MCSFP-16M

User's Manual

Rev. 1.10

We make no warranties with respect to this documentation and disclaim any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. We reserve the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

Trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective companies.

Contents

1. Introduction

CL-MCSFP-16M is a management media converter hub with sixteen TX-SFP pairs.   TX ports support 100/1000Mbps operation speed.   SFP ports supports 100Mbps or 1000Mbps SFP module.   CL-MCSFP-16M will auto-detect link speed on SFP port, and set TX port to the same operation mode.   If SFP port link down and link pass-through function is enabled, TX port will also force to link down.   Management functions are supported with Http, CLI, and SNMP interfaces for device configuration and monitor.

CL-MCSFP-16M is a smart and cost-effect Fast Ethernet/Gigabit Ethernet copper to SFP converter device.   It is powerful and flexible for network installation.

1.1 Package Contents

✓ One CL-MCSFP-16M
✓ This user manual
✓ One AC power Cord (*AC power model only)
✓ Rack-mount kits and screws
✓ One console cable

2. Where To Place the Device

This device can be placed on a flat surface (your desk, shelf or table).
Place the device at a location with these connection considerations in mind:

- The device configuration does not break the rules as specified in Section 3.
- The device is accessible and cables can be connected easily to it.
- The cables connected to the device are away from sources of electrical interference such as radio, computer monitor, and light fixtures.
- There is sufficient space surrounding the device to allow for proper ventilation (the device may not function according to specifications beyond the temperature range of 0 to 50 degrees C).

You can install the device on a 19" rack with rack-mount kits as the picture.
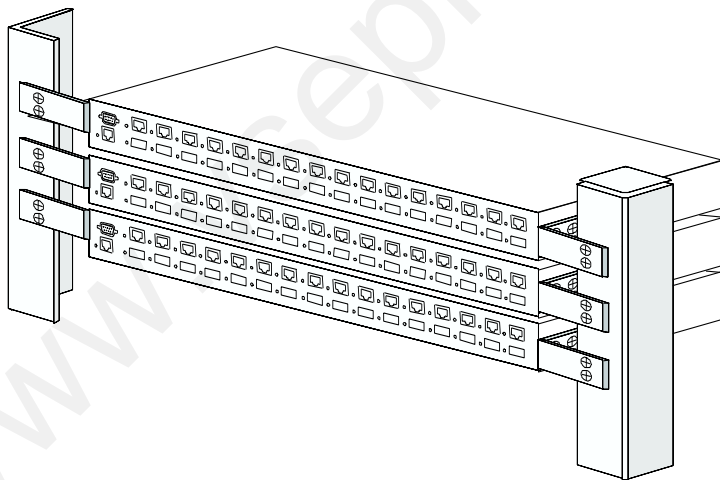
<< Rack-Mount Installation >>

Before rack mounting the device,please pay attention to the following factors :

1. **Temperature** - Because the temperature in a rack assembly could be higher than the ambient room temperature, check that the rack-environment temperature is within the specified operating temperature range. (Please refer to Product Specifications in the manual.)   Air flow is necessary in a rack for temperature stable.
2. **Mechanical Loading** - Do not place any equipment on top of this rack-mounted device.
3. **Circuit Overloading** - Be sure that the supply circuit to the rack assembly is not overload after installing this device.
4. **Grounding** - Rack-mounted equipment should be properly and well grounded. Particular attention should be given to supply connections other than direct connections to the mains.

[Attach Rack-Mount Brackets to the Device]
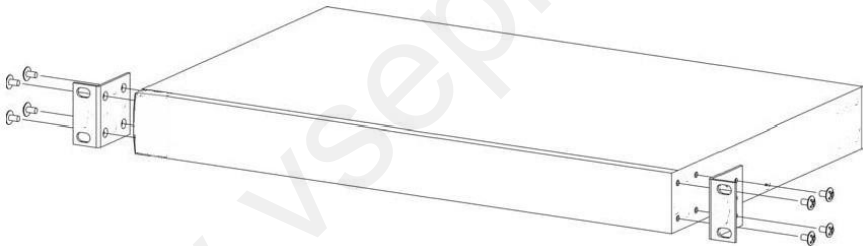
1. Position a Rack-Mount Bracket on one side of the device.
2. Line up the screw holes on the bracket with the screw holes on the side of the device.
3. Use a screwdriver to install the M3 flat head screws through the mounting bracket holes into the device. (There could have two or four screws for one bracket.   That depends on the model that installed.)
4. Repeat Step 1~3 to install another bracket to the device.
5. Now it is ready to mount to a rack.

