ADLINK Software for Networking Configuration Guide

Manual Revision: 1.4
Revision Date: May 24, 2016
Part Number: 50-1G026-1000

Advance Technologies; Automate the World.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Revision History

Rev	Date	Description
1.0	09/07/2014	Preliminary release
1.1	10/30/2014	Initial release
1.2	12/13/2015	Add SNMP feature
1.3	5/6/2016	Add DHCP and event log features
1.4	5/24/2016	Add cPCI support

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Preface

Copyright 2014 ADLINK Technology, Inc.

This document contains proprietary information protected by copyright. All rights are reserved. No part of this manual may be reproduced by any mechanical, electronic, or other means in any form without prior written permission of the manufacturer.

Disclaimer

The information in this document is subject to change without prior notice in order to improve reliability, design, and function and does not represent a commitment on the part of the manufacturer. In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the product or documentation, even if advised of the possibility of such damages.

Environmental Responsibility

ADLINK is committed to fulfill its social responsibility to global environmental preservation through compliance with the European Union's Restriction of Hazardous Substances (RoHS) directive and Waste Electrical and Electronic Equipment (WEEE) directive. Environmental protection is a top priority for ADLINK. We have enforced measures to ensure that our products, manufacturing processes, components, and raw materials have as little impact on the environment as possible. When products are at their end of life, our customers are encouraged to dispose of them in accordance with the product disposal and/or recovery programs prescribed by their nation or company.

Trademarks

Product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Table of Contents

Revision History **1**

Preface **3**

Table of Contents **4**

1 Scope **6**

1.1 Manual Scope 6

1.2 Audience 6

2 Introduction **6**

3 Command Line Interface (CLI) **7**

4 Login **8**

5 Installation and upgrade **10**

6 Configuration **11**

6.1 View Mode 11

6.1.1 Get Help 11

6.1.2 Enter Configure Mode 12

6.1.3 Exit ADSN Shell 12

6.1.4 Show System Information 12

6.2 Configure Mode 14

6.2.1 Get Help 15

6.2.2 Exit Current Mode 16

6.2.3 Clear Configuration 17

6.2.4 Restore 17

6.2.5 Command List 17

6.2.6 Negate Command 18

6.2.7 Password 18

6.2.8 Check Network Connectivity 19

6.2.9 Show Current System Information 19

6.2.10 Save Configuration 20

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.11 Port Configuration 21
6.2.12 Port Mirror Configuration 22
6.2.13 IP Configuration 22
6.2.14 ACL Configuration 23
6.2.15 L2 Configuration 25
6.2.16 xSTP Configuration 26
6.2.17 Route Configuration 27
6.2.18 Trunk Configuration 28
6.2.19 VLAN Configuration 29
6.2.20 IGMP Snooping Configuration 30
6.2.21 IGMP Proxy Configuration 30
6.2.22 Quality of Service Configuration 32
6.2.23 LACP Configuration 33
6.2.24 LLDP Configuration 33
6.2.25 SNMP Configuration 35
6.2.26 DHCP Configuration 37
6.2.27 Event log Configuration 39
Glossary 41

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

1 Scope

1.1 Manual Scope

Administrators and users of the ADSN Platform can manage and monitor the network via the Command Line Interface (CLI), either through a TELNET connection or by direct access through a serial port on the ADSN system blade.
This ADLINK Software for Networking Configuration Guide documents the commands used to configure the ADSN equipment and to monitor traffic and events.

1.2 Audience

This manual is intended for:

- Technical staff responsible for the configuration, provisioning, and management of network devices and services;
- Network operations center personnel who manage and monitor ADSN equipment alarms and events.

The document assumes that users of ADSN equipment are familiar with CLIs in general and particularly with network management software and telecom equipment and terminology.

2 Introduction

This guide describes how to use ADLINK Software for Networking on ADLINK blades, such as the aTCA-3420, aTCA-N700, aTCA-3710 and cPCI-6S10.
All the commands listed in this document are configured using the following hardware architecture, shown in Figure 1. In this figure, the client is running on a standalone server. However, it also can run on the LMP on the blade.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

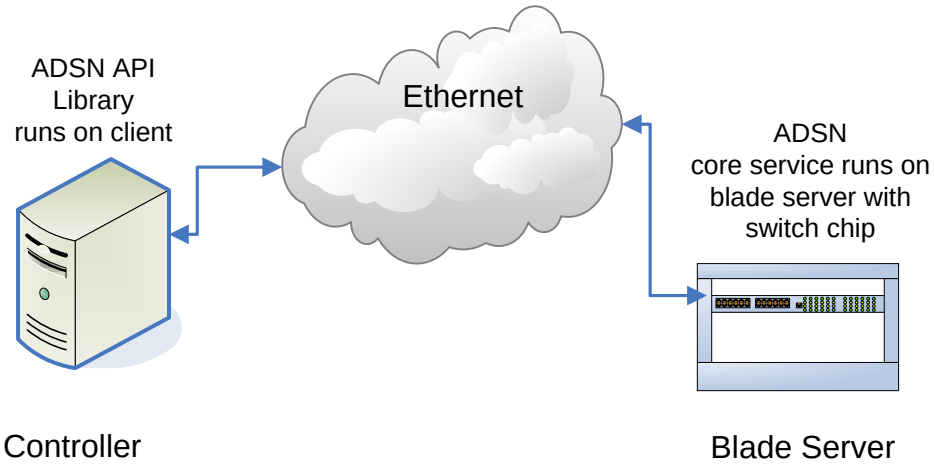


Figure 1. Hardware Architecture for Configuration

The ADSN provides two modes for users to configure the switch blade: View Mode and Configure Mode. Users have limited privileges in View Mode and can only read system information and version. They don't have privileges to configure the system. Users have higher privileges in Configure Mode than View Mode and not only have reading rights but also writing privileges. They can configure VLAN, TRUNK, ACL and other functions in Configure Mode to meet their requirements.

Since the ADSN almost has the same features in different ADLINK hardware platform. We use the blade aTCA-3710 and cPCI 6S10 as the example. The differences of features and configurations between aTCA and cPCI products are also provided to help you to apply software functions in different hardware platforms. If there is no special instruction, The hardware platform is aTCA-3710 in this document.

Some features may not support to all aTCA and cPCI products for different level of processor computing power. Contact ADLINK for assistance for specific application requirements.

3 Command Line Interface (CLI)

The ADSN platform is driven by the ADLINK Software for Networking System and supports a utility program that enables remote network management, including object configuration and service provisioning. The utility program uses a Command Line Interface (CLI) to communicate with the platform. The CLI documented in this Configuration Guide supports the ADSN system.

