	x / LSI	x / LSI	NA	x / LSI	x / LSI

Table 7-23 The expected status of hitted MAC entry as well as the status of new added MAC entry in the case that the MAC entry to be added hits the entry of PVC_FDB

The reason to add a MACentry / Status of matched MAC entry of PVC_FDB	Manual addition			Dynamicaly learning on ATM PVC of		
	a static MAC	a MAC ACL Permit MAC	a MAC ACL Deny MAC	RFC2684 routed mode	"aged" RFC2684 bridged mode	"non-aged" RFC2684 bridged mode
S	x / S	x / S	x / S	NA	x / S	x / S
AP	x / AP	x / AP	x / AP	NA	x / AP	x / AP
AD	x / AD	x / AD	x / AD	NA	x / AD	x / AD
LR	x / LR	x / LR	x / LR	o / LR	NA	NA
LU	r / LU	r+& / LU	r+c / LU	NA	x / LU	NA
LUN	r / LUN	r+& / LUN	r+c / LUN	NA	NA	x / LUN
LSA	x / LSA	x / LSA	x / LSA	NA	x / LSA	NA
LSI	x / LSI	x / LSI	x / LSI	NA	x / LSI	x / LSI

Enter to the "**status fdb**" sub-group directory to view learning MAC addresses from the associate ATM VC.

```
CLI# status fdb
CLI(status fdb)#
```

Table 7-24 shows the commands to show the VC MAC Learning Table. Example 89 shows the usage of these commands as well as their related parameters.

Table 7-24 VC MAC Learning Table

The following command is to display the MAC addresses learned on the specified xDSL line port.	
CLI(status fdb)# show port <*port-range*>	
The following command is to display the spoofed MAC addresses and the xDSL line ports where spoofed MAC addresses are learned.	
CLI(status fdb)# show spoofed	
The following command is to display the xDSL line ports where the specified MAC addresses are learned.	
CLI(status fdb)# show mac <*mac-addr*>	
Parameters	**Task**
<*port--range* >	Identify the port id of the system wish to display current list of learning MAC addresses from their remote network. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*mac-addr*>	Indicate the target MAC address. **Type:** Mandatory **Valid values:** Valid MAC addresses form. (for example: 00:1F:AA:19:78:03)

Example 89 Displaying the MAC addresses learned on the specified xDSL line port

```
CLI(status fdb)# show port 1.6

Port  1. 6

 ID  VPI  VCI     MAC Address    Status
 --- --- ----- ------------------ ------
   1   8    35 00:00:00:00:00:11     LU
```

Example 90 Displaying the spoofed MAC addresses and the xDSL line ports where spoofed MAC addresses are learned

```
CLI(status fdb)# show spoofed

   MAC address      port     VPI/VCI   VLAN  status
------------------  -------  ----------  ----  -------
00:00:00:00:00:11     1. 6    8/   35     0     LSA
                      1.23    8/   35     0     LSI
```

Example 91 Displaying the xDSL line ports where the specified MAC addresses are learned

```
CLI(status fdb)# show mac 00:00:00:00:00:11

   MAC address      port     VPI/VCI   VLAN  status
------------------  -------  ----------  ----  -------
00:00:00:00:00:11     1. 6    8/   35     0     LSA
                      1.23    8/   35     0     LSI
```

This page is leave in blank for note or memo use

Chapter 8 Managing the System Operations

This chapter describes the system functions of NCT192 IP-DSLAM.

This chapter contains the following sections:

- System Administrating
- Alarm Definition and Relay Setting

System Administrating

The system administrating provides command for you to logout the Telnet session or reboots the system device.

Reset the Line Card and Port

Reset the line card and port using the "**reset**" command at the prompt for CLI#.

Table 8-1 shows the commands to reset the planning of line card and port. Example 92 shows the usage of these commands as well as their related parameters.

Table 8-1 Line Card and Port Reset Command

The following command is to reset the specify line card.
CLI# reset lc <*lc-id*>
The following command is to reset the specify NC card.
CLI# reset nc <*nc-id*>
The following command is to reset the specify xDSL port interface.
CLI# reset port <*port-id*>
The following command is to reset (reboot) the system device.
CLI# reset system

Parameters	Task
<*lc-id*>	Identify the slot id of the system **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*nc-id*>	Identify the slot id of the network card **Type:** Mandatory **Valid values:** 1 | 2
<*port-id*>	Identify the port id of the system **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.

Example 92 Reset the line card and xDSL port

```
CLI# reset lc 2
OK

CLI# reset port 1.2.1
OK
```

The pop-up information for reset line card command shows only on Console port access.

Reboot the System

The reboot command activates the software restart of system device. The configuration change will be lost if you did not committed (store) it.

Reboot the system using the "**reboot**" command at the prompt for CLI#.

Table 8-2 System Reboot Command

The following command is to reboot the system device.
CLI# reboot

Alarm Definition and Relay Setting

The alarm definition profile allows you to define the rule of alarm element in system. Through this profile, you are able to change the severity of individual alarm element and decide to report it or not. Alarm element is specified in the class of module or port. Different types of module may present different alarm element. Different types of port may also present different alarm element.

The relay input management allows you to define the alarm relay input. Please see "*System Installation Guide*" for the definition. Once the normal status of input signal is different from the current status, the NE will launch an "abnormal status" alarm of the specified relay input to LCT and NCT192 server.

Configuring the Alarm Definition

Enter to the "**config alarm definition**" sub-group directory to manage the alarm definition. Please refer to Appendix B for the detailed description of defined alarms and their default severity.

```
CLI# config alarm definition
CLI(config alarm definition)#
```

Table 8-3 shows the commands to configure the alarm definition of line card and port. Example 93 shows the usage of these commands as well as their related parameters.

Table 8-3 Alarm Definition Configuration

The following command is to change the default alarm severities
CLI(config alarm definition)# set <*vendorType*> <*alarmType*> {*none* | *critical* | *major* | *minor* | *info*} {*true* | *false*} <*suppressby*>
The following command is to view the status of system alarm severities.
CLI(config alarm definition)# show

Parameters	Task
<*vendorType*>	It specifies an entuty of NE. **Type:** Mandatory **Valid values:** noEntity, cpuModule, adslModule, powerModule, fanModule, adslPort, alarmRelayModule, gePort, alarmRelayInPort
<*alarmType*>	It specifies a numerical representation of the condtion may happen to an entity (<*vendorType*>) of NE. (see the note below) **Type:** Mandatory **Valid values:** 0 ~ 31
{*none* | *critical* | *major* | *minor* | *info*}	Defines the severity level of alarm type. **Type:** Mandatory **Valid values:** none, critical, major, minor, info
{*true* | *false*}	Defines the filtering status of specific alarm type. **Type:** Mandatory **Valid values:** true, false true – The NE is not to send alarm trap to the trap host whenever there is an alarm indicated by <*vendorType*> and <*alarmType*> false –The NE is to send alarm trap to the trap host whenever there is an alarm indicated by <*vendorType*> and <*alarmType*>
<*suppressby*>	Defines the prevent alarms from being reported on another alarm, when an alarm or condition exists but you do not want it to appear instead of another.. (see the note below) **Type:** Mandatory **Valid values:** Hexadecimal number

The alarm suppression (suppressed by) allows you to mask specific alarms when there are sequences occurred at the same time. For example, let the LOF (Loss of Frame) be configured to be suppressed by the LOS (Loss of Signal), the LOF will not be display on the screen but only LOS whenever the corresponding ADSL loop is cut.

In Example 93, the “name” represents an abbreviation of the condtion indicated by <*alarmType*>.

<*alarmType*> may indicate different condtions when it appeas with different <*vendorType*>. For example, in Example 93, the <*alarmType*> of value 6 represents

“TCA_DHCP_BC” when it appears with “cpuModule”,

“UAS_FE_15_MIN” when it appears with “adslPort”

and

“TCA_SNR_NE” when it appears with “shdslPort”.

Example 93 Display the system alarm definition

```
CLI# config alarm definition set adslModule 0 critical true 0x0a
OK

CLI# config alarm definition show

Alarm definition
    vendor-type  type          name          severity  filtered  supress-by
    -----------  ----  --------------------  --------  --------  ----------
       noEntity     0                 EMPTY      none     false         0x0
      cpuModule     0               MISSING     major     false         0x0
```