[Mount the Device on a Rack]
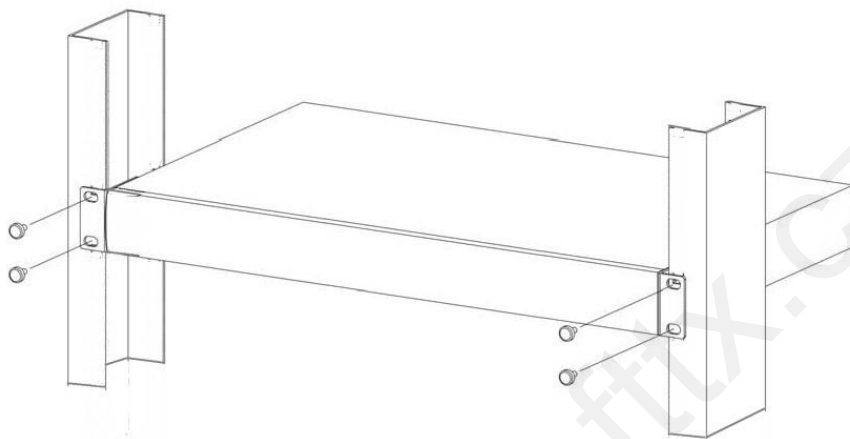
1. Position a bracket that is already attached to the device on one side of the rack.
2. Line up the screw holes on the bracket with the screw holes on the side of the rack.
3. Use a screwdriver to install the rack screws through the mounting bracket holes into the rack.
4. Repeat Step 1~3 to attach another bracket that is already attached to the device on another side of the rack.

3. Configure Network Connection

3.1 Connecting to the Device

[Connection Guidelines:]
- For 100BaseTX connection: Category 5 twisted-pair Ethernet cable
- For 1000BaseTX connection: Category 5e or 6 twisted-pair Ethernet cable
- For TX cable connection, always limit the cable distance to 100 meters (328 ft) as defined by IEEE specification
- For 100BaseFX / 1000BaseSX / 1000BaseLX connections, you can connect long distance fiber optic cable to the device.
- Because this device supports **Auto MDI/MDI-X** detection on each TX port, you can use normal straight through cable for both workstation connection and hub/switch cascading.

Fiber Optic Cable
10 KM away

Cat.5e Twisted Pair Cable
100 meters max.
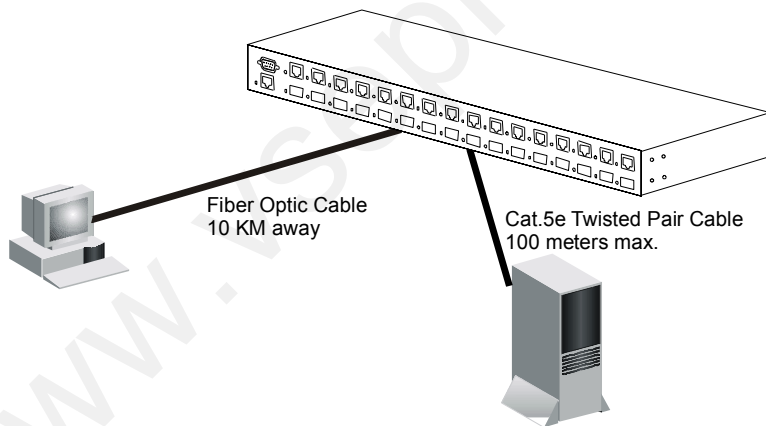
3.2 Application

The device can be used to convert different Ethernet media(e.g.fiber optic cable) to copper cable. It depends on the SFP module that plugged on SFP slot. Because fiber optic cable application is popular now, this device provides an easy way to convert it to copper cable that is used for most network device connections.

The example below demonstrates the device ability to connect a network. Number of nodes are connected with Ethernet fiber optic cables. With the device, they are connected to a normal Ethernet switch and switching network traffic there. If fiber optic cable connection fail, copper connection will also be link down to pass down the problem if link pass-through function is enabled.