The Command Line Interface is organized into a number of command modes and sub_modes where related functions are grouped in a hierarchical tree structure. System maintenance and configuration commands are reserved for users with administrator privileges, while users with lower access levels can only perform provisioning tasks or view statistics and status information.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4 Login

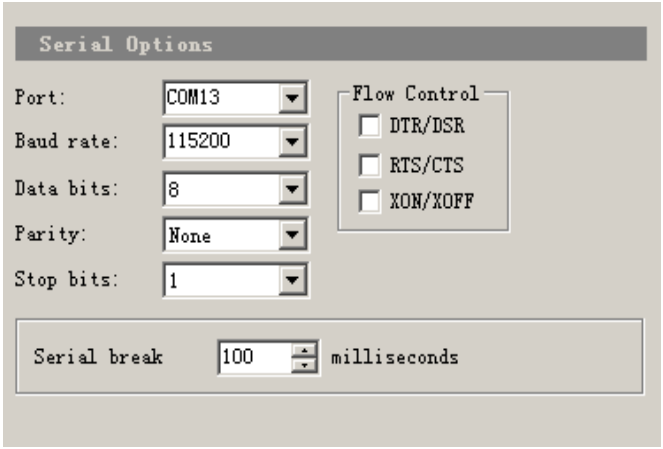
Following initial configuration and after the connection to the LAN is established, you can log in to the system IP address via TELNET and use the CLI to execute remote platform management and service provisioning.

Serial Port Connection To The Blade

For serial port connection to the ADSN blade, a DB-9 cable assembly is required. Connect the DB9 cable to the serial port on the blade. To connect to the system using the serial port:

1. Launch the terminal emulation program (for example, HyperTerminal) on the Craft terminal.
2. Configure the COM port as follows:

   115200 bps
   8 data bits
   1 stop bit
   no parity
   no flow control



3. Press <Enter>, then type the user name and password as prompted.

Note:

Both login user name and password are casesensitive. If you are logging on for the first time, type the default user name (root) and password (root).

TELNET Connection From the LMP

After entering the LMP OS, run the ADSN with the command ***cli***. First, you will enter View Mode.

```
[root@aTCA-3710~]# cli
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
ADLINK>
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

To enter Configure Mode use the command *enable* and default password ***adlink***. The display will not echo the password. After entering Configure Mode successfully, the prompt will change from ">" to "#".

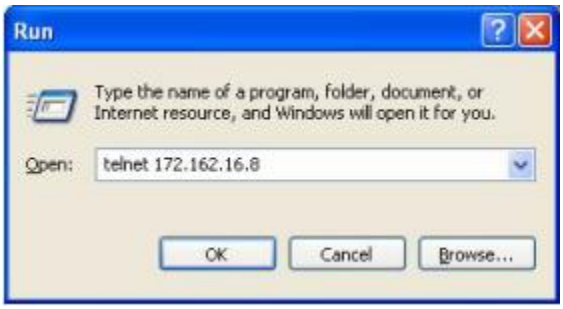
```
ADLINK> enable
Password:
ADLINK#
```

TELNET Connection From Remote Server

The following example illustrates a TELNET connection provided by Microsoft Windows.

Alternatively, you can use any TELNET application. To open a CLI session using TELNET:

1. Click the Windows Start button and select Run.
2. Type telnet and the system IP address assigned to the blade. For example, telnet 172.162.16.8.



3. Click OK to open a command line window.
4. Type your user name and password as prompted. If you are logging on for the first time, use the default user name and password (root and root).

Note:

The passwords you enter do NOT echo on the screen.

Note:

The#line indicates that the following items are sub commands. In this example, (config)# indicates that all the subsequent items are submode level commands to the config mode.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

5 Installation and upgrade

The following procedure is for ADSN installation on an ADLINK aTCA and cPCI blade.

1. Transfer the file " ADSN_3710_V1.1_s.xxx " to the blade and extract it.

```
[root@aTCA-3710:/home]# ls
ADSN_3710_V1.1_s.690.tar.gz
[root@aTCA-3710:/homeaTCA-3710]# tar -xzvf ADSN_3710_V1.1_s.690.tar.gz
```

2. Run the script “install.sh” to install the ADSN.

```
[root@aTCA-3710:/home]# cd ADSN_3710_V1.1_s.690

[root@aTCA-3710:/home/ ADSN_3710_V1.1_s.690]# ./install.sh
Old start-up config will be cleared. Please make sure that it has been backuped!
Continue to install? (y/n): y
Stoping Broadcom Switch Software .OK
Begin to install...
Starting Broadcom Switch Software ..... OK
```

Note:
We could add permissions to the software folder before beginning the installation if the permission denied alarm is raised.
[root@aTCA-3710:/home]# chmod -R 777 ADSN_3710_V1.1_s.xxx.tar.gz

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6 Configuration

This chapter describes the features of the ADSN, and guides you through the software configuration procedures. Configuration examples are also provided to help you to apply software features to different network scenarios.

6.1 View Mode

View Mode provides limited right for users. Users can only read system information and version. They don't have writing privileges.

The following commands are available in View Mode.

Command	Description
enable	Turn on Configure Mode command
quit	Exit ADSN shell
show	Show system information

6.1.1 Get Help

Entering a question mark (?) at the system prompt displays a list of commands or Sub commands available for the current command mode. You can also type a "?" in the middle of a command line to view the list of valid arguments or parameters needed to complete the command.

The following commands are available for getting help.

Command	Description
?	Show all commands available under the current command mode. Can be used as a command string input hint.

Note:

The question mark (?) you enter is a no display character; it does not show on the command line.

Example

Show all available commands in this mode.

```
ADLINK> ?
  enable   Turn on privileged mode command
  quit     Leave switch manager shell
  show     Show running system information
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.1.2 Enter Configure Mode

The following command allows you to enter Configure Mode.

Command	Description
enable	Turn on privileged mode command.

Example

Turn on privileged mode, and enter ***adlink***

```
ADLINK> enable
Password:
ADLINK#
```

6.1.3 Exit ADSN Shell

The following command allows you to exit the ADSN.

Command	Description
quit	Leave ADSN shell (in View Mode)

Example

Leave the ADSN shell.

```
ADLINK> quit
Connection closed by foreign host.
[root@aTCA-3710 ~]#
```

6.1.4 Show System Information

The following commands are available for displaying system information.