cpuModule	1	TEMP	major	false	0x0
cpuModule	2	VOL	major	false	0x0
cpuModule	3	MISMATCH	major	false	0x0
cpuModule	6	TCA_DHCP_BC	warning	false	0x0
cpuModule	30	HW_INFO_INV	major	false	0x0
adslModule	**0**	**MISSING**	**critical**	**true**	**0xa**
adslModule	1	TEMP	major	false	0x0
adslModule	2	VOL	major	false	0x0
adslModule	3	MISMATCH	major	false	0x0
adslModule	4	NOT_OPERABLE	major	false	0x0
adslModule	30	HW_INFO_INV	major	false	0x0
shdslModule	0	MISSING	major	false	0x0
shdslModule	1	TEMP	major	false	0x0
shdslModule	2	VOL	major	false	0x0
shdslModule	3	MISMATCH	major	false	0x0
shdslModule	4	NOT_OPERABLE	major	false	0x0
shdslModule	30	HW_INFO_INV	major	false	0x0
powerModule	0	MISSING	major	false	0x0
powerModule	4	NOT_OPERABLE	major	false	0x0
powerModule	5	PWR_FAIL	major	false	0x0
fanModule	0	MISSING	major	false	0x0
fanModule	1	FAN1	major	false	0x0
fanModule	2	FAN2	major	false	0x0
fanModule	9	VOL	major	false	0x0
adslPort	1	ES_NE_15_MIN	minor	false	0x0
adslPort	2	SES_NE_15_MIN	minor	false	0x0
adslPort	3	UAS_NE_15_MIN	minor	false	0x0
adslPort	4	ES_FE_15_MIN	minor	false	0x0
adslPort	5	SES_FE_15_MIN	minor	false	0x0
adslPort	6	UAS_FE_15_MIN	minor	false	0x0
adslPort	7	ES_NE_1_DAY	minor	false	0x0
adslPort	8	SES_NE_1_DAY	minor	false	0x0
adslPort	9	UAS_NE_1_DAY	minor	false	0x0
adslPort	10	ES_FE_1_DAY	minor	false	0x0
adslPort	11	SES_FE_1_DAY	minor	false	0x0
adslPort	12	UAS_FE_1_DAY	minor	false	0x0
adslPort	13	LOS	minor	false	0x0
adslPort	14	LOF	minor	false	0x0
adslPort	15	LPWR	minor	false	0x0
adslPort	16	GEN_LINE_INIT_FAIL	minor	false	0x0
adslPort	17	CONFIG_ERROR	minor	false	0x0
adslPort	18	HIGH_BIT_RATE	minor	false	0x0
adslPort	19	COMM_PROBLEM	minor	false	0x0
adslPort	20	NO_PEER_DETECTED	minor	false	0x0
adslPort	21	TRAINING	warning	false	0x0
adslPort	22	NO_CONFIG	warning	false	0x0
adslPort	23	PS_L2_MANUAL	info	false	0x0
adslPort	24	PS_L2_AUTO	info	false	0x0
adslPort	25	PS_L3_CO	info	false	0x0
adslPort	26	PS_L3_CPE	info	false	0x0
adslPort	29	ILLEGAL_IP	warning	false	0x0
adslPort	30	MAC_SPOOFED	warning	false	0x0
adslPort	31	DISABLED	info	false	0x0
ugePort	0	MISSING	major	false	0x0
ugePort	4	LOS	major	false	0x0
ugePort	27	LINK_DOWN	major	false	0x0
ugePort	29	STP_LEARN	info	false	0x0
ugePort	30	STP_BLOCK	info	false	0x0
ugePort	31	DISABLED	info	false	0x0
relayModule	0	MISSING	major	false	0x0
relayInPort	1	RELAY_ABNORMAL	major	false	0x0
relayInPort	31	DISABLED	info	false	0x0
shdslPort	1	TCA_ES_NE_15MIN	minor	false	0x0
shdslPort	2	TCA_SES_NE_15MIN	minor	false	0x0
shdslPort	3	TCA_UAS_NE_15MIN	minor	false	0x0
shdslPort	4	TCA_CRC_NE_15MIN	minor	false	0x0
shdslPort	5	TCA_LOSW_NE_15MIN	minor	false	0x0
shdslPort	6	TCA_SNR_NE	minor	false	0x0

```
shdslPort     7          TCA_ATTN_NE     minor     false        0x0
shdslPort     8                  OPI     minor     false        0x0
shdslPort     9                  LOS     minor     false        0x0
shdslPort    10                 SEGA     minor     false        0x0
shdslPort    11                 LPWR     minor     false        0x0
shdslPort    12                 SEGD     minor     false        0x0
shdslPort    13              PBO_NE      info     false        0x0
shdslPort    14          DEVFAULT_NE     minor     false        0x0
shdslPort    15            DCCONT_NE     minor     false        0x0
shdslPort    16              LOSW_NE     minor     false        0x0
shdslPort    17           INI_CFG_NE     minor     false        0x0
shdslPort    18     INI_PROTOCOL_NE      minor     false        0x0
shdslPort    22              NOPEER     minor     false        0x0
shdslPort    23              PBO_FE      info     false        0x0
shdslPort    24          DEVFAULT_FE     minor     false        0x0
shdslPort    25            DCCONT_FE     minor     false        0x0
shdslPort    26              LOSW_FE     minor     false        0x0
shdslPort    27           INI_CFG_FE     minor     false        0x0
shdslPort    28     INI_PROTOCOL_FE      minor     false        0x0
shdslPort    31             DISABLED      info     false        0x0
```

Configuring the System Relay-In Alarm

The NCT192 support housekeeping alarm relays for input signals.

Enter to the "**config alarm input**" sub-group directory to activate and monitor the alarm relay-in.

```
CLI# config alarm input
CLI(config alarm input)#
```

Table 8-4 shows the commands to configure system relay-in alarm input configuration. Example 94 shows the usage of these commands as well as their related parameters.

Table 8-4 System Relay-In Alarm Configuration

The following command is to set the name and index of system relay-in alarm input function.
CLI(config alarm input)# set name <*index*> <*input-name*>
The following command is to set the normal state of system relay-in alarm input function.
CLI(config alarm input)# set normal-state <*index*> <*state*>
The following command is to enable the system relay-in alarm input function.
CLI(config alarm input)# enable <*index*>
The following command is to disable the system relay-in alarm input function.
CLI(config alarm input)# disable <*index*>
The following command is to view the status of system relay-in alarm input function.
CLI(config alarm input)# show

Parameters	Task
< *index*>	Identify the port number of relay-in alarm. **Type:** Mandatory **Valid values:** 1 ~ 4
< *input-name* >	This specifies the name of given relay-in alarm port. **Type:** Mandatory **Valid values:** String of up to 10 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
< *state* >	Identify one of the parameter of expects normal status of the relay-in alarm port. **Type:** Mandatory **Valid values:** open, close

Example 94 Display the system relay-in alarm input port status

```
CLI(config alarm input)# set name 1 Door
OK

CLI(config alarm input)# set normal-state 1 closed
OK

CLI(config alarm input)# enable 1
OK

CLI(config alarm input)# show

 index                name               admin-state  normal-state
-------  --------------------------------  -----------  ------------
     1                             Door       enabled        closed
     2              << not defined >>     disabled        opened
     3              << not defined >>     disabled        opened
     4              << not defined >>     disabled        opened
```

Configuring the System Relay-Out Alarm

The NCT192 support housekeeping alarm relays to trigger external device such as speaker or light to launch warning signal.

Enter to the "**config alarm output**" sub-group directory to activate and monitor the alarm relay-in.

```
CLI# config alarm output
CLI(config alarm output)#
```

Table 8-5 shows the commands to configure system relay-in alarm output configuration of line card and port. Example 95 shows the usage of these commands as well as their related parameters.

Table 8-5 System Relay-Out Alarm Configuration

The following command is to set the name and index of system relay-in alarm output function.
CLI(config alarm output)# set name <*index*> <*output-name*>
The following command is to set the severities of system relay-in alarm output function.
CLI(config alarm output)# set alarm-severities <*index*> <*severities*>
The following command is to enable the system relay-in alarm output function.
CLI(config alarmoutput)# enable <*index*>
The following command is to disable the system relay-in alarm output function.
CLI(config alarm output)# disable <*index*>
The following command is to view the status of system relay-in alarm output function.
CLI(config alarm output)# show

Parameters	Task
< *index*>	Identify the port number of relay-in alarm. **Type:** Mandatory **Valid values:** 1 ~ 1
<*output-name* >	This specifies the name of given relay-in alarm port. **Type:** Mandatory **Valid values:** String of up to 10 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').
< *severities* >	Identify one of the parameter of expects normal status of the relay-in alarm port. **Type:** Mandatory **Valid values:** open, close

Example 95 Display the system relay-in alarm input port status

```
CLI(config alarm output)# set name 1 Alarm_Output
OK

CLI(config alarm output)# set alarm-severities 1 major
OK

CLI(config alarm output)# enable 1
OK

CLI(config alarm output)# show

name                : Alarm_Output
alarm severities    : major
admin state         : enabled
```

This page is leave in blank for note or memo use

Chapter 9 Diagnosis and Performance Monitoring

This chapter describes the filtering rule in different network layer.

This chapter contains the following sections:

- Performance Monitoring on System and Network Interface
- Performance Monitoring on ADSL Subscriber Interface
- Performance Monitoring on SHDSL Subscriber Interface
- Monitoring System Alarms
- OAM and Loop Diagnostic Test on Subscriber Interface
- Network Ping Test
- Monitoring the System Environment
- Monitoring the System Performance

Performance Monitoring on System and Network Interface

Enter to the "**status perf**" sub-group directory to display performance parameters on the Network interface.

```
CLI# status perf
CLI(status perf)#
```

Table 9-1 shows the commands to display the performance parameters on system and network interface of NE. Example 96 shows the usage of its command as well as its related parameters.

Table 9-1 Performance Monitoring on System and Network Interface

The following command is to viewing the performance parameters on the Network interface.
CLI(status perf)# show nc

Example 96 Display the performance parameters on network interface

```
CLI(STA-PERF)# show nc
       interface        unicast    broadcast   multicast    discard      error
    ----------------  -----------  ----------  ----------  ----------  ----------
      UGE-01  inPkts            0           0           0           0           0
              outPkts           0           3           0           0           0
      UGE-02  inPkts            0           0           0           0           0
              outPkts           0           0           0           0           0
      LC-01   inPkts         6218          84           0           0           0
              outPkts         6281           1           0           0           0
      LC-02   inPkts         9448          88           0           0           0
              outPkts         9522           1           0           0           0
      LC-03   inPkts         5912          80           0           0           0
              outPkts         5976           1           0           0           0

      LC-04   inPkts           79          83           0           0           0
              outPkts          78          78           0           0           0

       interface       pause/RX    pause/TX
    ----------------  -----------  ----------
       UGE-01  pkts             0           0
       UGE-02  pkts             0           0
```

Performance Monitoring on ADSL Subscriber Interface

Enter to the "**status perf**" sub-group directory to display performance parameters on the ADSL Subscriber interface.

```
CLI# status perf
CLI(status perf)#
```

Table 9-2 shows the commands to display the performance parameters on subscriber interface of NE. Example 97 shows the usage of its command as well as its related parameters.

Table 9-2 Performance Monitoring on ADSL Subscriber Interface

Use this command to view the performance parameters on the specified ADSL line port.	
CLI(status perf)# show current *<port-id> <side>*	
Parameters	**Task**
<port-id>	Identify the port id of the system wish to display the performance parameters with associated time period. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<side>	Identify the performance parameters display on Near-End or Far-End, show both if not specify. **Type:** Optional **Valid values:** near, far

Example 97 Display the performance parameters on subscriber interface

```
CLI(status perf)# show current 1.1.2

[UserCells/1.1.2]
               Curr15Min     Prev15Min     Curr1Day      Prev1Day
                ---------     ---------     ---------     ---------
        rxCells         0             0             0             3
        txCells         0             0             0             0

[Perf/NE/1.1.2]
               Curr15Min     Prev15Min     Curr1Day      Prev1Day
                ---------     ---------     ---------     ---------
             UAS         0             0             0          8627
            LOFs         0             0             0            30
            LOSs         0             0             0             0
            LPRs         0             0             0             0
           INITs         0             0             0             6
       FullINITs         0             0             0             6
              ES         0             0             0             0
             SES         0             0             0             0
              CV         0             0             0             0

[Perf/FE/1.1.2]
               Curr15min     Prev15Min     Curr1Day      Prev1Day
                ---------     ---------     ---------     ---------
             UAS         0             0             0          8577
            LOFs         0             0             0             8
            LOSs         0             0             0             7
            LPRs         0             0             0          8329
              ES         0             0             0           144
             SES         0             0             0            45
              CV         0             0             0          1618
```

Performance Monitoring on SHDSL Subscriber Interface

Enter to the "**status perf**" sub-group directory to display performance parameters on the SHDSL Subscriber interface.

```
CLI# status perf
CLI(status perf)#
```

Table 9-3 shows the commands to configure the performance parameters on SHDSL subscriber interface of NE. Example 98 shows the usage of its command as well as its related parameters.