Complete the network connection and do some simple configuration. Then it works and could be monitored remotely.
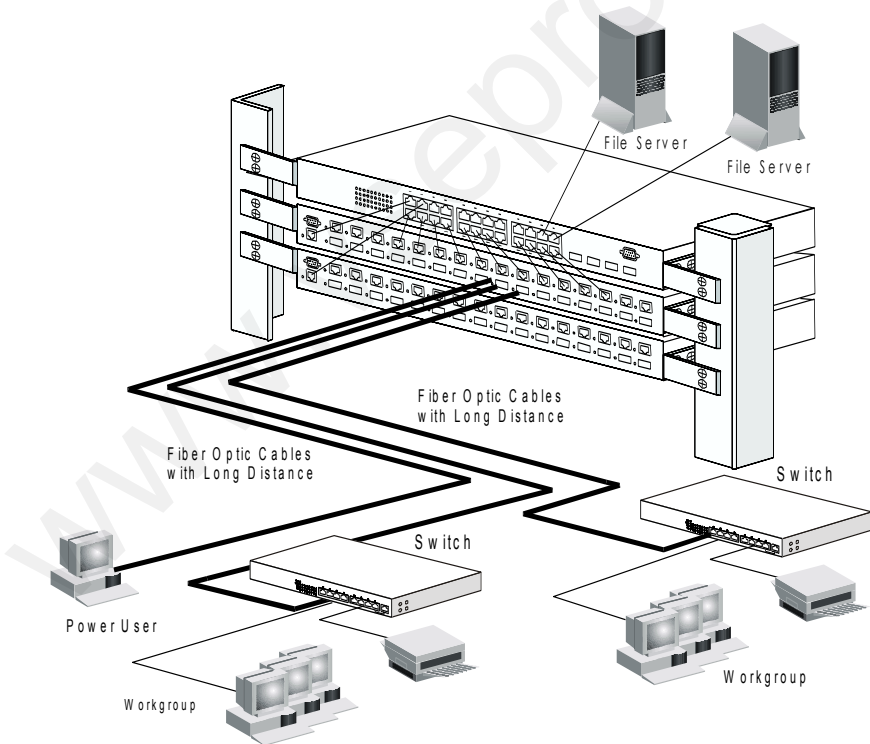
4. Add/Remove SFP Module

This device supports SFP module (100FX / 1000SX / 1000LX / …) network connection.   Because SFP slots support hot-swap function, you can plug/unplug SFP transceiver to/from SFP slot directly.   The device can auto-detect the Ethernet connection from SFP slot.
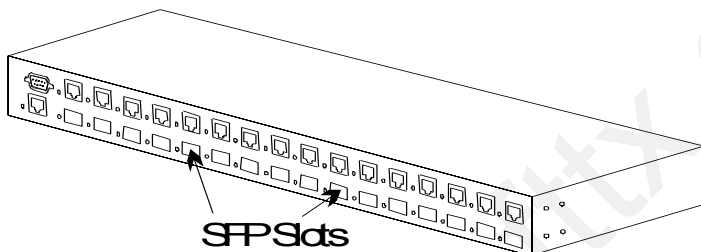
SFP Slots

Follow the steps for module adding and removing.

[Add SFP Transceiver]
1. Plug in the SFP Transceiver to SFP slot directly.
2. Connect network cable to the SFP Transceiver. If the connected devices are working and TX port of the pair is ready for link up, the Link/Act/Speed LED will be ON.

[Remove SFP Transceiver]
Unplug the SFP Transceiver from SFP slot directly.

5. LED Condition Definition

5.1 LED Indication

The LEDs provide useful information about the device and the status of all individual ports.

LED	Status	Description
Power	ON	The device is power ON.
	OFF	The device is power OFF.
Link/Speed/Act	ON-Green	The port is link as 1000Mbps speed.
	ON-Yellow	The port is link as 100Mbps speed.
	Flash-Green	Send/Receive data in 1000Mbps.
	Flash-Yellow	Send/Receive data in 100Mbps.
	OFF	The port is link down.
LAN (Management)	ON-Green	The port is link as 100Mbps speed.
	ON-Yellow	The port is link as 10Mbps speed.
	Flash-Green	Send/Receive data in 100Mbps.
	Flash-Yellow	Send/Receive data in 10Mbps.
	OFF	The port is link down.

6. Operation of the Device

This device consists of sixteen TX-SFP pairs.   Each pair works individually from each other.   Each TX-SFP pair works in pure converter mode - convert the connection media at SFP port to copper TX connection.   No any packets will be blocked or filtered in the media conversion.

Here is the description about its operation.

1. Detect the connection at SFP port
   When SFP module is plugged into a SFP slot and network cable is connected, the device will detect the link speed of the connection.   The link speed could be 100Mbps or 1000Mbps.   After the link speed is detected, TX port of the pair will be set to the same operation speed.

2. Check the link status of SFP port
   The device will always check the link status of SFP ports.   If any SFP port is link down, the device will force TX port of the pair to link down to pass down the link status if link pass-through function is enabled.

3. About the link status of TX port
   The device will also check the link status of TX ports.   If any TX port is link down, the device will force the SFP port of the pair to link down to pass down the link status if link pass-through function is enabled.
   The TX port will be forced to the same link speed as SFP port of the pair.   If the connecting Ethernet device is a gigabit port, it will be link as 100Mbps or 1000Mbps - depending on the link speed of SFP port.   If the connecting Ethernet device is a 100Mbps port, it will be link as 100Mbps only.   If SFP port will be link as 1000Mbps, the TX port of the pair will not be link up.   In this case, please change the connecting Ethernet device to a gigabit port for link up.