Command	Description
show system	Show brief system information
show version	Show the version information

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Example

Show brief system information and version information.

```
ADLINK> show system
Device ID                    : 18
Manufacturer ID              : 24339
Manufacturer Name            : name (0x5F13)
Product ID                   : 1792 (0x0700)
Product Name                 : name (0x700)
Device Available             : yes
Provides Device SDRs         : yes
Fabric Port Number           : 1 - 26
```

```
ADLINK> show version
OS version                   : Linux aTCA-3710 3.0.48-rt70-gdd5a5aa #6 SMP Wed Apr 3 12:08:34 HKT 2013 ppc GNU/Linux
Device Revision              : 0
Firmware Revision            : 1.0
IPMI Version                 : 2.0
ADLINK sdk Version           : 1.0.0
Build on:Jun 19 2013 11:35:18
Copyright 2012, ADLINK TECHNOLOGY Inc.
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2 Configure Mode

Configure Mode provides more privileges than View Mode. Users can configure VLAN, TRUNK, ACL and other functions in Configure Mode to meet their requirements.

The following commands are available in aTCA configure mode.

Command	Description
clear	Clear functions
exit	Exit current mode and return to the previous mode
restore	Reset start-up configuration to factory default
list	Print command list
no	Negate a command or set its defaults
password	Assign the privileged level password
ping	Send count echo messages
show	Show current system information
write	Write current configuration to start-up configuration file
quit	Leave switch manager shell
acl	ACL
port	Port subsystem
route	Route
trunk	Trunk group setting
vlan	VLAN subsystem
qos	QoS
spanning-tree	spanning tree
vrrp	vrrp configuration
ip	IP information
l2	Layer-2 subsystem
lldp	lldp command
igmp-snooping	IGMP Snooping command
igmp-proxy	IGMP proxy service configure

The following commands are available in cPCI configure mode.

Command	Description
clear	Clear functions
exit	Exit current mode and return to the previous mode
restore	Reset start-up configuration to factory default
list	Print command list
no	Negate a command or set its defaults
password	Assign the privileged level password

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

ping	Send count echo messages
show	Show current system information
write	Write current configuration to start-up configuration file
quit	Leave switch manager shell
acl	ACL
port	Port subsystem
route	Route
trunk	Trunk group setting
vlan	VLAN subsystem
qos	QoS
stp	spanning tree subsystem
ip	IP information
l2	Layer-2 subsystem

6.2.1 Get Help

The following command allows you to get help.

Command	Description
?	Show all available commands on this mode.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Example

Show all available commands on this mode for aTCA.

```
ADLINK# ?
  acl         ACL
  clear       Clear functions
  diag        Enter into diagnostic mode
  exit        Exit current mode and down to previous mode
  ip          IP information
  l2          Layer-2 subsystem
  list        Print command list
  no          Negate a command or set its defaults
  password    Assign the privileged level password
  ping        send count echo messages
  port        Port subsystem
  restore     Reset start-up configuration to factory default. Never try unless you know the
meaning!
  route       route
  show        how running system information
  trunk       Trunk group setting
  vlan        VLAN subsystem
  write       Write running configuration to start-up configuration file
```

6.2.2 Exit Current Mode

The following command allows you to exit the current mode.

Command	Description
exit	Exit current mode and return to the previous mode

Example

Exit current mode and return to the previous mode.

```
ADLINK# exit
ADLINK>
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.3 Clear Configuration

The following commands allows you to clear counters on the specified port.

Command	Description
clear port [PORT_ID] counters	Clear counters of specified port

Example
Clear counters on port xe0.

```
ADLINK# clear port xe0 counters
ADLINK# show port xe0 counters
Statistics of port 1 --
Bytes Received:      0(Bytes)      Bytes Transed:      0(Bytes)
Bytes RX Rate :      0(Bps)        Bytes TX Rate:      0(Bps)
Pakts Received:      0(packets)    Pakts Transed:      0(packets)
Pakts RX Rate :      0(pps)        Pakts TX Rate:      0(pps)
```

6.2.4 Restore

Command “restore” can reset start-up configuration to factory default. Do not use this command unless you are clear on what it does. You should reboot the switch blade after executing this command to make it effective.

The following command allows you to to reset configuration to factory default.

Command	Description
restore	Reset start-up configuration to factory default.

6.2.5 Command List

Command “list” can print all commands which are available in Configure Mode.

The following commands are available for basic command list.

Command	Description
base	Enter into Base chip config mode
diag	Enter into diagnostic mode

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

exit	Exit current mode and down to previous mode
fabric	Enter into Fabric chip config mode
list	Print command list
no	Negate a command or set its defaults
password	Assign the privileged level password
restore	Reset start-up configuration to factory default. Never try unless you know the meaning!
show	Show running system information
write	Write running configuration to start-up configuration file

6.2.6 Negate Command

The following commands are available for deleting settings.

Command	Description
no ip	Delete IP information
no password	Turn off the privileged level password
no port	Delete port subsystem setting
no trunk	Delete trunk group setting
no vlan	Delete VLAN subsystem setting

Example
Delete the existing trunk setting.

```
ADLINK(fabric)#show trunk
Trunk 2 -- mode: Src_MAC          ; ports: xe2-xe4.
ADLINK(fabric)# no trunk 2
ADLINK(fabric)# show trunk
No trunk group is in use.
```

6.2.7 Password

User can enter Configure Mode by inputting the correct password. The default password is “adlink”, and you can change it as below.

The following command allows you to change the password.

Command	Description
password 8 WORD	Specifies an ENCRYPTED ‘enable’ password
password LINE	The UNENCRYPTED (cleartext) 'enable' password

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Example

Change the password, and login to Configure Mode with the new password.

```
ADLINK# password aaa
ADLINK# exit
ADLINK> enable
Password: <now use aaa to enter enable node>
ADLINK-2#
```

6.2.8 Check Network Connectivity

Configure Mode provides a ping tool to check whether the network is ok.

The following command allows you to check the network connectivity.

Command	Description
Ping IP_ADDR COUNT	Ping destination address or hostname and stop after sending NUM ECHO_REQUEST packets.

Example

Connect the switch blade to the 172.20.5.0 network segment, and set the IP address of the switch blade to 172.20.5.19. Use the ping command to check the network connectivity between the switch blade with the 172.20.5.0 network segment.

```
ADLINK# ping 172.20.5.18 2
PING 172.20.5.18 (172.20.5.18): 56 data bytes
64 bytes from 172.20.5.18: icmp_seq=0 ttl=64 time=0.3 ms
64 bytes from 172.20.5.18: icmp_seq=1 ttl=64 time=0.3 ms

--- 172.20.5.18 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.3 ms
```

6.2.9 Show Current System Information

The **show** commands display status information about managed objects on the network, service provisioning settings, and traffic statistics.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

The following commands are available for displaying system information.

Command	Description
show acl	Show ACL rule
show ip	Show IP information
show mac	Show L2 mac address table
show port	Show information of port system
show route	Show route table
show running-config	Show running configuration
show startup-config	Show start up configuration
show system	Show brief system information
show trunk	Show trunk group setting
show version	Show the version information
show vlan	Show all VLAN
show vrrp	Show all vrrp infomation

Example

Show VLAN and trunk information.

```
ADLINK# show vlan 2
Name                        : VLAN 2
Administrative State: enabled
Member ports             : xe2-xe3,
Untagged ports          : None
ADLINK# show trunk
Trunk    2 -- mode: Src_MAC              ; ports: xe2-xe4.
```

6.2.10 Save Configuration

All configurations changes are stored in RAM. When the ADSN restarts, the configurations will be lost. To save configuration changes, execute the command “write” before the next restart. All configurations will be saved into the startup configuration file.

This will prevent the information from being lost if you reset or reboot the system.

The following command allows you to save the current configuration.