Table 9-3 Performance Monitoring on SHDSL Subscriber Interface

The following command is to view the performance parameters on specific SHDSL line port.	
CLI(status perf)# show current *<port-id> <side>*	
The following command is to show the shdsl line historical performance data (15 minutes per interval).	
CLI(status perf)# show history-15-min *<port-id> <start-interval>*	
The following command is to show the shdsl line historical performance data (1day per interval).	
CLI(status perf)# show history-1-day *<port-id>*	
Parameters	**Task**
<port-id>	Identify the port id of the system wish to perform the link monitoring, the define line port must operate in running status. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<start-interval>	This specifies the adsl line historical performance data (15 minutes per interval). **Type:** Mandatory **Valid values:** 1 ~ 96
<side>	Identify the given performance parameter value in Near-End or Far-End side, CLI Ex will apply the same performance parameter value for Near-End and Far-End if not specify. **Type:** Optional **Valid values:** near, far

Example 98 Display the performance parameters on SHDSL subscriber interface

```
CLI(status perf)# show current 1.6 near

[UserCells/1.6]
              Curr15Min     Prev15Min     Curr1Day      Prev1Day
              ---------     ---------     ---------     ---------
       rxCells    52980        267862      22000803             0
       txCells        0             0             0             0

[Perf/NE/1.6]
    Current 15 Min Elapsed :   178 seconds
    Current 1 Day Elapsed  : 73978 seconds

              Curr15Min     Prev15Min     Curr1Day      Prev1Day
              ---------     ---------     ---------     ---------
           UAS        0             0            44             0
          LOFs        0             0             0             0
          LOSs        0             0             0             0
          LPRs        0             0             0             0
         INITs        0             0             1             0
     FailINITs        0             0             0             0
            ES        0             0             0             0
           SES        0             0             0             0
            CV        0             0             0             0
```

Monitoring System Alarms

This section explains how to monitor alarms with CLI Ex, which includes viewing current and historical alarm data.

The CLI Ex detects and reports system alarms generated by the NCT192 and the adjacent network. You can use CLI Ex to monitor alarms at a card, port, or network level and view alarm with severities.

Enter to the "**status alarm**" sub-group directory to monitor system alarms.

```
CLI# status alarm
CLI(status alarm)#
```

Table 9-4 shows the commands to configure the diagnostic the system alarm of NE. Example 100 ~ Example 102 shows the usage of its command as well as its related parameters.

Table 9-4 Viewing the System Alarm

The following command is to determine if the NE reports the current alarm on the CLI Ex in real-time.
CLI(status alarm)# reportconsole {*on* | *off*}
The following command is to view the current alarm data.
CLI(status alarm)# show current
The following command is to view the historical alarm data.
CLI(status alarm)# show history
The following command is to view the setting of reportconsole
CLI(status alarm)# show reportconsole
The following command is to view the detailed description of the condition happen to the entity indicated by <*unit*>.
CLI(status alarm)# show detail <*unit*>
The following command is to view the status of system relay-in alarm inputput function.
CLI(status alarm)# show input
The following command is to view the status of system relay-in alarm output function.
CLI(status alarm)# show output

Parameters	Task
{*on* | *off*}	This specifies to let the NE report the current alarm on the CLI Ex in real-time or not. **Type:** Mandatory **Valid value:** on, off
{*unit*}	This indicates the entity on IP-DSLAM. **Type:** Mandatory **Valid value:** All the alarm unit on IP-DSLAM (see Example 100)

Example 99 Viewing the active alarm on NE via Console Port (RS232 port)

```
CLI(status alarm)# reportconsole on
OK

CLI# Alarm <10121> ( 0x00082000 | LOS | COMM_PROBLEM ) at THU NOV 08 15:28:39 2007
CLI#
```

Example 99 shows the active alarm on NE via Console Port (RS232 port) when the loop between the NE and the ADSL CPE is broken.

Example 100 Viewing the current active alarm on NE

```
CLI(status alarm)# show current
       unit       on-line type  planned type alarm    last change      severity
    ------------  ------------  ------------  ---  ------------------  ---------
          shelf         shelf         shelf    -  11-07-07 11:42:49       none
           LC01    adslModule    adslModule    v  11-08-07 09:39:01      major
     LC01/port01      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port02      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port03      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port04      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port05      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port06      adslPort      adslPort    -  11-08-07 09:39:42       none
     LC01/port07      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port08      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port09      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port10      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port11      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port12      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port13      adslPort      adslPort    v  11-08-07 09:39:30      minor
     LC01/port14      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port15      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port16      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port17      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port18      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port19      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port20      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port21      adslPort      adslPort    -  11-08-07 09:39:45       none
     LC01/port22      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port23      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port24      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port25      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port26      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port27      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port28      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port29      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port30      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port31      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port32      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port33      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port34      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port35      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port36      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port37      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port38      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port39      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port40      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port41      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port42      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port43      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port44      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port45      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port46      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port47      adslPort      adslPort    v  11-08-07 09:39:01       info
     LC01/port48      adslPort      adslPort    v  11-08-07 09:39:30      minor
           LC02      noEntity      noEntity    v  11-07-07 11:43:00       none
           LC03      noEntity      noEntity    v  11-07-07 11:43:00       none
           LC04      noEntity      noEntity    v  11-07-07 11:43:00       none
             NC     cpuModule     cpuModule    v  11-08-07 11:21:05      major
           UGE1       ugePort       ugePort    -  11-07-07 15:40:45       none
           UGE2      noEntity       ugePort    v  11-07-07 11:42:49       info
         powerA   powerModule   powerModule    v  11-07-07 11:43:23      major
         powerB   powerModule   powerModule    -  11-07-07 11:42:57       none
            fan     fanModule     fanModule    v  11-07-07 11:43:26      major
          relay      noEntity   relayModule    v  11-07-07 11:42:49      major
      relayin-1   relayInPort   relayInPort    -  11-08-07 10:42:08       none
      relayin-2   relayInPort   relayInPort    v  11-07-07 11:42:49       info
      relayin-3   relayInPort   relayInPort    v  11-07-07 11:42:49       info
```

```
relayin-4   relayInPort   relayInPort    v  11-07-07 11:42:49      info
```

Example 100 shows the current active alarm on NE. It is noted that the notation "v" in the colume "alarm" indicates an alarm occurs on the corresponding "unit". Example 100 also shows "last change" time instance and the "severity" of the current active alarm.

Example 101 Display the detailed description of an alarm

```
CLI(status alarm)# show detail LCO2

Detail alarm list is:
          alarm name         severity                description
    ----------------------  --------  ----------------------------------------
                      EMPTY       none        Neither plan type nor on-line type
```

Example 101 shows the CLI command to inspect the details of a current active alarm which include the alarm condition ("alarm name") and its description ("description").

Example 102 Display the history of alarms

```
CLI(status alarm)# show alarmhistory
History Table
     idx   phyidx   planned type   online type  alarm type      occurtime
    -----  -------  -------------  -----------  ----------  -------------------
    12562    10236       adslPort     adslPort          20   10-10-00 09:18:44
    12563    10236       adslPort     adslPort          21   10-10-00 09:18:44
    12564    10236       adslPort     adslPort          22   10-10-00 09:18:44
    12565    10236       adslPort     adslPort          23   10-10-00 09:18:44
    12566    10236       adslPort     adslPort          24   10-10-00 09:18:44
    12567    10236       adslPort     adslPort          25   10-10-00 09:18:44
    12568    10236       adslPort     adslPort          26   10-10-00 09:18:44
    12569    10236       adslPort     adslPort          29   10-10-00 09:18:44
    12570    10236       adslPort     adslPort          30   10-10-00 09:18:44
    12571    10236       adslPort     adslPort          31   10-10-00 09:18:44
    12572    10237       adslPort     adslPort           1   10-10-00 09:18:44
    12573    10237       adslPort     adslPort           2   10-10-00 09:18:44
    12574    10237       adslPort     adslPort           3   10-10-00 09:18:44
    12575    10237       adslPort     adslPort           4   10-10-00 09:18:44
    12576    10237       adslPort     adslPort           5   10-10-00 09:18:44
    12577    10237       adslPort     adslPort           6   10-10-00 09:18:44
    12578    10237       adslPort     adslPort           7   10-10-00 09:18:44
    12579    10237       adslPort     adslPort           8   10-10-00 09:18:44
    12580    10237       adslPort     adslPort           9   10-10-00 09:18:44
    12581    10237       adslPort     adslPort          10   10-10-00 09:18:44
```

Example 103 Display the status of alarm input

```
CLI(status alarm)# show input
                                          admin     normal    current
 index                name                state     state     state
-------  ---------------------------------  --------  --------  --------
      1                      Alarm_Input    enabled    opened    opened
      2                << not defined >>   disabled    opened       n/a
      3                << not defined >>   disabled    opened       n/a
      4                << not defined >>   disabled    opened       n/a
```

Example 104 Display the status of alarm output

```
CLI(status alarm)#   show output

name               : Alarm_Output
alarm severities   : major
admin state        : enabled
```

```
current state       : enabled
```

OAM and Loop Diagnostic Test on Subscriber Interface

In order to diagnose and fix problem, the NE supports to perform the ATM Operation, Administration, and Maintenance (OAM) F5 diagnosis at data connection layer and the ADSL loop diagnosis at physical layer, respectively.

ATM OAM F5 VC Diagnosis

Via ATM OAM F5 loopback diagnosis, the operator is able to diagnose the health of existant ATM VC connection between the NE and ADSL CPE in intrest.

Enter to the "**diag**" group directory with "**oam**" command to perform the OAM F5 VC diagnostic.

```
CLI# diag
CLI(diag)#
```

Table 9-5 shows the commands to configure OAM F5 VC diagnosis test of NE. Example 105 shows the usage of its command as well as its related parameters.