7. Manage / Configure the Device

7.1 Introduction of the management functions

This device is a management device.   An Ethernet port is supported for out-band management function from Http/Telnet/SNMP interfaces. Console is supported for local command-line settings.

DDMI of SFP modules and port link up/down status could be monitored through the management interface.

The following is a brief introduction about these functions before the detail operation sections.

1. DDMI of SFP module
   DDMI(Digital Diagnostics Monitoring Interface) is a function for network device information and status monitor.   If a SFP module supports DDMI function, this device can read the information and status of the SFP module.   If alarm or warning conditions happen, this device will send a SNMP trap.

2. Link Pass-through
   For a TX-SFP pair, the link status of TX or SFP port will be passed through to another side to make the link status being transparent.

3. Logging and syslog
   Logging function can record system events to flash.   That is helpful for system diagnostics.   And syslog function can send the event log to a remote server through syslog protocol.

4. Software Backup/Update
   This device supports backup and update functions for its internal software and its network configuration.   It could be done in two ways.

   a. From console when booting : doing by Xmodem protocol and by terminal program for boot code and run-time code updating.

   b. From web browser : doing by http protocol and by web browser for

run-time code and configuration backup/update.

c. From telnet or console command : doing by tftp protocol for run-time code and configuration backup/update.

7.2 Settings with Console Connection

7.2.1 Basic of the Console Interface

<< Enter Console Interface >>
Follow the steps to complete the console hardware connection first.
1. Connect from console port of the device to COM port of PC with the console cable.
2. Start the terminal program of Windows.   Create a new connection and select COM port of PC used for the console.   Set the configuration of the terminal as **[9600,8,N,1]**. (You can find the terminal program in [Start] -> [Programs] -> [Accessory Programs] -> [Communication] -> [Terminal].   If you cannot find it, please install it from your Windows Installation Disk.   Please refer to your Windows user manual for the installation.)
3. Power on the device.

If everything is correct, the booting message will appear in the terminal program when the device is powered on.   It will stop at the following screen after some initializing messages.

Bootloader Ver. 1.05.00(256K Config),at 13:50:52, Sep   8 2009

RAM: 0x00000000-0x00800000, 0x0000cc78-0x007f3000 available
FLASH: 0x05800000 - 0x05a00000, 32 blocks of 0x00010000 bytes each.
==> enter ^C to abort booting within 3 seconds ......

Start to run system initialization task.
[System Configuration]
Company Name   :
Model Name   : CL-MCSFP-16M
MAC   Address   : 00:00:00:00:00:88

Firmware version : 1.00.01 (built at Jun   2 2011 10:50:54)
Username:

<< User Modes >>
There are two user modes for the device - one is administrator mode (privileged mode), another is guest mode (normal mode).

[administrator mode]

The default user name and password is "**admin**" / "**admin**".

After login the device, a prompt will be shown.   Because this device supports command-line for console interface, you can press "**?**" to check the command list first.

With "**?**" command, you can find the command list as follow.

```
-------------------------------------------------------------------------------------
# ?
   exit                  Exit from current mode
   help                   Show available commands
   history              Show a list of previously run commands
   logout                Disconnect
   ping                   Sends ICMP echo packets to other network nodes
   quit                  Quit commands
   reload                Halts and performs a warm restart
   show                    Shows information
   calendar              Data and time information
   configure             Enter configuration mode
   copy                   Copies from one file to another
#
-------------------------------------------------------------------------------------
```

These are the basic system commands for the device.

For system configuring, "**configure**" command can enter the configure mode.   And the prompt will become ...

```
---------------------------------------------------------------
# configure
xxxx(config)#
---------------------------------------------------------------
```

In the configure mode, the general configuration of the device can be done.   And "exit" command can leave this mode.

If settings for port, "**interface**" command is used.   And the prompt will become ...

```
---------------------------------------------------------------
xxxx(config)# interface ethernet 1/5
xxxx(config-if)#
---------------------------------------------------------------
```

"ethernet 1/5" means Ethernet interface 1, port 5.   And "exit" command can leave this mode.