Command	Description
write	Write running configuration to start-up configuration file

Example

Save all configurations into startup configuration file. When you reboot the blade, all the configurations will not be lost.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

```
ADLINK# write
Configuration saved
```

6.2.11 Port Configuration

The following commands are available for configuring port parameters.

Command	Description
port PORT_ID autoneg disable	Disable autoneg for the specified port
port PORT_ID autoneg enable	Enable autoneg for the specified port
port PORT_ID cos <0-7>	Set cos for specified port
port PORT_ID disable	Disable the specified port
port PORT_ID enable	Enable the specified port
port PORT_ID macfilter dst MAC_ADDR <1-4094>	Block specific destination MAC on a port
port PORT_ID macfilter src MAC_ADDR <1-4094>	Block specific source MAC on a port
port PORT_ID mtu <1518-16360>	Set mtu for specified port
port PORT_ID name STRING	Set name for specified port
port PORT_ID pvlan <1-4096>	Set pvlan ID for specified port
port PORT_ID speed VALUE	Set speed for specified port

Notes:
Enabling autonegotiation is ineffective unless the link partner also has autonegotiation enabled. If autonegotiation is disabled, you must set the line speed of the physical port.

Example
Set parameters of port xe0, such as: autoneg, mtu, name, etc.

```
ADLINK(config)# port xe0 autoneg disable
ADLINK(config)# port xe0 mtu 2000
ADLINK(config)# port xe0 name xe0
ADLINK(config)# port xe0 disable
ADLINK(config)# port xe0 cos 4
ADLINK(config)# show port xe0
Information of port xe0 --
Name                : xe0
Admin status        : Disable          Link status        : Down
Auto-neg            : Off
Link speed          : 10000M           Duplex mode        : Full
Vlan filter         : None             Stp state          : Forward
Default VLAN        : 4                Default COS        : 4
Flow control        : None             MTU                : 2000
Mcast limit         : Disable          Mcast max rate     : 0 pps
Bcast limit         : Disable          Bcast max rate     : 0 pps
Flood limit         : Disable          Flood max rate     : 0 pps
```

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.12 Port Mirror Configuration

Port mirroring can be used for network traffic sniffer and debug purposes. This is done for specific ports of the switch blade. Such as, many switch ports are configured as source ports and one switch port is configured as a destination port. You can configure how traffic is mirrored on a source port. Packets that are received on the source port, that are transmitted on a port, or are both received and transmitted, can be mirrored to the destination port.

The following commands are available for Port Mirror

Command	Description
port PORT_ID mirror-to PORT_ID both	Duplicate both ingress and egress traffic
port PORT_ID mirror-to PORT_ID egress	Duplicate port egress traffic
port PORT_ID mirror-to PORT_ID ingress	Duplicate port ingress traffic

Example

Duplicate both ingress and egress traffic of port xe2 to port xe3.

```
ADLINK# port xe2 mirror-to xe3 both
ADLINK# show port mirror
SRC_PORT      DST_PORT      MODE
xe2             xe3         ingress, egress
```

6.2.13 IP Configuration

The ADSN provides IPv4, IPv6 address and MAC address configuration functions on the physical network interface card and logical VLAN-interface.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

The following commands are available for IP configuration on interfaces.

Command	Description
ip -6	IPV6 information
ip address ETHNAME IPADDRESS NETMASK	Configure the IP address for the specified interface
Ip igmp	IGMP sub-system
ip hwaddr ETHNAME MAC_ADDR	Configure Ethernet MAC address for the specified interface
ip status ETHNAME up	Enable the specified interface running
ip status ETHNAME down	Disable the specified interface running
ip vlan-interface <1-4094> address IPADDRESS NETMASK	Configure the IP address for the specified VLAN interface
ip vlan-interface <1-4094> enable	Enable the specified VLAN interface
ip vlan-interface <1-4094> disable	Disable the specified VLAN interface

Example

Configure IP address for the VLAN interface 2.

```
ADLINK# vlan 2 enable
ADLINK# ip vlan 2 address 1.1.1.1 255.255.255.0
ADLINK# ip vlan 2 enable
ADLINK# show ip vlan-interface
Interface VLAN-2: status UP , IP: 1.1.1.1, Mask: 255.255.255.0
root@atca-3710:~## ifconfig f.vlan.2
f.vlan.2      Link encap:Ethernet  HWaddr 46:73:44:ef:e2:2a
              inet addr:1.1.1.1  Bcast:1.1.1.255  Mask:255.255.255.0
              inet6 addr: fe80::4473:44ff:feef:e22a/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:0 errors:0 dropped:0 overruns:0 frame:0
              TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:0 (0.0 B)  TX bytes:468 (468.0 B)
```

6.2.14 ACL Configuration

Access Control Lists (ACLs) provide an optional control capability that allows or disallows transp ort from certain source or to certain destination addresses. An access control list (ACL) is a set of rules (or permit or deny statements) for identifying traffic based on criteria such as source IP address, destination IP address, and port number.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

ACLs are primarily used for packet filtering. A packet filter drops packets that match a deny rule and permits packets that match a permit rule. The following commands are available for ACL.

Command	Description
acl add <0-1> ACTION QUALIFIER	Add a ACL rule.
acl clear	Clear all ACL rule and init acl table.
acl delete <0-1023>	Clear a specified ACL rule.
acl list actions	List all ACL actions.
acl list qualifiers	List all ACL qualifiers.

The following table lists the types supported by ADSN blade.

Table 1 Actions Table

Type	Description
drop	Drop the packet.
RedirectPort	Forwarding the packet to the port XE x.
RedirectTrunk	Forwarding the packet to the trunk x.

Table 2 Qualifiers Table

Type	Description
INPORTS	Filter for the port id a packet comes from..
SRCIP	Filter for source IP address of a packet.
DSTIP	Filter for destination ip address of a packet.
IPPROTOCOL	Filter for IP protocol (such as 0x06 for TCP) of a packet.
L4SRCPORT	Filter for L4 source port of a packet.
L4DSTPORT	Filter for L4 destination port of a packet.
SRCMAC	Filter for source MAC address of a packet.
DSTMAC	Filter for destination MAC address of a packet.
SRCTRUNK	Filter for the trunk ID a packet comes from.
ETHERTYPE	Filter for Ethernet type (such as 0x0806 for ARP) of a packet.
INNERVLAN	Filter for the inner VLAN id of a packet.
OUTERVLAN	Filter for the outer VLAN id of a packet.