Table 9-5 OAM F5 VC Diagnosis Test

The following command is to testing the OAM F5 on both End-to-End and Segment-to-Segment.	
CLI(diag)# oam set F5 <*port-id*> <*vpi*> <*vci*> **both**	
The following command is to testing the OAM F5 on End-to-End only.	
CLI(diag)# oam set F5 <*port-id*> <*vpi*> <*vci*> **end-to-end**	
The following command is to testing the OAM F5 on Segment-to-Segment only.	
CLI(diag)# oam set F5 <*port-id*> <*vpi*> <*vci*> **seg-to-seg**	
Parameters	**Task**
<*port-id*>	Identify the port id of the system wish to perform the OAM F5, the define VC must existed at defines line port. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<*vpi*>	Defines the VPI (Virtual Path Identifier) value. **Type:** Mandatory **Valid values:** 0 ~ 255
<*vci*>	Defines the VCI (Virtual Channel Identifier) value. **Type:** Mandatory **Valid values:** 1 ~ 65535 (1 ~ 31 are reserved)

Example 105 shows the OAM F5 diagnostic. When the xDSL CPE echos to the OAM F5 cells, the CLI Ex shows "**alive**". On the other hand, check both xDSL physical layer and ATM layer setting if shows "**OAM timeout**" otherwise.

Example 105 Diagnosing the OAM F5 in ATM layer of Subscriber interface

```
CLI(diag oam )# set F5 1.1.2 0 35 both
Port 1.1.2 pvc 0/35: alive.
OK

CLI(diag oam )# set F5 1.1.1 0 35 both
Port 1.1.1 pvc 0/35: OAM timeout.
OK
```

ADSL Loop Diagnosis (DELT <Dual-Ended Line Test>)

The DELT loop diagnosis function provides mechanism to measure the ADSL loop quality. This action will interrupt the ADSL connection. However, more detailed inform are gathered in comparison with the aforementioned loop monitoring function.

This function is available on ADSL2 and ADSL2+ connection only, the ADSL CPE who did not complied with ITU-T standard G.992.3, G.992.4, and G.992.5 may not be able to perform the loop diagnostics.

Enter to the "**diag**" group directory with "**delt**" command to perform the ADSL loop diagnostic.

```
CLI# diag
CLI(diag)#
```

Table 9-6 shows the commands to configure ADSL loop diagnostic test of NE. Example 106 shows the usage of its command as well as its related parameters.

Table 9-6 ADSL Loop Diagnosis

The following command is to start the ADSL loop diagnosis (DELT) process on the specific ADSL line port.	
CLI(diag delt)# loopdiag start *<port-id> <profile-name>*	
The following command is to manually terminate the ADSL loop diagnosis (DELT) process.	
CLI(diag delt)# loopdiag stop	
The following command is to view the test result of DELT	
CLI(diag delt)# loopdiag show	
Parameters	**Task**
<port-id>	Identify the port id of the system wish to perform the loop diagnostic, the define line port must operate in run-time status. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.
<profile-name>	This specifies the ADSL connection profile of the specific ADSL line port. **Type:** Mandatory **Valid values:** String of up to 32 characters ('0'~'9', 'A'~'Z', 'a'~'z', '-', '_', '.', '@').