"interface" command has another sub-command "**vlan**".   IP address of the device can be configured in this mode.

```
---------------------------------------------------------------
```

```
xxxx(config)# interface vlan 1
xxxx(config-if)#
---------------------------------------------------------------
```

[guest mode]
If "**guest**" / "**guest**" is used for username / password, the console interface will enter guest mode.   Its prompt is ended with "**>**".   With "**?**" command, you can find the command list as follow.

```
------------------------------------------------------------------------------------------
> ?
   exit                 Exit from current mode
   help                  Show available commands
   history              Show a list of previously run commands
   logout               Disconnect
   ping                  Sends ICMP echo packets to other network nodes
   quit                 Quit commands
   show                  Shows information
>
------------------------------------------------------------------------------------------
```

In guest mode, it is allowed to view the device configuration only.   No setup/ configure commands are supported.

<< Function Keys >>
Here is the function keys for console interface.

[**Tab**] key: this key can help to get the full command keyword with just several beginning letters.   For example, "cal-Tab" will get the full "calendar" command word.
[**Esc**] key: this key can use to break message display and go back to command prompt.
[**Up-Arrow**] key: this key can get last input command.
[**Down-Arrow**] key: this key can get next input command.
[**Left-Arrow**]/[**Right-Arrow**] key: the key can move the cursor.
[**Backspace**] key: this key can delete the letter in front of cursor
[**?**] key: this key can get the command list.

<< Command Mode >>
There are three command modes for console interface.

1. General Basic Commands

These are basic commands after login. Users can show device configueartion/status, ping network device, reboot device, ... The prompt is "**xxx#**" for admin user, and "**xxx>**" for guest user.

2. Configure Mode Commands

With "configure" command, user can enter Configure Mode. Commands in Configuring Mode are for general device settings. And its prompt is "**(config)#**".

3. Interface Configuring Commands for Port Group

If the settings are for ports, it is done with "interface ethernet 1/x" command in configure mode. And the prompt will become "**(config-if)#**". For example, "interface ethernet 1/5" is for settings on Port 5.

7.2.2 General Basic Commands

When "admin" / "admin" is used for username/password, the console will enter administrator mode.   Enter "?", command list will be shown.

```
---------------------------------------------------------------------------------------
# ?
  exit                    Exit from current mode
  help                     Show available commands
  history                 Show a list of previously run commands
  logout                   Disconnect
  ping                     Sends ICMP echo packets to other network nodes
  quit                    Quit commands
  reload                  Halts and performs a warm restart
  show                     Shows information
  calendar                Data and time information
  configure               Enter configuration mode
  copy                     Copies from one file to another
#
---------------------------------------------------------------------------------------
```

1. **exit** command
   This command is used to leave current operation mode.   It will do logout at this basic command interface.

2. **help** command
   This is a help command and the console will prompt with all available commands.

3. **history** command
   This command will show the history of entering commands.

4. **logout** command
   This is a logout command.

5. **ping** command
   User can use this command to ping another network device to verify the network connection and activity.   (It is similar to the ping command in MS-DOS.)

Enter "ping ?" at the prompt, the command syntax will be shown.
ping ?
Syntax: ping [-n count] [-l length] [-t] [-w timeout] ip
-n count   : Number of echo requests to send.
-l length : Send buffer size, and length is between 64~8148
-t   : Ping the specified host until stopped by <ESC> key.
-w   : Timeout in milliseconds to wait for each reply.
ip   : IP address (xxx.xxx.xxx.xxx)

For example, "ping 192.168.1.80".   "Esc" can be used to break
continuous ping operation.

6. **quit** command
   This command is used to quit the console interface.

7. **reload** command
   This command is used to reset device.   It will halt and perform a warm
   restart.
   Enter "reload" at the prompt, you will be asked to confirm the action.
   # reload
   Are you sure to reset now?(Y/N)

   If "y" is entered, the device will reboot.   If "n" is entered, just leave and
   no any action will go.

8. **show** command
   This command is used to show current system information and system
   configuration.

   Enter "show ?" at the prompt, the sub-command list will be shown.
   # show ?
     aaa   Show AAA service configuration
     calendar   Date and time information
     history   History information
     interface   Interface information
     ip   IP information
     line   TTY line information
     log   Log records
     management   Management IP filter
     radius-server   RADIUS server information
     running-config   Information on the running configuration
     snmp   Simple Network Management Protocol statistis
     sntp   Simple Network Time Protocol configuration
     system   System information

version   System hardware and software versions

With sub-commands, function configuration settings will be displayed. And more help information for functions will be prompted with "show xxxx ?" (xxxx is the sub-command).   For example, entering "show ip ?" will get the prompt message...

show ip ?
   interface   Interface information
   redirects   Default gateway configured for this device

And entering "show ip redirects" will get the gateway settings...
show ip igmp redirects
gateway: 192.168.1.254

If the display is more than one console page, "Esc" can be used to break the display.