Example

Add an ACL rule to make all packets with source IP in the 10.10.10.0 network segment redirect to port xe0.

```
ADLINK# acl add 0 redirectport=xe0 srcip=10.10.10.10/255.255.255.0
ADLINK# show acl
index   priority    action     qualifiers.....
0       0             RedirectPort=xe0 SrcIp=10.10.10.10/255.255.255.0
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.15 L2 Configuration

A device maintains a MAC address table for frame forwarding. Each entry in this table indicates the MAC address of a connected device, to which interface this device is connected and to which VLAN the interface belongs. After adding a MAC address into the L2 table, the packets with that MAC address can be forwarded to the destination by the L2 table directly rather than by broadcasting.

The following commands are available for L2 configuration.

Command	Description
l2 add MAC_ADDR <1-4094> PORT_ID	Add Ethernet MAC address to L2 table
l2 add MAC_ADDR <1-4094> PORT_ID l3 TRUE/FALSE hit TRUE/FALSE	Add Ethernet MAC address to L2 table by using L3 lookup
l2 delete MAC_ADDR <1-4094>	Remove item from L2 table
l2 init	Initialize layer-2 tables

Example

Add mac address 00:11:22:33:44:55 to L2 table.

```
ADLINK# l2 add 00:11:22:33:44:55 3 xe2    l3 true hit    true
ADLINK# show mac
      MAC Address            VID        PORT       Flag
   00:11:22:33:44:55          3           3       Static
   Total: 1 item(s).
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.16 xSTP Configuration

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network.
Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The RSTP takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree. Reconfiguration of the spanning tree can occur in less than 1 second (in contrast to 50 seconds with the default settings in the IEEE 802.1D spanning tree).
The primary goal in using RapidSpanning Tree Protocol (RSTP) is to prevent loops in a network, where the same packets might be re - sent to the same recipients. Use of RSTP is optional depending on the needs of the service provider.

The following commands are available for RSTP configuration on aTCA products.

Command	Description
disable	disable STP
enable	enable STP
force-version	force the STP work at STP or RSTP
forward-delay	forward-delay
hello-time	hello time
max-age	maximum time
path-cost	set path cost
port-edge	set port edge
port-mcheck	set port mcheck
port-p2p	set port p2p
port-priority	set port priority
port-stp	set port stp status
priority	bridge priority
show	show

The following commands are available for STP configuration on cPCI products.

The cPCI product does not support RSTP feature.

Command	Description
add-bridge	add bridge
add-interface	add interface to bridge

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

del-bridge	delete bridge
del-interface	delete interface from bridge
set-bridge-priority	set bridge priority
set-forward-delay	set forward delay time
set-hello-time	set hello time
set-max-age-time	set max message age
set-path-cost	set path cost
set-port-priority	set port priority
set-state	set current bridge stp on/off
show	show a list of bridges
show-stp	show bridge stp info

Example

Set bridge maximum forwarding delay time.

```
ADLINK(fabric)# spanning-tree forward-delay 15
ADLINK(fabric)# spanning-tree show
          ---------------------------SPANNING TREE information in STP domain ------------
Designated Root                    : 00:30:64:2b:2d:97
Designated Root Priority           : 32768
Designated Root Path Cost          : 4000
Root Max Age       20     Hello Time    2       Forward Delay    15

Bridge ID Mac Address              : 00:30:64:2b:2d:c2
Bridge ID Priority                 : 32768
Bridge ForceVersion                : RSTP
Bridge Max Age    20     Hello Time    2       Forward Delay    15
```

6.2.17 Route Configuration

Without a default route, a packet with no matching routing entry is discarded and an ICMP destination-unreachable packet is sent to the source. After adding a route into the routing table, the packets can be forwarded to the destination by that route.

The following commands are available for route configuration.

Command	Description
route -6	IPV6 information
route add DST-IP MASK GW	Add a route entry

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

route clear	Clear all route entries
route delete DST-IP MASK	Delete a route entry

Example

Add a route into the routing table.

```
ADLINK# route  add  200.200.200.200 255.255.255.0 192.168.2.1 xe3
ADLINK# show route
index  dstip            mask            gateway         out_port  reachable
0      200.200.200.0    255.255.255.0   192.168.2.1       xe3       yes
```

6.2.18 Trunk Configuration

Trunks, which are also known as link aggregation groups (LAGs), allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it is a single link, which increases fault tolerance and provides load sharing. The following commands are available for trunk configuration.

command	Description
Trunk <1-8> add port PORT_LIST	Add ports to specified trunk
Trunk <1-8> delete port PORT_LIST	Delete ports form specified trunk
trunk <1-8> mode <0-6>	Set the hash algorithm for specified trunk
trunk destroy	Remove all trunk groups
trunk monitor add <1-8>	Add a specified trunk into monitor
trunk monitor delete <1-8>	Delete a specified trunk from monitor

There are 7 different trunk modes, as described below.

Trunk mode value	Description
1	Source MAC
2	Destination MAC
3	Source & Destination MAC
4	Source IP
5	Destination IP
6	Source & Destination IP
0	zero

Example

Add port xe2-xe4 into trunk 2, to make the three ports into a virtual link. Set the mode of trunk 2 to

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

1 to make the data stream load balance on trunk 2 based on the source MAC. Then add the trunk into monitor to monitor the status of ports in the trunk 2.

```
ADLINK# trunk 2 add port xe2-xe4
ADLINK# trunk 2 mode 1
ADLINK# show trunk
Trunk 2 -- mode: Src_MAC              ; ports: xe2-xe4.
ADLINK# trunk monitor add   2
ADLINK# show trunk monitor
Trunk 2 -- Port03.down Port04.down Port05.up
```

6.2.19 VLAN Configuration

Ethernet is a network technology based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) mechanism. Because the medium is shared, collisions and excessive broadcasts are common on Ethernet networks. To address the issue, virtual LAN (VLAN) was introduced to break a LAN down into separate VLANs.

Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic. Virtual Local Area Networks (VLANs) are used to provide connectivity between ports and other e ntities in the ADSN System and across Ethernet Virtual Connections across Ethernet Networks.

The following commands are available for VLAN.

command	Description
vlan <1-4094> associate mac MAC_ADDR [prio <0-7>]	Dynamic VLAN association
vlan <1-4094> disable	Switch administrative status to disabled
van <1-4094> enable	Switch administrative status to enabled
vlan <1-4094> name STRING	Add VLAN Description
vlan <1-4094> port PORT_ID tag	Add port to VLAN as tagged
vlan <1-4094> port PORT_ID untag	Add port to VLAN as untagged

Example

Create a VLAN with VLAN ID=2. Set port xe2 and xe3 as tag port and add them into VLAN 2.

```
ADLINK(config)# vlan   2 port   xe2 tag
ADLINK(config)# vlan   2 port   xe3 tag
ADLINK(config)# show vlan 2
Name                    : VLAN 2
Administrative State: enabled
Member ports            : xe2-xe3,
Untagged ports          : None
```

6.2.20 IGMP Snooping Configuration

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

The following commands are available for IGMP Snooping configuration.