Example 106 Diagnosing the ADSL loop performance via DELT

```
CLI(diag delt)# start 1.6 ADSL_P6
OK

CLI(diag delt)# show
Loop diag result:
Port  1. 6

Used Profile:  "ADSL_P6"
                        ATU-C  ATU-R
Attainable Rate(Kbps)   26204.0 1296.0
Loop Attenuation(dB)    0.7    0.0
Signal Attenuation(dB)  0.0    0.0
SnrMargin(dB)           6.0    0.0
TxPower(dBm)            12.3   12.2
H(f) logarithmic representation( Hlog(f) )
DS              Unit: dB
[  1]  -77.0  -35.0  -39.0  -39.0  -44.0  -47.0  -44.0  -44.0
[  9]  -47.0  -47.0  -44.0  -47.0  -53.0  -47.0  -47.0  -47.0
[ 17]  -46.0  -53.0  -50.0  -54.0  -54.0  -46.0  -44.0  -40.0
[ 25]  -38.0  -35.0  -34.0  -30.0  -28.0  -26.0  -23.0  -21.0
```

```
[ 33]  -19.0  -17.0  -15.0  -13.0  -11.0   -9.0   -7.0   -6.0
[ 41]   -5.0   -4.0   -4.0   -3.0   -3.0   -3.0   -2.0   -2.0
[ 49]   -2.0   -2.0   -2.0   -2.0   -2.0   -1.0   -1.0   -1.0
[ 57]   -1.0   -1.0   -1.0   -1.0   -1.0    0.0    0.0    0.0
[ 65]    0.0    0.0    0.0    0.0    0.0    0.0    1.0    1.0
[ 73]    1.0    1.0    1.0    1.0    1.0    1.0    1.0    1.0
[ 81]    1.0    2.0    2.0    2.0    2.0    2.0    2.0    2.0
[ 89]    2.0    2.0    2.0    2.0    2.0    2.0    2.0    2.0
...
...
[441]   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0
[449]   -1.0   -1.0   -1.0   -2.0   -2.0   -2.0   -2.0   -2.0
[457]   -2.0   -2.0   -2.0   -2.0   -3.0   -3.0   -3.0   -3.0
[465]   -3.0   -3.0   -3.0   -3.0   -4.0   -4.0   -4.0   -4.0
[473]   -4.0   -4.0   -5.0   -5.0   -5.0   -5.0   -5.0   -6.0
[481]   -6.0   -6.0   -6.0   -6.0   -7.0   -7.0   -7.0   -7.0
[489]   -8.0   -8.0   -8.0   -8.0   -9.0   -9.0   -9.0   -9.0
[497]  -10.0  -10.0  -10.0  -11.0  -11.0  -11.0  -11.0  -12.0
[505]  -12.0  -12.0  -12.0  -13.0  -13.0  -13.0  -13.0  -13.0

US              Unit: dB
[  1]  -34.0    N/A    N/A    N/A  -71.0  -61.0  -18.0   -8.0
[  9]    0.0    3.0    3.0    3.0    4.0    4.0    4.0    4.0
[ 17]    3.0    3.0    2.0    2.0    1.0    0.0   -1.0   -2.0
[ 25]   -3.0   -4.0   -5.0   -5.0   -6.0   -7.0   -8.0   -9.0
[ 33]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 41]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 49]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 57]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

Quiet Line Noise PSD ( QLN(f) )
DS              Unit: dB
[  1] -120.0 -140.0 -141.0 -141.0 -141.0 -141.0 -141.0 -141.0
[  9] -141.0 -141.0 -141.0 -141.0 -141.0 -141.0 -141.0 -141.0
[ 17] -141.0 -140.0 -140.0 -140.0 -139.0 -140.0 -140.0 -139.0
[ 25] -138.0 -138.0 -137.0 -136.0 -134.0 -134.0 -132.0 -130.0
[ 33] -129.0 -127.0 -125.0 -124.0 -124.0 -122.0 -121.0 -121.0
[ 41] -120.0 -119.0 -119.0 -118.0 -119.0 -119.0 -119.0 -119.0
[ 49] -119.0 -118.0 -119.0 -119.0 -118.0 -118.0 -118.0 -118.0
[ 57] -118.0 -118.0  -97.0 -117.0 -117.0 -117.0 -118.0 -118.0
[ 65] -118.0 -117.0 -117.0 -117.0 -117.0 -116.0 -117.0 -117.0
[ 73] -117.0 -117.0 -117.0 -117.0 -116.0 -116.0 -117.0 -117.0
[ 81] -117.0 -117.0 -117.0 -117.0 -117.0 -116.0 -117.0 -117.0
[ 89] -116.0 -116.0 -116.0 -116.0 -116.0 -116.0 -117.0 -116.0
...
...
[441] -113.0 -113.0 -114.0 -114.0 -113.0 -114.0 -114.0 -114.0
[449] -113.0 -114.0 -114.0 -114.0 -114.0 -113.0 -114.0 -114.0
[457] -113.0 -114.0 -114.0 -114.0 -114.0 -114.0 -114.0 -114.0
[465] -114.0 -114.0 -115.0 -115.0 -114.0 -114.0 -114.0 -114.0
[473] -115.0 -115.0 -114.0 -115.0 -114.0 -114.0 -114.0 -115.0
[481] -115.0 -115.0 -114.0 -114.0 -115.0 -115.0 -115.0 -114.0
[489] -116.0 -115.0 -115.0 -116.0 -115.0 -115.0 -115.0 -115.0
[497] -116.0 -116.0 -116.0 -115.0 -115.0 -115.0 -115.0 -115.0
[505] -115.0 -116.0 -115.0 -116.0 -116.0 -116.0 -116.0 -116.0

US              Unit: dB
[  1]    N/A -117.0 -118.0 -119.0 -118.0 -118.0 -117.0 -117.0
[  9] -113.0 -113.0 -114.0 -111.0 -114.0 -113.0 -113.0 -112.0
[ 17] -115.0 -115.0 -115.0 -113.0 -115.0 -116.0 -108.0 -113.0
[ 25] -116.0 -114.0 -115.0 -117.0 -116.0 -117.0 -117.0 -118.0
[ 33] -118.0 -118.0 -119.0 -119.0 -118.0 -118.0 -118.0 -118.0
[ 41] -119.0 -120.0 -118.0 -119.0 -118.0 -120.0 -120.0 -118.0
[ 49] -118.0 -118.0 -118.0 -118.0 -118.0 -119.0 -119.0 -118.0
[ 57] -119.0 -119.0 -118.0 -118.0 -118.0 -118.0 -118.0 -118.0

SNR(f)
```

```
DS              Unit: dB
[  1]    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
[  9]    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
[ 17]    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
[ 25]    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
[ 33]    0.0   31.0   32.0   32.0   34.0   35.0   36.0   38.0
[ 41]   40.0   41.0   43.0   44.0   45.0   46.0   48.0   49.0
[ 49]   50.0   52.0   52.0   53.0   54.0   54.0   56.0   57.0
[ 57]   57.0   57.0   44.0   58.0   59.0   59.0   58.0   59.0
[ 65]   60.0   59.0   60.0   60.0   60.0   60.0   60.0   61.0
[ 73]   61.0   61.0   61.0   61.0   61.0   61.0   62.0   61.0
[ 81]   61.0   61.0   61.0   61.0   61.0   61.0   61.0   61.0
[ 89]   61.0   61.0   62.0   61.0   61.0   61.0   61.0   61.0
...
...
[441]   55.0   55.0   55.0   54.0   55.0   55.0   55.0   54.0
[449]   55.0   55.0   54.0   55.0   54.0   54.0   54.0   54.0
[457]   54.0   54.0   54.0   54.0   54.0   54.0   54.0   53.0
[465]   54.0   53.0   54.0   53.0   54.0   53.0   53.0   53.0
[473]   53.0   53.0   53.0   52.0   53.0   52.0   53.0   52.0
[481]   52.0   52.0   51.0   51.0   52.0   51.0   51.0   51.0
[489]   50.0   50.0   50.0   50.0   49.0   49.0   49.0   48.0
[497]   48.0   46.0   45.0   43.0   43.0   42.0   42.0   41.0
[505]   41.0   38.0   38.0   38.0   37.0   32.0   32.0   25.0

US              Unit: dB
[  1]    N/A    N/A    N/A    N/A    N/A    N/A    N/A   30.0
[  9]   36.0   42.0   44.0   46.0   49.0   49.0   51.0   51.0
[ 17]   52.0   52.0   53.0   53.0   54.0   55.0   56.0   55.0
[ 25]   56.0   55.0   54.0   52.0   51.0   48.0   44.0   39.0
[ 33]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 41]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 49]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 57]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

CLI(diag delt)# stop
OK

CLI(diag delt)# show
Loop diag result:
Port  1. 6

Used Profile:  "ADSL_P6"
                        ATU-C  ATU-R
Attainable Rate(Kbps)   26204.0 1296.0
Loop Attenuation(dB)    0.7    0.0
Signal Attenuation(dB)  0.0    0.0
SnrMargin(dB)           6.0    0.0
TxPower(dBm)            12.3   12.2
H(f) logarithmic representation( Hlog(f) )
DS              Unit: dB
[  1]  -77.0  -35.0  -39.0  -39.0  -44.0  -47.0  -44.0  -44.0
[  9]  -47.0  -47.0  -44.0  -47.0  -53.0  -47.0  -47.0  -47.0
[ 17]  -46.0  -53.0  -50.0  -54.0  -54.0  -46.0  -44.0  -40.0
[ 25]  -38.0  -35.0  -34.0  -30.0  -28.0  -26.0  -23.0  -21.0
[ 33]  -19.0  -17.0  -15.0  -13.0  -11.0   -9.0   -7.0   -6.0
[ 41]   -5.0   -4.0   -4.0   -3.0   -3.0   -3.0   -2.0   -2.0
[ 49]   -2.0   -2.0   -2.0   -2.0   -2.0   -1.0   -1.0   -1.0
[ 57]   -1.0   -1.0   -1.0   -1.0   -1.0    0.0    0.0    0.0
[ 65]    0.0    0.0    0.0    0.0    0.0    0.0    1.0    1.0
[ 73]    1.0    1.0    1.0    1.0    1.0    1.0    1.0    1.0
[ 81]    1.0    2.0    2.0    2.0    2.0    2.0    2.0    2.0
[ 89]    2.0    2.0    2.0    2.0    2.0    2.0    2.0    2.0
...
...
[441]   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0
[449]   -1.0   -1.0   -1.0   -2.0   -2.0   -2.0   -2.0   -2.0
[457]   -2.0   -2.0   -2.0   -2.0   -3.0   -3.0   -3.0   -3.0
```

```
[465]   -3.0   -3.0   -3.0   -3.0   -4.0   -4.0   -4.0   -4.0
[473]   -4.0   -4.0   -5.0   -5.0   -5.0   -5.0   -5.0   -6.0
[481]   -6.0   -6.0   -6.0   -6.0   -7.0   -7.0   -7.0   -7.0
[489]   -8.0   -8.0   -8.0   -8.0   -9.0   -9.0   -9.0   -9.0
[497]  -10.0  -10.0  -10.0  -11.0  -11.0  -11.0  -11.0  -12.0
[505]  -12.0  -12.0  -12.0  -13.0  -13.0  -13.0  -13.0  -13.0

US              Unit: dB
[  1]  -34.0    N/A    N/A    N/A  -71.0  -61.0  -18.0   -8.0
[  9]    0.0    3.0    3.0    3.0    4.0    4.0    4.0    4.0
[ 17]    3.0    3.0    2.0    2.0    1.0    0.0   -1.0   -2.0
[ 25]   -3.0   -4.0   -5.0   -5.0   -6.0   -7.0   -8.0   -9.0
[ 33]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 41]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 49]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 57]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

Quiet Line Noise PSD ( QLN(f) )
DS              Unit: dB
[  1] -120.0 -140.0 -141.0 -141.0 -141.0 -141.0 -141.0 -141.0
[  9] -141.0 -141.0 -141.0 -141.0 -141.0 -141.0 -141.0 -141.0
[ 17] -141.0 -140.0 -140.0 -140.0 -139.0 -140.0 -140.0 -139.0
[ 25] -138.0 -138.0 -137.0 -136.0 -134.0 -134.0 -132.0 -130.0
[ 33] -129.0 -127.0 -125.0 -124.0 -124.0 -122.0 -121.0 -121.0
[ 41] -120.0 -119.0 -119.0 -118.0 -119.0 -119.0 -119.0 -119.0
[ 49] -119.0 -118.0 -119.0 -119.0 -118.0 -118.0 -118.0 -118.0
[ 57] -118.0 -118.0  -97.0 -117.0 -117.0 -117.0 -118.0 -118.0
[ 65] -118.0 -117.0 -117.0 -117.0 -117.0 -116.0 -117.0 -117.0
[ 73] -117.0 -117.0 -117.0 -117.0 -116.0 -116.0 -117.0 -117.0
[ 81] -117.0 -117.0 -117.0 -117.0 -117.0 -116.0 -117.0 -117.0
[ 89] -116.0 -116.0 -116.0 -116.0 -116.0 -116.0 -117.0 -116.0
...
...
[441] -113.0 -113.0 -114.0 -114.0 -113.0 -114.0 -114.0 -114.0
[449] -113.0 -114.0 -114.0 -114.0 -114.0 -113.0 -114.0 -114.0
[457] -113.0 -114.0 -114.0 -114.0 -114.0 -114.0 -114.0 -114.0
[465] -114.0 -114.0 -115.0 -115.0 -114.0 -114.0 -114.0 -114.0
[473] -115.0 -115.0 -114.0 -115.0 -114.0 -114.0 -114.0 -115.0
[481] -115.0 -115.0 -114.0 -114.0 -115.0 -115.0 -115.0 -114.0
[489] -116.0 -115.0 -115.0 -116.0 -115.0 -115.0 -115.0 -115.0
[497] -116.0 -116.0 -116.0 -115.0 -115.0 -115.0 -115.0 -115.0
[505] -115.0 -116.0 -115.0 -116.0 -116.0 -116.0 -116.0 -116.0

US              Unit: dB
[  1]    N/A -117.0 -118.0 -119.0 -118.0 -118.0 -117.0 -117.0
[  9] -113.0 -113.0 -114.0 -111.0 -114.0 -113.0 -113.0 -112.0
[ 17] -115.0 -115.0 -115.0 -113.0 -115.0 -116.0 -108.0 -113.0
[ 25] -116.0 -114.0 -115.0 -117.0 -116.0 -117.0 -117.0 -118.0
[ 33] -118.0 -118.0 -119.0 -119.0 -118.0 -118.0 -118.0 -118.0
[ 41] -119.0 -120.0 -118.0 -119.0 -118.0 -120.0 -120.0 -118.0
[ 49] -118.0 -118.0 -118.0 -118.0 -118.0 -119.0 -119.0 -118.0
[ 57] -119.0 -119.0 -118.0 -118.0 -118.0 -118.0 -118.0 -118.0

SNR(f)

DS              Unit: dB
[  1]    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
[  9]    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
[ 17]    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
[ 25]    0.0    0.0    0.0    0.0    0.0    0.0    0.0    0.0
[ 33]    0.0   31.0   32.0   32.0   34.0   35.0   36.0   38.0
[ 41]   40.0   41.0   43.0   44.0   45.0   46.0   48.0   49.0
[ 49]   50.0   52.0   52.0   53.0   54.0   54.0   56.0   57.0
[ 57]   57.0   57.0   44.0   58.0   59.0   59.0   58.0   59.0
[ 65]   60.0   59.0   60.0   60.0   60.0   60.0   60.0   61.0
[ 73]   61.0   61.0   61.0   61.0   61.0   61.0   62.0   61.0
[ 81]   61.0   61.0   61.0   61.0   61.0   61.0   61.0   61.0
[ 89]   61.0   61.0   62.0   61.0   61.0   61.0   61.0   61.0
```

```
...
...
[441]   55.0   55.0   55.0   54.0   55.0   55.0   55.0   54.0
[449]   55.0   55.0   54.0   55.0   54.0   54.0   54.0   54.0
[457]   54.0   54.0   54.0   54.0   54.0   54.0   54.0   53.0
[465]   54.0   53.0   54.0   53.0   54.0   53.0   53.0   53.0
[473]   53.0   53.0   53.0   52.0   53.0   52.0   53.0   52.0
[481]   52.0   52.0   51.0   51.0   52.0   51.0   51.0   51.0
[489]   50.0   50.0   50.0   50.0   49.0   49.0   49.0   48.0
[497]   48.0   46.0   45.0   43.0   43.0   42.0   42.0   41.0
[505]   41.0   38.0   38.0   38.0   37.0   32.0   32.0   25.0

US              Unit: dB
[  1]    N/A    N/A    N/A    N/A    N/A    N/A    N/A   30.0
[  9]   36.0   42.0   44.0   46.0   49.0   49.0   51.0   51.0
[ 17]   52.0   52.0   53.0   53.0   54.0   55.0   56.0   55.0
[ 25]   56.0   55.0   54.0   52.0   51.0   48.0   44.0   39.0
[ 33]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 41]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 49]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 57]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
```

It is suggested to view the graphical presentation of the DELT diagnosis via the NCT192 LCT or NCT192 client.

ADSL Link Monitoring

The ADSL link monitoring function provides the records of ADSL loop characteristics and Quite Line Noise (QLN) measured during the last training. It is noted that the measured results are only available in the show-time.

Enter to the "**diag**" group directory with "**portmon**" command to perform the ADSL link monitoring.

```
CLI# diag
CLI(diag)#
```

Table 9-7 shows the commands to configure ADSL link monitoring of NE. Example 107 shows the usage of its command as well as its related parameters.