For the details, please refer to section **7.2.6 Show commands**.

9. **calendar** command
This command is used to set the system time.   It is entered in <hour minute second month day year> order.
For example,
calendar set 10 30 0 october 15 2008
show calendar
Current Time : 2008/10/15-10:30:18

It is 18 seconds passby after the setting command.

10. **configure** command
This command will change the console interface to configure mode. And the prompt will become "(config)#".   In this mode, administrator can do system configuration of the device.

The operation of configure mode will be described in next section.

"exit" command can be used to quit this operation mode.

11. **copy** command
This command is used to backup system configuration/firmware to TFTP server, restore system configuration from TFTP server, and update firmware from TFTP server.

```
# copy ?
    binary-config          Copies binary configuration file
    config                 Copies configuration file
    firmware               Copies run-time firmware
```

copy binary-config running-config tftp xxx.xxx.xxx.xxx yyy command is used to backup current device running configuration to TFTP Server at IP "xxx.xxx.xxx.xxx" as file name "yyy" in binary format.
copy binary-config tftp running-config xxx.xxx.xxx.xxx yyy command is used to restore binary configuration file "yyy" from TFTP Server at IP "xxx.xxx.xxx.xxx".

copy config running-config tftp xxx.xxx.xxx.xxx yyy command is used to backup current device running configuration to TFTP Server at IP "xxx.xxx.xxx.xxx" as file name "yyy" in text format.
copy config tftp running-config xxx.xxx.xxx.xxx yyy command is used to restore text configuration file "yyy" from TFTP Server at IP "xxx.xxx.xxx.xxx".

copy firmware running-firmware tftp xxx.xxx.xxx.xxx yyy command is used to backup current running firmware to TFTP Server at IP "xxx.xxx.xxx.xxx" as file name "yyy" in binary format
copy firmware tftp running-firmware xxx.xxx.xxx.xxx yyy command is used to update the running firmware file "yyy" from TFTP Server at IP "xxx.xxx.xxx.xxx".

7.2.3 Configure Mode Commands

Entering "**configure**" command at console interface, the prompt will become ...
"(config)#".
All the general settings for the device can be done in this mode.

If the settings are for ports, it is done with "interface" command in configure mode.   For example, "interface ethernet 1/5" is for settings on Port 5 and "interface ethernet 1/5,6,10-15" is for settings on Port 5, 6, 10, 11, 12, 13, 14, 15.   Please refer to next section for the details of this command.

Enter "?" at the prompt, the sub-command list will be shown.

```
-------------------------------------------------------------------------------------
(config)# ?
  exit               Exit from current mode
  help                Show available commands
  history            Show a list of previously run commands
  logout              Disconnect
  quit               Quit commands
  aaa                 AAA Service
  default            Restore to factory default setting
  end                 Exit from configure mode
  hostname            Sets system's network name
  interface          Enters privileged interface configuration
  ip                  Global IP configuration sub commands
  logging             Modifies message logging facilities
  management            Specifies management IP filter
  no                  Negates a command or sets its defaults
  prompt              Sets system's prompt
  radius-server       Configures login to RADIUS server
  snmp-server         Modifies SNMP server parameters
  sntp               Simple Network Time Protocol configuration
  username             Establishes user name authentication
-------------------------------------------------------------------------------------
```

1 **exit** command
   This command is used to leave current operation mode.   Go back to last mode.

2 **help** command
   This command is used to show all the available commands in this

mode.

3 **history** command
This command is used to show the history of entering commands.

4 **logout** command
This command is used to logout from console interface.

5 **quit** command
This command is used to quit from console interface.   It has the same function as logout.

6 **aaa** command
This command is used to set the authentication manner for administrator of the device when login by http(s)/telnet for management. It could be authenticated by local device or by RADIUS Server.

Here is the command for the setting.
aaa authentication login local command will set the authentication manner for administrator by local device when login by http(s)/telnet for management.
aaa authentication login radius command will set the authentication manner for administrator by RADIUS Server when login by http(s)/telnet for management.
aaa authentication login local radius command will set the authentication manner for administrator by local device first when login by http(s)/telnet for management.   If authentication fail, try by RADIUS Server next.

RADIUS Server is set by **radius-server** command for command line interface or set in Security function for web interface.

7 **default** command
This command is used to restore factory default settings.   Before start it, a confirm message wil be prompted.

8 **end** command
This command is used to exit from configure mode.

9 **hostname** command

This command is used to set the name of the device in network.   This name is also used as the hostname for SNMP agent function of the device.

10 **interface** command

This command is used to entering **interface configuring mode**. There are two sub-commands for it - one is "ethernet", it is for port setting, another is "vlan", it is for device IP address setting on VLAN.