The cPCI product does not support this feature.

command	Description
igmp-snooping STRING	[enable|disable] IGMP snooping
add-query-port	Add query port
add-router-port	Set router port
del-query-port	Delete query port
del-router-port	Del router port
group-life	Change group life time
query-interval	Change query interval value
response-time	Change host response time
robustness	Change Robustness variable
set-mc-flood-mode	Set multicast flood mode
show	Show

Example

Enable IGMP-snooping function and display default configuration.

```
ADLINK(fabric)# igmp-snooping enable
ADLINK(fabric)# igmp-snooping show config
GROUP LIFE:                 250
QUERY INTERVAL:             125
RESPONSE TIME:              10
ROBUSTNESS:                 2
ADLINK(fabric)#
```

6.2.21 IGMP Proxy Configuration

The ADSN Platform supports multicast forwarding as a bandwidth-efficient method to provide point-to-multipoint broadcast video. Thesimple Internet Group Management Protocol (IGMP) is sufficient to control the multicast forwarding. In brief, IGMP builds a per-group forwarding tree. With this multicast forwarding tree, a single copy of any IP multicast packet from a particular

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

sender will pass through port regardless of how many receivers are on the tree.
To connect to a wider multicast network, a multicast router interface can be explicitly configured using the proxy command. In most cases, it is through a WAN port on OLC, but this need not be the case. When a switch is IGMP-enabled, it acts as a proxy client on the router interface by performing the host portion of the IGMP protocol.

Note:

The following rules should be performed when using IGMP proxy configuration.

1. IGMP-Proxy service should be enabled on each vlan-interface;
2. Both host-side & router-side vlan-interfaces have to enable IGMP proxy;
3. Support only one uplink port & one uplink vlan;
4. IGMP proxy & IGMP snooping cannot be enabled at the same time;
5. TTL of ingress multicast flow should be bigger than 1 (2 or larger);

The following commands are available for IGMP Proxy configuration.

The cPCI product does not support this feature.

command	Description
ip igmp proxy	start IGMP proxy service
no ip igmp proxy	stop IGMP proxy service
ip igmp-proxy uplink-port xe.	designate uplink port (host interface)
ip igmp-proxy uplink-vlan xxx	multicast VLAN ID
ip igmp-proxy vlan-interface xxx	enable proxy service on a vlan-interface
no ip igmp-proxy vlan-interface	disable proxy service of a vlan-interface
show ip igmp-proxy group	display group info
show ip igmp-proxy uplink	display uplink info
show ip igmp-proxy vlan-interface	display proxy service enabled vlan-interface

Example

Set the VLAN ID and port for the proxy.

```
ADLINK(fabric)# ip igmp proxy
ADLINK(fabric)# ip igmp-proxy uplink-port xe0
ADLINK(fabric)# ip igmp-proxy uplink-vlan 10
ADLINK(fabric)# ip igmp-proxy vlan-interface 10
ADLINK(fabric)#
ADLINK(fabric)# show ip igmp-proxy
   group                Multicast group information
   uplink               Proxy uplink information
   vlan-interface   Proxy service VLAN information
ADLINK(fabric)# show ip igmp-proxy uplink
IGMP proxy uplink port: xe0.
IGMP proxy uplink VLAN: 10.
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.22 Quality of Service Configuration

Quality of Service (QoS) is one of the means by which a service provider establishes the rules for traffic forwarding and handling. These rules apply prioritization schemes to data packets by defining QoS classifications and binding various QoS profiles to physical ports on the network, and mapping the QoS types to specific priority values.

The following commands are available for QoS configuration.

command	Description
class-map	Class information
global-config	Qos global config
policy-map	Policy information
profile	Profile information
show	show
cos-global-config	cos-global-config
cos-port-config	cos-port-config
port-config	Config policy on a port

Example

Bind the available match types of QoS to current profile aaa.

```
ADLINK(fabric)# qos profile create aaa
ADLINK(fabric)# qos profile aaa bind source-mac

ADLINK(fabric)# qos    show    profile
Total 3 profile(s).
=====================================================
    Profile name:                       user-default
    Class number bound:                   0
    Profile BindMode:
        VLAN_BIND
        IP_PROTOCOL_BIND
        SIP_BIND
        DIP_BIND
        SPORT_BIND
        DPORT_BIND
        ETHERTYPE_BIND
=====================================================
    Profile name:                       aaa
    Class number bound:                   0
    Profile BindMode:
        SMAC_BIND
=====================================================
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.23 LACP Configuration

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer.

The following commands are available for LACP configuration.

The cPCI product does not support this feature.

command	description
trunk add <0-7> mode manual	Create a static trunk, <0-7> is the trunk ID.
trunk add <0-7> mode lacp	Create a LACP trunk, <0-7> is the trunk ID. The members in the trunk negotiate with LACPDU.
trunk <0-7> add port xe<0-31>	Add a port into the trunk. Only one port can be added into the trunk in a command.
trunk <0-7> delete port xe<0-31>	Remove a port from the trunk.
trunk <0-7> delete	Remove a specific trunk.
trunk destroy	Remove all trunk groups.
trunk <0-7> set active num <0-7>	Set the M active ports in LACP trunk. Assume there is M+N links are available, set M ports as active for packet forwarding, N ports as standby for backup.
show trunk	Display information of all the trunks.
show trunk <0-7>	Display information of the specific trunk.
show trunk <0-7> detail	Display detail information of the specific trunk and the ports information in the trunk.
trunk <0-7> set balance type <0-7>	Set the balance type of the specific trunk. The balance type including “0-Always zero; 1-SA; 2-DA; 3-SA&DA; 4-SIP; 5-DIP; 6-SIP&DIP; 7-enhanced hash”
trunk l4port enable	Add L4Port into hash key together with IP
trunk l4port disable	Won't use L4Port as part of hash key together with IP
trunk enhanced-hash 4-tuple	Set the hash algorithm in enhanced hash balance type.
trunk enhanced-hash 5-tuple	Set the hash algorithm in enhanced hash balance type.

6.2.24 LLDP Configuration

The switch blade supports the IEEE 802.1AB Link Layer Discovery Protocol (LLDP). LLDP is a

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors. This protocol can advertise details such as configuration information, device capabilities, and device identity. The default LLDP global state is disabled.

The following commands are available for LLDP configuration.