Table 9-7 ADSL Link Monitoring

The following command is to start the link monitoring process on the specific ADSL line port.	
CLI(diag portmon)# start <*port-id*>	
The following command is to manually terminate the ADSL link monitoring process.	
CLI(diag portmon)# stop	
The following command is to view the ADSL loop charactertics	
CLI(diag portmon)# show	
Parameters	**Task**
<*port-id*>	Identify the port id of the system wish to perform the link monitoring, the define line port must operate in running status. **Type:** Mandatory **Valid values:** See the Section "Port Interface Indication" of Chapter 3.

Example 107 Display the ADSL loop charactertics (H(f)) and QLN

```
CLI(diag portmon)# start 1.6
```

```
OK

CLI(diag portmon)# show
Port monitor result:
Port  1. 6

H(f) logarithmic representation( Hlog(f) )
DS              Unit: dB
[  1]  -77.0  -37.0  -39.0  -41.0  -41.0  -43.0  -44.0  -44.0
[  9]  -47.0  -47.0  -46.0  -47.0  -43.0  -46.0  -44.0  -47.0
[ 17]  -44.0  -47.0  -53.0  -51.0  -48.0  -41.0  -45.0  -40.0
[ 25]  -37.0  -36.0  -32.0  -30.0  -28.0  -25.0  -23.0  -21.0
[ 33]  -19.0  -17.0  -15.0  -13.0  -11.0   -9.0   -7.0   -6.0
[ 41]   -5.0   -4.0   -4.0   -3.0   -3.0   -3.0   -2.0   -2.0
[ 49]   -2.0   -2.0   -2.0   -2.0   -2.0   -1.0   -1.0   -1.0
[ 57]   -1.0   -1.0   -1.0   -1.0   -1.0    0.0    0.0    0.0
[ 65]    0.0    0.0    0.0    0.0    0.0    0.0    1.0    1.0
[ 73]    1.0    1.0    1.0    1.0    1.0    1.0    1.0    1.0
[ 81]    1.0    2.0    2.0    2.0    2.0    2.0    2.0    2.0
[ 89]    2.0    2.0    2.0    2.0    2.0    2.0    2.0    2.0
...
...
[441]   -1.0   -1.0   -1.0   -2.0   -1.0   -2.0   -2.0   -2.0
[449]   -2.0   -2.0   -2.0   -2.0   -2.0   -2.0   -2.0   -2.0
[457]   -3.0   -3.0   -3.0   -3.0   -3.0   -3.0   -3.0   -3.0
[465]   -3.0   -4.0   -4.0   -4.0   -4.0   -4.0   -4.0   -4.0
[473]   -4.0   -4.0   -5.0   -5.0   -5.0   -5.0   -5.0   -5.0
[481]   -5.0   -5.0   -5.0   -6.0   -6.0   -6.0   -6.0   -6.0
[489]   -6.0   -6.0   -6.0   -7.0   -7.0   -7.0   -7.0   -7.0
[497]   -7.0   -7.0   -7.0   -7.0   -7.0   -7.0   -7.0   -8.0
[505]   -8.0   -8.0   -8.0   -8.0   -8.0   -8.0   -8.0   -8.0

US              Unit: dB
[  1]  -32.0    N/A    N/A  -68.0  -66.0  -59.0  -18.0   -8.0
[  9]    0.0    3.0    3.0    3.0    4.0    4.0    4.0    4.0
[ 17]    3.0    3.0    2.0    2.0    1.0    0.0   -1.0   -2.0
[ 25]   -3.0   -4.0   -5.0   -5.0   -6.0   -7.0   -8.0   -9.0
[ 33]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 41]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 49]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 57]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

Quiet Line Noise PSD ( QLN(f) )
DS              Unit: dB
[  1]  -54.0 -110.0 -124.0 -134.0 -133.0 -144.0 -146.0 -146.0
[  9]  -35.0  -35.0  -31.0  -35.0 -144.0  -30.0 -146.0  -35.0
[ 17] -146.0  -35.0  -63.0  -52.0  -38.0 -130.0  -23.0 -128.0
[ 25] -112.0 -107.0  -89.0  -78.0  -68.0  -54.0  -44.0  -33.0
[ 33] -149.0 -139.0 -128.0 -118.0 -109.0 -100.0  -92.0  -85.0
[ 41]  -80.0  -76.0  -73.0  -70.0  -69.0  -68.0  -67.0  -66.0
[ 49]  -65.0  -65.0  -64.0  -63.0  -63.0  -62.0  -61.0  -61.0
[ 57]  -60.0  -60.0  -59.0  -58.0  -58.0  -57.0  -57.0  -56.0
[ 65]  -55.0  -55.0  -54.0  -54.0  -53.0  -53.0  -52.0  -52.0
[ 73]  -51.0  -51.0  -50.0  -50.0  -49.0  -49.0  -48.0  -48.0
[ 81]  -48.0  -47.0  -47.0  -46.0  -46.0  -46.0  -46.0  -45.0
[ 89]  -45.0  -45.0  -45.0  -44.0  -44.0  -44.0  -44.0  -44.0
...
...
[441]  -61.0  -62.0  -62.0  -63.0  -62.0  -63.0  -63.0  -63.0
[449]  -64.0  -64.0  -65.0  -65.0  -66.0  -66.0  -67.0  -67.0
[457]  -68.0  -68.0  -69.0  -69.0  -70.0  -70.0  -71.0  -71.0
[465]  -72.0  -73.0  -73.0  -74.0  -74.0  -75.0  -75.0  -76.0
[473]  -77.0  -77.0  -78.0  -78.0  -79.0  -80.0  -80.0  -80.0
[481]  -81.0  -82.0  -82.0  -83.0  -84.0  -84.0  -85.0  -85.0
[489]  -86.0  -86.0  -87.0  -88.0  -88.0  -88.0  -89.0  -89.0
[497]  -90.0  -90.0  -91.0  -91.0  -92.0  -92.0  -92.0  -93.0
[505]  -93.0  -93.0  -93.0  -93.0  -94.0  -94.0  -94.0  -93.0
```

```
US              Unit: dB
[  1]  -86.0    N/A    N/A -140.0 -131.0  -95.0 -145.0  -93.0
[  9]  -53.0  -42.0  -40.0  -38.0  -36.0  -35.0  -35.0  -36.0
[ 17]  -38.0  -40.0  -44.0  -47.0  -51.0  -56.0  -61.0  -65.0
[ 25]  -69.0  -74.0  -78.0  -82.0  -87.0  -91.0  -95.0  -98.0
[ 33]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 41]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

[ 49]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 57]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

CLI(diag portmon)# stop
OK
CLI(diag portmon)# show
Port monitor result:
Port  1. 6

H(f) logarithmic representation( Hlog(f) )
DS              Unit: dB
[  1]  -77.0  -37.0  -39.0  -41.0  -41.0  -43.0  -44.0  -44.0
[  9]  -47.0  -47.0  -46.0  -47.0  -43.0  -46.0  -44.0  -47.0
[ 17]  -44.0  -47.0  -53.0  -51.0  -48.0  -41.0  -45.0  -40.0
[ 25]  -37.0  -36.0  -32.0  -30.0  -28.0  -25.0  -23.0  -21.0
[ 33]  -19.0  -17.0  -15.0  -13.0  -11.0   -9.0   -7.0   -6.0
[ 41]   -5.0   -4.0   -4.0   -3.0   -3.0   -3.0   -2.0   -2.0
[ 49]   -2.0   -2.0   -2.0   -2.0   -2.0   -1.0   -1.0   -1.0
[ 57]   -1.0   -1.0   -1.0   -1.0   -1.0    0.0    0.0    0.0
[ 65]    0.0    0.0    0.0    0.0    0.0    0.0    1.0    1.0
[ 73]    1.0    1.0    1.0    1.0    1.0    1.0    1.0    1.0
[ 81]    1.0    2.0    2.0    2.0    2.0    2.0    2.0    2.0
[ 89]    2.0    2.0    2.0    2.0    2.0    2.0    2.0    2.0
...
...
[441]   -1.0   -1.0   -1.0   -2.0   -1.0   -2.0   -2.0   -2.0
[449]   -2.0   -2.0   -2.0   -2.0   -2.0   -2.0   -2.0   -2.0
[457]   -3.0   -3.0   -3.0   -3.0   -3.0   -3.0   -3.0   -3.0
[465]   -3.0   -4.0   -4.0   -4.0   -4.0   -4.0   -4.0   -4.0
[473]   -4.0   -4.0   -5.0   -5.0   -5.0   -5.0   -5.0   -5.0
[481]   -5.0   -5.0   -5.0   -6.0   -6.0   -6.0   -6.0   -6.0
[489]   -6.0   -6.0   -6.0   -7.0   -7.0   -7.0   -7.0   -7.0
[497]   -7.0   -7.0   -7.0   -7.0   -7.0   -7.0   -7.0   -8.0
[505]   -8.0   -8.0   -8.0   -8.0   -8.0   -8.0   -8.0   -8.0

US              Unit: dB
[  1]  -32.0    N/A    N/A  -68.0  -66.0  -59.0  -18.0   -8.0
[  9]    0.0    3.0    3.0    3.0    4.0    4.0    4.0    4.0
[ 17]    3.0    3.0    2.0    2.0    1.0    0.0   -1.0   -2.0
[ 25]   -3.0   -4.0   -5.0   -5.0   -6.0   -7.0   -8.0   -9.0
[ 33]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 41]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 49]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 57]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A

Quiet Line Noise PSD ( QLN(f) )
DS              Unit: dB
[  1]  -54.0 -110.0 -124.0 -134.0 -133.0 -144.0 -146.0 -146.0
[  9]  -35.0  -35.0  -31.0  -35.0 -144.0  -30.0 -146.0  -35.0
[ 17] -146.0  -35.0  -63.0  -52.0  -38.0 -130.0  -23.0 -128.0
[ 25] -112.0 -107.0  -89.0  -78.0  -68.0  -54.0  -44.0  -33.0
[ 33] -149.0 -139.0 -128.0 -118.0 -109.0 -100.0  -92.0  -85.0
[ 41]  -80.0  -76.0  -73.0  -70.0  -69.0  -68.0  -67.0  -66.0
[ 49]  -65.0  -65.0  -64.0  -63.0  -63.0  -62.0  -61.0  -61.0
[ 57]  -60.0  -60.0  -59.0  -58.0  -58.0  -57.0  -57.0  -56.0
[ 65]  -55.0  -55.0  -54.0  -54.0  -53.0  -53.0  -52.0  -52.0
[ 73]  -51.0  -51.0  -50.0  -50.0  -49.0  -49.0  -48.0  -48.0
[ 81]  -48.0  -47.0  -47.0  -46.0  -46.0  -46.0  -46.0  -45.0
[ 89]  -45.0  -45.0  -45.0  -44.0  -44.0  -44.0  -44.0  -44.0
...
```

```
...
[441]  -61.0  -62.0  -62.0  -63.0  -62.0  -63.0  -63.0  -63.0
[449]  -64.0  -64.0  -65.0  -65.0  -66.0  -66.0  -67.0  -67.0
[457]  -68.0  -68.0  -69.0  -69.0  -70.0  -70.0  -71.0  -71.0
[465]  -72.0  -73.0  -73.0  -74.0  -74.0  -75.0  -75.0  -76.0
[473]  -77.0  -77.0  -78.0  -78.0  -79.0  -80.0  -80.0  -80.0
[481]  -81.0  -82.0  -82.0  -83.0  -84.0  -84.0  -85.0  -85.0
[489]  -86.0  -86.0  -87.0  -88.0  -88.0  -88.0  -89.0  -89.0
[497]  -90.0  -90.0  -91.0  -91.0  -92.0  -92.0  -92.0  -93.0
[505]  -93.0  -93.0  -93.0  -93.0  -94.0  -94.0  -94.0  -93.0

US              Unit: dB
[  1]  -86.0    N/A    N/A -140.0 -131.0  -95.0 -145.0  -93.0
[  9]  -53.0  -42.0  -40.0  -38.0  -36.0  -35.0  -35.0  -36.0
[ 17]  -38.0  -40.0  -44.0  -47.0  -51.0  -56.0  -61.0  -65.0
[ 25]  -69.0  -74.0  -78.0  -82.0  -87.0  -91.0  -95.0  -98.0
[ 33]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 41]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 49]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
[ 57]    N/A    N/A    N/A    N/A    N/A    N/A    N/A    N/A
```