(config)# interface ?
  ethernet   Ethernet port
  vlan   Virtual LAN interface

All the port setting commands are put in interface configuring mode - like port name.   And characteristics settings for VLAN are also done in interface configuring mode - like IP address assignment.

For example, the console will enter interface configuring mode for Port 5 with "interface ethernet 1/5" command.   And the prompt will become ...

(config)# interface ethernet 1/5
(config-if)#

With "interface ethernet 1/5,6,10-13", the console will enter interface configuring mode for Port 5, 6, 10, 11, 12, 13.   And all the settings will be applied to those ports at the same time.

The description of commands in interface configuring mode is put in Section **7.2.4 Interface Configuring Commands**.   Please refer to the section for the details.

11 **ip** command

This command is used to configure some IP-depending functions.
Entering "ip ?", the sub-commands will be shown.

(config)# ip ?
  default-gateway   Specifies the default gateway
  http   HTTP server configuration

ip default-gateway x.x.x.x command is used to specify the default gateway of IP configuration of the device.   x.x.x.x is the IP address of

the gateway device.

ip http ... command is used to configure http service of the device.
Entering "ip http ?", the sub-command will be shown.
(config)# ip http ?
  secure-server   Enable secure HTTP server
  server   Enable HTTP server

ip http secure-server command is used to enable the SSL function of
http service (https) of the device. And **no ip http secure-server**
command can be used to disable it.
ip http server command is used to enable http service of the device.
And **no ip http server** command can be used to disable it.
Because hacker or worm/virus (like ColdRed) often attacks http
server, this command is provided to enable/disable http service to
prevent it. (If this device is installed in public Internet without any
firewall protection, we suggest users to disable the http interface and
use Telnet or SNMP instead.)

12 **logging** command
This command is used to configure logging function of the device. The
logging function can record events at local flash or remote log server.
Entering "logging ?", the sub-commands will be shown.
(config)# logging ?
  log-level   Log level
  on   Enable logging to all supported destination
  remote-log   Enable logging to remote host
  clear   Clear logging table information

logging log-level x command is used to define the log level of events.
The valid value of "**x**" is 0~7.
logging on command is used to enable the logging function. And **no
logging on** command is used to disable the logging function.
logging remote-log command is used to configure remote logging
function. Entering "logging remote-log ?", the sub-commands will be
shown.
(config)# logging remote-log ?
  <1-5>   Index
  <cr>

logging remote-log command is used to enable the remote logging
function. Events will also be sent to syslog servers. **no logging
remote-log** command is used to disable it.
logging remote-log x host y.y.y.y command is used to set IP

27

address "y.y.y.y" for syslog server indexed "x".   Up to five (x=1~5) syslog servers are supported.

logging clear command is used to clear log table.

13 **management** command

This command is used to setup management interface security function.   The management interface security function can limit the IP / subnet / remote interfaces(http,telnet,snmp) / access right(view,modify) for management from network.   Different administrators could have different rights to manage this device.   This is for security of this management device.   (Four user groups are supported for this function.)

Entering "management ?", the sub-commands will be shown.
(config)# management ?
  <1-4>   Index
(config)# management 2 ?
  enable   Set enable for a specified set
  ipaddr   Set IP and net mask for a specified set
  mode   Set mode for a specified set
  protocol   Set protocol for a specified set

management x enable command is used to enable the security settings for some user groups ("**x**" is the index of the user group).   And **no management x enable** command can be used to disable it.   And users in this group are allowed to manage this device remotely.
management x ipaddr y.y.y.y z.z.z.z command is used to set the IP/subnet for some user groups ("**x**" is the index of the user group, **y.y.y.y** is the IP address, **z.z.z.z** is the IP subnet mask).   Users in this IP subnet will belong to this users groups.
management x mode modify/view command is used to set the access right for some user groups ("**x**" is the index of the user group). If "management x mode modify" command, users in this groups have "modify" right for management.   If "management x mode view" command, users in this groups have "view" right only.
management x protocol http|snmp|telnet command is used to enable the remote management protocol for some user groups ("**x**" is the index of the user group). More than one protocols can be enabled at the same time - e.g. "management 2 protocol http snmp telnet".   And **no management x protocol** command is used to disable all remote management protocols for the user group.

14 **no** command
This command can do the following settings.   And it depends on the command after it.

1) **Disable a function**.For example, "logging" command can enable the logging function and "no logging" command can disable it.

2) **Restore a setting to factory default of the device**.   For example, "ip default-gateway 192.168.1.100" will set the IP gateway of the device to 192.168.1.100, and "no ip default-gateway" will put it to factory default setting 192.168.1.254.