The cPCI product does not support this feature.

command	description
pause	Pause lldpd operations
resume	Resume lldpd operations
show	LLDP system running info
txhold	Set LLDP transmit hold,[2,10]
txinterval	Set LLDP transmit delay,[5,32768]
update	Pause lldpd operations

This example shows how to configure LLDP characteristics.

```
ADLINK(fabric)# lldp txhold 5
set lldp tx_hold successfully!
ADLINK(fabric)# lldp txinterval 100
set lldp tx_interval successfully!
ADLINK(fabric)# lldp show
   local        local chassis info
   neighbor    Show neighbors data
ADLINK(fabric)# lldp show local
LOCAL CHASSIS:
  ------------------------------------------------
CHASSISID: 00:30:64:2a:56:48
SYSNAME: aTCA-3710
SYSDESC: Linux 3.0.48-rt70-svn233 #16 SMP Tue Dec 30 14:24:56 CST 2014 ppc
MGMTIP: 192.168.25.213
CAPCABILITY: Station ON
CAPCABILITY: Router ON
CAPCABILITY: Wlan OFF
CAPCABILITY: Bridge OFF
------------------------------------------------
ADLINK(fabric)#
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.25 SNMP Configuration

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB.

The SNMP manager can be part of a network management system (NMS). The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1-The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:
  - SNMPv2 - Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
  - SNMPv2C-The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.
- SNMPv3 - Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:
  - Message integrity-ensuring that a packet was not tampered with in transit
  - Authentication-determining that the message is from a valid source
  - Encryption-mixing the contents of a package to prevent it from being read by an unauthorized source.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

SNMPv2C report the error type.
SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security mechanism is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

Using SNMP to Access MIB Variables

An example of an NMS is the MibBrowser as network management software. MibBrowser software uses the switch MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.
As shown in Figure 25-1, the SNMP agent gathers data from the MIB. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps alert the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in get-request, get-next-request, and set-request format.

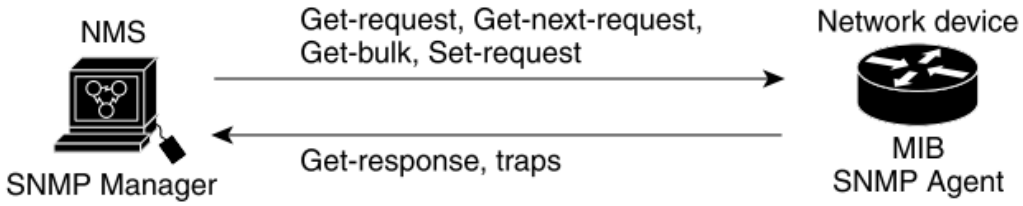


Figure 25-1 SNMP Network

This example shows how to configure SNMP characteristics.

The cPCI product does not support this feature.

Set SNMP trap receiver address as below:

Vi /usr/share/snmp/snmpd.conf
…
####
#notification configuration
trap2sink 172.99.1.251:162 public
informsink 172.99.1.251:162 public

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.26 DHCP Configuration

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and a mechanism for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The ADSN switch can act as a DHCP server. The DHCP server assigns IP addresses from specified address pools on the switch to DHCP clients and manages them.

Limitations and Restrictions: The IP addresses from specified address pools should be on the same LAN with the switch management IP address.

The Switch can support DHCP server to let the processor blades to request IP addresses dynamically. For ADSN implementation, it can support acquire the configuration parameters based on slot id read from local IPMC/BMC via backplane. On switch blades, ADSN can provide DHCP configuration templates for both aTCA and MICA platforms to allocate IP addresses based a preconfigured static mapping to each client identifier which is derived from the logical slot number and interface ID. On processor blades, ADSN can provide a sample scripts to enable send a DHCP request with a customized client identifier which is derived from the logical slot number and interface ID.

The following configurations are available for DHCP configuration.

The cPCI product does not support this feature.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

1. Login the switch blade and enter DHCP pool configuration mode and create a name for the DHCP Server address pool.
   1) Specify the subnet network number and mask of the DHCP address pool.
   2) Specify the IP address range and mask for the interface of processor blade in different slot.
   3) Save the configuration file.

```
root@aTCA-3710:~# vi /etc/dhcpd.conf
……
      shared-network hostname {
         subnet 192.168.25.0 netmask 255.255.255.0 {
            option domain-name "Adlink";
            option domain-name-servers 192.168.2.22, 192.168.2.21;
            option routers 192.168.1.1;
            option subnet-mask 255.255.255.0;
            default-lease-time 21600;
            max-lease-time 43200;
         }
         pool {
            allow members of "slot01";
            range 192.168.25.11 192.168.25.20;
         }
         pool {
            allow members of "slot02";
            range 192.168.25.21 192.168.25.30;
         }
         pool {
            allow members of "slot03";
            range 192.168.25.31 192.168.25.40;
      }
……
```

2. Start dhcpd process or reboot this switch and the interface of process blade in corresponding slot can acquire the IP addresses correctly.

```
root@aTCA-3710:~# dhcpd
```

3. Login the processor blade and download the script from ADSN software package in the following directory, then execute this script on the processor blade with specified port. This port will be assigned an IP address dynamically from specified address pools.
   ADSN_3710_V1.1_s.xxx/dhcp/dhcpClient.sh