It is suggested to view the graphical presentation of the ADSL loop characteristics and QLN via the NCT192 LCT or NCT192 client.

Loop SELT Test (Single End Loop Test)

The SELT loop function diagnosis function is to estimate the distance of the DSL connection from the NE to the subscriber's location without connecting a subscriber device.

Enter to the "**diag**" group directory with "**selt**" command to perform the SELT link monitoring.

```
CLI# diag selt
CLI(diag selt)#
```

Table 9-8 shows the commands to configure SELT link monitoring of NE. Example 108 shows the usage of its command as well as its related parameters.

Table 9-8 SELT Link Monitoring

The following command is to start the SELT process on the specific ADSL line port.	
CLI(diag selt)# start <*port-id*>	
The following command is to view the SELT result.	
CLI(diag selt)# show	
Parameters	**Task**
<*port-id*>	Identify the port id of the system wish to perform the link monitoring, the define line port must operate in running status. **Valid values:** See the Section "Port Interface Indication" of Chapter 3.

Example 108 Diagnosing the run-time ADSL line port loop performance

```
CLI(diag selt)# start 1.6
OK: But the result displays by diag selt show.

CLI(diag selt)# show

Port single end loop test result: Port  1. 6


    Cable Type: 24 AWG
```

```
Loop Length: 13468 (ft.)
```

Please refer to ITU-T 992.3 for the details of SELT.

Network Ping Test

The "**ping**" command is a very common method for troubleshooting the accessibility of devices. It uses a series of ICMP (Internet Control Message Protocol) Echo messages to determine if the NE can reach the target or not.

To diagnose the remote hosts using the "ping" command at the prompt for CLI#. (From UGE or MGE)

Table 9-9 shows the commands to set network ping test. Example 109 shows the usage of its command as well as its related parameters.

Table 9-9 Network Ping Test

The following command is to send the ICMP Echo message to target host.	
CLI# ping <*hostname*>	
Parameters	**Task**
<*hostname*>	Defines IP address or hostname of the target host to reply ICMP Echo message. **Type:** Mandatory **Valid values:** 0.0.0.0 ~ 255.255.255.255 | string

Example 109 Using Ping command to test the remote host status

```
CLI# ping 192.168.192.1

192.168.192.1 PING Statistics: 5 packets transmitted, 5 packets received
```

Monitoring the System Environment

In the hardware monitoring list dialog, you can monitor the temperature and voltage status of any specific card module.

Enter to the "**status**" group directory with proper command to perform the system environment monitoring.

```
CLI# status
CLI(status)#
```

Table 9-10 shows the commands to display the system environment monitoring.Example 110 shows the usage of its command as well as its related parameters.

Table 9-10 System Environment Monitoring

The following command is to display the system ventilation fan speed information.
CLI(status)# fanspeed show
The following command is to display the temperature of specific line card.
CLI(status)# temp show lc <*lc-id*>
The following command is to display the temperature of network card.
CLI(status)# temp show nc
The following command is to display the voltage of fan module.
CLI(status)# voltage show fan
The following command is to display the voltage of specific line card.
CLI(status)# voltage show lc <*lc-id*>
The following command is to display the voltage of network card.
CLI(status)# voltage show nc

Parameters	Task
<*lc-id*>	Identify the slot range of the line card **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.

Example 110 Display the performance monitor of the system environment

```
CLI(status)# fanspeed show

    fan  fan speed (rpm)      fan status
    ---  ----------------  -------------------
      1             4428  FAILED (2880~4320)
      2             4551  FAILED (2880~4320)


CLI(status)# temp show lc 1
Temperature of LC 1 (centigrade)
          sensor          temperature  threshold-high  threshold-low
    ----------------------  -----------  --------------  -------------
    sensor1 (g767 local )           43              95              5
    sensor2 (g767 remote)           41              95              5
    sensor3 (max6652 #1 )           37              95              -
    sensor4 (max6652 #1 )           34              95              -


CLI(status)# temp show nc
Temperature of network card 1 (centigrade).
          sensor          temperature  threshold-high  threshold-low
    ----------------------  -----------  --------------  -------------
    sensor1 (g767 local )           40              95              5
    sensor2 (g767 remote)           35              95              5
    sensor3 (max6652 #1 )           35              95              -


CLI(status)# voltage show fan

    fan tray (5V)     : 4.97 V
    low threshold     : 4.00 V
    high threshold    : 5.00 V


CLI(status)# voltage show lc 1
```

```
LC 1
    voltage of the first max6652
             item        voltage  threshold-high  threshold-low
        ---------------  -------  --------------  -------------
        voltage (1.2 V)     1.17            1.31           1.08
        voltage (12  V)    11.78           13.19          10.88
        voltage (1.8 V)     1.77            1.98           1.63
        voltage (3.2 V)     3.15            3.51           2.89
    voltage of the second max6652
             item        voltage  threshold-high  threshold-low
        ---------------  -------  --------------  -------------
        voltage (1.5 V)     1.47            1.64           1.35
        voltage ( 0  V)     0.00            0.00           0.00
        voltage (2.5 V)     2.49            2.75           2.27
        voltage (3.2 V)     3.15            3.51           2.89


CLI(status)# voltage show nc
Voltage of network card 1
          item        voltage  threshold-high  threshold-low
    ---------------  -------  --------------  -------------
    voltage (1.25V)     1.22            1.36           1.13
    voltage (2.5 V)     2.48            2.75           2.25
    voltage (1.8 V)     1.77            1.98           1.63
    voltage (3.3 V)     3.28            3.61           2.99
```

Monitoring the System Performance

Enter to the "**status**" group directory with proper command to perform the system environment monitoring.

```
CLI# status
CLI(status)#
```

Table 9-11 shows the commands to display the system performance parameters.Example 111 shows the usage of its command as well as its related parameters.

Table 9-11 System Performance Monitoring

The following command is to show adsl line historical performance data (15 minutes per interval).
CLI(status)# perf show history-15-min <*port-id*> <*start-interval*>
The following command is to show adsl line historical performance data (1day per interval).
CLI(status)# perf show history-1-day <*port-id*>
The following command is to show those VLANs on specific line cards that currently are allowed to forward broadcast packets.
CLI(status)# broadcast dsfilter show [<*slot-range*>]
The following command is to display LACP status.
CLI(status)# lacp show
The following command is to display line card status.
CLI(status)# lcstatus show
The following command is to display RSTP status.
CLI(status)# rstp show [*bridge* | *uge*]
The following command is to display the system up time.
CLI(status)# time show

Parameters	Task
<*port-id*>	Identify the port id of the system wish to perform the link monitoring, the define line port must operate in running status. **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.
<*start-interval*>	This specifies the adsl line historical performance data (15 minutes per interval). **Type:** Mandatory **Valid values:** 1 ~ 96
<*slot-range*>	Identify the slot range of the line card **Type:** Mandatory **Valid values:** See the Section “Port Interface Indication” of Chapter 3.
[*bridge* | *uge*]	This specifies the Rapid Spanning Tree Protocol status **Type:** Mandatory **Valid value:** bridge, uge

Example 111 Display the performance monitor of the system

```
CLI(status)# perf show history-15-min 1.6 5
Port: 1.6  interval: 5/96
      rxCells:         0   txCells:         0

               Near End   Far End
              ---------- ----------
          UAS          0          0
         LOFs          0          0
         LOSs          0          0
         LPRs          0          0
           ES          0          0
          SES          0          0
           CV          0          0
        INITs          0      -----
    FailINITs          0      -----

Port: 1.6  interval: 6/96
      rxCells:         0   txCells:         0

               Near End   Far End
```

```
                 ---------- ----------
            UAS          0          0
           LOFs          0          0
           LOSs          0          0
           LPRs          0          0
             ES          0          0
            SES          0          0
             CV          0          0
          INITs          0       ----
     FailINITs          0       ----

Port: 1.6  interval: 7/96
       rxCells:          0   txCells:          0

                 Near End   Far End
                 ---------- ----------
            UAS          0          0
           LOFs          0          0
           LOSs          0          0
           LPRs          0          0
             ES          0          0
            SES          0          0
             CV          0          0
          INITs          0       ----
     FailINITs          0       ----

Port: 1.6  interval: 8/96
       rxCells:          0   txCells:          0

                 Near End   Far End
                 ---------- ----------
            UAS          0          0
           LOFs          0          0
           LOSs          0          0
           LPRs          0          0
             ES          0          0
            SES          0          0
             CV          0          0
          INITs          0       ----
     FailINITs          0       ----

CLI(status)# broadcast dsfilter show 1
Down stream broadcast filters
    No any filter.


CLI(status)# lacp show

    LACP                 : disabled


CLI(status)# lcstatus show

Line card status
    LC  type     status
    --  -----  -----------
     1   ADSL      active
     2  SHDSL      active
     3   ADSL      active
     4   ADSL      active


CLI(status)# rstp show

[bridge]
    oper status                      : disabled
    force version                    : RSTP
    bridge ID                        : 0x8000-00:60:64:dc:7a:17
```

```
    bridge priority                  : 32768
    bridge hello time                : 2 sec
    bridge forward delay             : 15 sec
    bridge max age                   : 20 sec
    bridge message age               : 0 sec
    bridge Tx hold count             : 3
    root path cost                   : 0
    root port ID                     : 0x0000
    root bridge ID                   : 0x8000-00:60:64:dc:7a:17
    root bridge priority             : 0x8000
    topology change count            : 0
    time since last topology change  : 0 sec
    root hello time                  : 2 sec
    root forward delay               : 15 sec
    root max age                     : 20 sec
    designated bridge ID             : 0x8000-00:60:64:dc:7a:17
    designated port ID               : 0x0000


[UGE 1]
    STP admin status                 : enabled
    STP oper status                  : enabled
    port ID                          : 0x8001
    port priority                    : 128
    STP state                        : broken
    role                             : disabled
    admin path cost                  : 0 (default)
    oper path cost                   : 20000
    admin non-STP                    : no
    admin edge port                  : no
    oper edge port                   : no
    admin P2P MAC                    : auto
    oper P2P MAC                     : yes
    send RSTP BPDU                   : yes
    mcheck                           : no
    root bridge ID                   : 0x8000-00:60:64:dc:7a:17
    root bridge priority             : 0x8000
    root hello time                  : 2 sec
    root forward delay               : 15 sec
    root max age                     : 20 sec
    designated bridge ID             : 0x8000-00:60:64:dc:7a:17
    designated port ID               : 0x8001


CLI(status)# time show

    system uptime      : 120:56:43
    system datetime    : 2007-10-31 11:08:42 GMT+8
```

Appendix A Abbreviations and Acronyms

The abbreviations and acronyms used in this document.

Table A-1 Abbreviations and Acronyms Table

Abbreviations	Full Name
AAL	ATM Adaptation Layer
ADSL	Asymmetric Digital Subscriber line
ATM	Asynchronous Transfer Mode
ATU-C	ADSL Transceiver Unit at the central office end
ATU-R	ADSL Transceiver Unit at the remote end
CV	Coding Violation
DSCP	Differentiated Service Code Point
DSLAM	Digital Subscriber line Access Multiplexer
ES	Error Seconds
EOA	Ethernet over ATM
GBIC	Gigabit Interface Converter
GE	Gigabit Ethernet
IP	Internet Protocol
LAN	Local Area Network
LOF	Loss of Frame
LOS	Loss of Signal
LPR	Loss of Power
OAM	Operation, Administration, and Maintenance
PSD	Power Spectral Density
PVC	Permanent Virtual Channel
SFP	Small Form Pluggable
SNR	Signal-to Noise Ratio
SNMP	Simple Network Management Protocol
UAS	Unavailable Seconds
UBR	Unspecified Bit Rate
VC	Virtual Channel
VCI	Virtual Channel Identify
VCL	Virtual Channel Link
VLAN	Virtual Local Area Network
VP	Virtual Path
VPI	Virtual Path Identifier
WAN	Wide Area Network
xDSL	ADSL/SHDSL

This page is leave in blank for note or memo use

Appendix B Alarm Definition

Table B-1 Alarm Definition

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
All	noEntity	EMPTY	No	Neither plan type nor on-line type configured
NCT192	CPU Module	MISSING	Major	CPU Module is off-line
		TEMP	Major	Temperature is over the threshold
		VOL	Major	Voltage is below the threshold
		MISMATCH	Major	Planned type and online type are mismatched
		TCA_DHCP_BC	Warning	DHCP broadcast request rate threshold-crossing alert
	ADSL Module	MISSING	Major	ADSL module is off-line
		TEMP	Major	Temperature is over the threshold
		VOL	Major	Voltage is below the threshold
		MISMATCH	Major	Planned type and online type are mismatched
		NOT_OPERABLE	Major	ADSL line card is not operable
	Power Module	MISSING	Major	Power module is off-line
		NOT_OPERABLE	Major	Power card is not operable
	Fan Module	MISSING	Major	Fan module is off-line
		FAN1_SPEED	Major	Fan1 speed is below the threshold
		FAN2_SPEED	Major	Fan2 speed is below the threshold
		VOL	Major	Voltage is below the threshold
	ADSL Port	ES_NE_15_MIN	Minor	15 min near end ES is over threshold
		SES_NE_15_MIN	Minor	15 min near end SES is over threshold
		UAS_NE_15_MIN	Minor	15 min near end UAS is over threshold
		ES_FE_15_MIN	Minor	15 min far end ES is over threshold
		SES_FE_15_MIN	Minor	15 min far end SES is over threshold
		UAS_FE_15_MIN	Minor	15 min far end UAS is over threshold
		ES_NE_1_DAY	Minor	1 day near end ES is over threshold
		SES_NE_1_DAY	Minor	1 day near end SES is over threshold
		UAS_NE_1_DAY	Minor	1 day near end UAS is over threshold
		ES_FE_1_DAY	Minor	1 day far end ES is over threshold
		SES_FE_1_DAY	Minor	1 day far end SES is over threshold
		UAS_FE_1_DAY	Minor	1 day far end UAS is over threshold
		LOS	Minor	Loss of signal
		LOF	Minor	Loss of frame
		LPWR	Warning	CPE loss of power
		GEN_LINE_INIT_FAIL	Minor	Generic line initialization failure
		CONFIG_ERROR	Minor	Line initialization failure - configuration error
		HIGH_BIT_RATE	Minor	Line initialization failure - high bit rate
		COMM_PROBLEM	Minor	Line initialization failure - communication problem
		NO_PEER_DETECTED	Minor	No peer detected
		TRAINING	Warning	Port is under training
		NO_CONFIG	Information	Port is not configured
		PS_L2_MANUAL	Information	ADSL2/ADSL2+ Power State transfers to L2 by manual mode

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
NCT192	ADSL Port	PS_L2_AUTO	Information	ADSL2/ADSL2+ Power State transfers to L2 by automatic mode
		PS_L3_CO	Information	ADSL2/ADSL2+ Power State transfers to L3 by CO side
		PS_L3_CPE	Information	ADSL2/ADSL2+ Power State transfers to L3 by CPE side
		ILLEGAL_IP	Warning	Packets with illegal IP addresses have been dropped
		ILLEGAL_MAC	Warning	duplicated MAC addresses from different line ports are made out
		DISABLED	Information	The port is disabled
	GE Port	MISSING	Major	GE Port is off-line
		NOT_OPERABLE	Major	GE Port is not operable
		STP_LEARN	Information	GE port is transited to STP-learning state
		STP_BLOCK	Information	GE port is transited to STP-blocking state
		DISABLED	Information	GE port is disabled
	Alarm Relay Module	MISSING	Major	Alarm relay module is off-line
	Alarm Relay Port	MISSING	Major	Alarm relay port is off-line
		RELAY_ABNORMAL	Major	The alarm relay port is under abnormal status
		DISABLED	Information	The alarm repay port is disabled
	SHDSL Module	MISSING	Major	SHDSL module is off-line
		TEMP	Major	Temperature is over the threshold
		VOL	Major	Voltage is below the threshold
		MISMATCH	Major	Planned type and online type are mismatched
		NOT_OPERABLE	Major	Line card is not operable
	SHDSL Port	TCA_ES_NE_15_MIN	Minor	15-min near end ES is over the threshold
		TCA_SES_NE_15_MIN	Minor	15-min near end SES is over the threshold
		TCA_UAS_NE_15_MIN	Minor	15-min near end UAS is over the threshold
		TCA_CRC_NE_15MIN	Minor	15-min near end CRC is over the threshold
		TCA_LOSW_NE_15MIN	Minor	15-min near end LOSW is over the threshold
		TCA_SNR_NE	Minor	Near end SNR margin is over the threshold
		TCA_ATTN_NE	Minor	Near end loop attenuation is over the threshold
		OPI	Information	Operation state change indication
		LOS	Minor	Loss of signal (FOH lost bit)
		SEGA	Minor	Segment anomaly - CRC anomaly (FOH sega bit)
		LPR	Minor	Loss of power - power status (FOH ps bit)
		SEGD	Minor	Segment defect - LOSW defect (FOH segd bit)
		PBO_NE	Minor	Near end enhanced power back off
		DEVFAULT_NE	Minor	Near end device fault - Diagnostic or self-test fault
		DCCONT_NE	Minor	Near end DC continuity fault - interfere with span powering
		LOSW_NE	Minor	Near end LOSW failure
		INI_CFG_NE	Minor	Near end indicates Far end not able to support requested configuration
		INI_PROTOCOL_NE	Minor	Near end indicates incompatible protocol used by Far end
		NOPEER	Minor	No peer detected
		PBO_FE	Minor	Far end enhanced power back off
		DEVFAULT_FE	Minor	Far end device fault - Diagnostic or self-test fault
		DCCONT_FE	Minor	Far end DC continuity fault - interfere with span powering

NE Model	Module Name	Alarm Name	Default Severity	Alarm Description
NCT192	SHDSL Port	LOSW_FE	Minor	Far end LOSW failure
		INI_CFG_FE	Minor	Far end indicates Near end not able to support requested configuration
		INI_PROTOCOL_FE	Minor	Far end indicates incompatible protocol used by Near end
		DISABLED	Information	The port is disabled

Appendix C: Legal & Regulatory Information

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

- Change the direction or relocate the receiving antenna.
- Increase the separation between this equipment and the receiver.
- Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
- Consult an experienced radio/TV technician for help.

(3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.

6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at

www.netcomm.com.au

NetComm®
www.netcomm.com.au

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website **www.netcomm.com.au**.

Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

Note: NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.

NetComm®
www.netcomm.com.au

NETCOMM LIMITED PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: sales@netcomm.com.au **W:** www.netcomm.com.au

Dynalink
www.dynalink.co.nz

DYNALINK NZ 224b Bush Road, Albany, Auckland, New Zealand
P: 09 448 5548 **F:** 09 448 5549
E: sales@dynalink.co.nz **W:** www.dynalink.co.nz