```
[root@server ~]# ./dhcpClient.sh <port name>
```


Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6.2.27 Event log Configuration

The event log can support remote logging via Linux syslog mechanism. The local logging can be retained when the remote logging is enabled. The remote logging debug level configuration is independent of the local debugging level, which means the user can configure different debug levels for local logging and remote logging respectively.

The following commands are available for event log configuration.

The cPCI product does not support this feature.

command	description
local	Local setting enable | disable
remote	Remote setting
remote debuglevel	Remote log debug level
remote disable	Disable remote log
remote enable	Enable remote log
remote hostip	Receiving host ip setting

This example shows how to configure event log characteristics.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

1. Local log can be saved in below files:

   root@aTCA-3710:/usr/local# ls -l

   -rw-r----- 1 root root 532064390 Apr 23 00:33 adlink_sx_app.log

   -rw-r--r-- 1 root root 146706717 Apr 23 00:33 adlink_sx_chassis.log

2. For remote log setting:
   1) Login the receiving host and enter log configuration file.(e.g, syslog.conf)
   2) Create a file name and file path for remote log receiving.
   3) Run Linux syslog process.

      For example:

      The receiver machine is a Red hat Linux server 192.168.25.213

      ---

      root@aTCA-receiver:/etc# **vi syslog.conf**

      ….

      #daemon.* -/var/log/daemon.log

      #kern.* -/var/log/kern.log

      #lpr.* -/var/log/lpr.log

      #mail.* -/var/log/mail.log

      #user.* -/var/log/user.log

      local7.debug **-/home/root/z0506.log**

      ….

      root@aTCA-receiver:/etc# **syslogd -r**

      ---

   4) Login the log sender card and specify the hostip and debug level on which to collect event logs, and enter remote log enable mode.

      ADLINK# log remote debuglevel 7

      ADLINK# log remote hostip 192.168.25.213

      ADLINK# log remote enable

   5) View the event log successfully in the receiver machine.

      root@aTCA-receiver:/etc# cat /home/root/z0506.log

      May 9 18:17:53 aTCA-3710 SX_Controller: unit=1,port=11

      May 9 18:17:53 aTCA-3710 SX_Controller: Link status : Up

      May 9 18:29:03aTCA-3710 SX_Controller: USER:127.0.0.1 COMMAND:show vlan

      ….

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Management API

For information on the Management API, please refer to the document “ADLINK ADSN API Programming Guide”.

Glossary

Most of the term definitions found in this Glossary are gleaned from various public and commercial websites.

ACE

Access Control Entry. An ACE is a description of access rights associated with a user or process.

ACL

An ACL is a list of permissions assigned to an object. The list describes which users or which processes are allowed to access and manipulate an object. An ACL is made up of ACEs.

Bandwidth

A measurement of the information‐carrying capacity of a line or a network. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).

bps

Bits per second. A measurement for determining transmission speed.

Class of Service

Class of Service is a way of managing network traffic by grouping similar types of data (for example, e‐mail, streaming video, voice, large document file transfer) and treating each type as a class with its own level of service priority. Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a “best‐effort.” One can think of CoS as “coarsely‐grained” traffic control and QoS (Quality of Service) as “finely‐grained” traffic control.

CoS

See Class of Service.

CRC

Cyclic Redundancy Checking. A method of checking for errors in data that has been transmitted on a communications link. A sending device applies a 16‐ or 32‐bit polynomial to a block of data that is to be transmitted and appends the resulting cyclic redundancy code (CRC) to the block. The receiving end applies the same

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

polynomial to the data and compares its result with the result appended by the sender. If they agree, the data has been received successfully. If not, the sender can be notified to resend the block of data.

Differentiated Services
Also known as DiffServ or Type of Service, is a field in the IP header that allows users to provide Quality of Service (QoS) for network traffic. See also Type of Service.

Fast Ethernet
Fast Ethernet is a LAN transmission standard that provides a data rate of 100 megabits per second (referred to as 100BASE‐T).

ICMP
Internet Control Message Protocol. This protocol is used to transmit messages in IP networks. It also includes utilities such as ping and traceroute which are useful for diagnostic analysis of network connectivity.

IEEE
Institute of Electrical and Electronics Engineers. The largest international non‐profit, professional organization for the advancement of technology related to electricity.

IGMP
Internet Group Management Protocol. A communications protocol that focuses on the membership of Internet Protocol multicast groups.

IP
Internet Protocol. The computer networking protocol used on the Internet. IP may also stand for:
Internet Provider (more commonly referred to as Internet Service Provider or ISP). A business or organization that offers users access to the Internet and related services.
Intellectual Property. The legal term which encompasses copyrights, patents, trademarks, and trade secrets (amongst others).

ITU
International Telecommunications Union. Created to standardize and regulate international radio and telecommunications. Originally (in 1865) formed as the International Telegraph Union, the ITU is one of the oldest active international organizations.

Kbps
Kilobits per second

LAN
Local Area Network. A computer network covering a local area, like a home, office or

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

small group of buildings such as a college. When using ethernet, the computers are usually wired to a hub or to a switch. LANs can be interlinked via a router to form a Wide Area Network (WAN).

MEF

The MEF (Metro Ethernet Forum) is a non‐profit organization promoting the adoption of Carrier‐class Ethernet networks and services. The Forum membership includes service providers, incumbent local exchange carriers, network equipment vendors, test equipment vendors, and other networking companies that share an interest in metro Ethernet. (See Metro Ethernet Network.)

MEN

Metro Ethernet Network. The Ethernet network created by service providers.

MIB

Management Information Base. A database of network performance information (such as error counts and on/off information), stored on a Network Agent and retrieved by a Network Management Station (NMS).

OSI

Open Systems Interconnection was a new effort in networking started in 1982 by the International Organization for Standardization (ISO), along with the ITU‐T.
Prior to OSI, networking was completely vendor‐developed and proprietary, which lead to interoperability issues resulting from a lack of common protocols between network devices. OSI was a new industry effort, attempting to get everyone to agree to common network standards to provide multi‐vendor interoperability.
The OSI approach was eventually eclipsed by the Internet's TCP/IP protocol suite. Its pragmatic approach to computer networking and independent implementations of simplified protocols made it a practical standard.

STP

Spanning Tree Protocol. A network management protocol that facilitates loop‐free traffic forwarding for any bridged LAN.

VLAN

Virtual Local Area Network. A group of devices on different physical LANs which can communicate with each other as if they were on the same physical LAN segment.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Getting Service

ADLINK Technology, Inc.
Address: 9F, No.166 Jian Yi Road, Zhonghe District
New Taipei City 235, Taiwan
Tel: +886-2-8226-5877
Fax: +886-2-8226-5717
Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.
Address: 5215 Hellyer Avenue, #110, San Jose, CA 95138, USA
Tel: +1-408-360-0200
Toll Free: +1-800-966-5200 (USA only)
Fax: +1-408-360-0222
Email: info@adlinktech.com

ADLINK Technology (China) Co., Ltd.
Address: 300 Fang Chun Rd., Zhangjiang Hi-Tech Park,
Pudong New Area, Shanghai, 201203 China
Tel: +86-21-5132-8988
Fax: +86-21-5132-3588
Email: market@adlinktech.com

ADLINK Technology Beijing
Address: Rm. 801, Power Creative E, No. 1, B/D
Shang Di East Rd., Beijing, 100085 China
Tel: +86-10-5885-8666
Fax: +86-10-5885-8625
Email: market@adlinktech.com

ADLINK Technology Shenzhen
Address: 2F, C Block, Bldg. A1, Cyber-Tech Zone, Gao Xin Ave. Sec. 7,
High-Tech Industrial Park S., Shenzhen, 518054 China
Tel: +86-755-2643-4858
Fax: +86-755-2664-6353
Email: market@adlinktech.com

LiPPERT ADLINK Technology GmbH
Address: Hans-Thoma-Strasse 11, D-68163, Mannheim, Germany
Tel: +49-621-43214-0
Fax: +49-621 43214-30
Email: emea@adlinktech.com

ADLINK Technology, Inc. (French Liaison Office)
Address: 15 rue Emile Baudot, 91300 Massy CEDEX, France
Tel: +33 (0) 1 60 12 35 66
Fax: +33 (0) 1 60 12 35 66
Email: france@adlinktech.com

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

ADLINK Technology Japan Corporation
Address: KANDA374 Bldg. 4F, 3-7-4 Kanda Kajicho,
Chiyoda-ku, Tokyo 101-0045, Japan
Tel: +81-3-4455-3722
Fax: +81-3-5209-6013
Email: japan@adlinktech.com

ADLINK Technology, Inc. (Korean Liaison Office)
Address: 8F Mointer B/D,1675-12, Seocho-Dong, Seocho-Gu,
Seoul 137-070, Korea
Tel: +82-2-2057-0565
Fax: +82-2-2057-0563
Email: korea@adlinktech.com

ADLINK Technology Singapore Pte. Ltd.
Address: 84 Genting Lane #07-02A, Cityneon Design Centre,
Singapore 349584
Tel: +65-6844-2261
Fax: +65-6844-2263
Email: singapore@adlinktech.com

ADLINK Technology Singapore Pte. Ltd. (Indian Liaison Office)
Address: 1st Floor, #50-56 (Between 16th/17th Cross) Margosa Plaza,
Margosa Main Road, Malleswaram, Bangalore-560055, India
Tel: +91-80-65605817, +91-80-42246107
Fax: +91-80- 23464606
Email: india@adlinktech.com

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000