3) **Clear a setting**.   For example, "hostname abc" will set the SNMP host name as "abc".   And "no hostname" will clear this setting.

Entering "no ?", the sub-commands will be shown.
```
# no ?
  aaa                 AAA Service
  hostname             Sets system's network name
  ip                  Global IP configuration sub commands
  logging             Modifies message logging facilities
  management           Specifies management IP filter
  radius-server       Configures login to RADIUS server
  snmp-server          Modifies SNMP server parameters
  sntp                Simple Network Time Protocol configuration
```

15 **prompt** command
This command is used to set the prompt word for command line interface.
For example,
```
(config)# prompt AAA
AAA(config)#
```

16 **radius-server** command
This command is used to configure the settings of RADIUS Server for administrator authentication operation.   This device supports two RADIUS Servers for redundant applications.

Entering "radius-server x ?" (x=1 for first RADIUS Server. x=2 for second RADIUS Server.), the sub-commands will be shown.
```
(config)# radius-server ?
  active                Active the RADIUS server
  host                  Specifies the RADIUS server
```
29

key	Sets the RADIUS encryption key
port	Sets the RADIUS server network port

radius-server x active command is used to activate RADIUS Server x. "**x**" is 1 or 2.(x=1 for first RADIUS Server. x=2 for second RADIUS Server.)

radius-server x host y.y.y.y command is used to set the IP address of RADIUS Server x. "**x**" is 1 or 2.(x=1 for first RADIUS Server. x=2 for second RADIUS Server.). "**y.y.y.y**" is the IP address.

radius-server x key yyy command is used to set the security key to handshake with RADIUS Server x. "**x**" is 1 or 2.(x=1 for first RADIUS Server. x=2 for second RADIUS Server.) "**yyy**" is the key string.

radius-server x port y command is used to set the communication port of RADIUS Server x. "**x**" is 1 or 2.(x=1 for first RADIUS Server. x=2 for second RADIUS Server.) "**y**" is the port number and its valid value is 1~65535

17 **snmp-server** command

This command is used to configure SNMP operation of the device.

Entering "snmp-server ?", the sub-commands will be shown.
(config)# snmp-server ?

<1-5>	Index of Trap
community	Defines SNMP community access string
contact	Sets the system contact string
location	Sets the system location string
username	Sets the snmpv3 user informations
version	Sets the snmp version

snmp-server community get xxx command is used to set the community string of get command for SNMP operation. "**xxx**" is the community string.

snmp-server community set xxx command is used to set the community string of set command for SNMP operation. "**xxx**" is the community string.

snmp-server contact xxx command is used to set the contact information for this device. "**xxx**" is the contact information string.

snmp-server location xxx command is used to set the location information for this device. "**xxx**" is the location information string.

snmp-server version x command is used to select the SNMP operation version. "**x**" could be **v1**, **v2c**, **v3**, **v3v2c**, **v3v2cv1**.

The following commands are for SNMPv3 function.

snmp-server username xxx securitylevel y command is used set security level of user xxx. "**xxx**" is the user name. "**y**" could be **noauth**, **auth**, or **priv**.

- "noauth" : no authentication, no encryption
- "auth" : do authentication, no encryption
- "priv" : do authentication and encryption(by DES)

snmp-server username xxx authentication y command is used to set the authentication manner. "**xxx**" is the user name. "**y**" could be **md5**or **sha**.

18 **sntp** command

This command is used to configure SNTP protocol of the device.

Entering "sntp ?", the sub-commands will be shown.
(config)# sntp ?
    client   Accepts time from specified time server
    server   Specified one time server
    zone   Set time zone
    dst   Config daylight saving time function.
    start-time   Set start time of daylight saving time
    end-time   Set end time of daylight saving time

sntp client command is used to enable SNTP protocol. And **no sntp client** command can be used to disable it. If it is disabled, the system time will be got from manual setting.

sntp server x.x.x.x command is used to set the IP address of network time server for SNTP protocol operation. "**x.x.x.x**" is the IP address.

sntp zone xxx command is used to set the time zone. "**xxx**" is the location of the time zone. With "sntp zone ?", the locations will be shown.

sntp dst command is used enabled Daylight Saving Time function. And **no sntp dst** command can be used to disabled it. Daylight Saving Time function will set the system time one-hour early than normal time in a period of time. "start-time" and "end-time" sub-commands can be used to set the time period.

sntp start-time w/x/y/z command is used to set the start time of Daylight Saving Time.

- "**w**" is the week number in the month. Its value is 1~5.
- "**x**" is the day number in the week. Its value is 0~6.
- "**y**" is the month number. Its value is 1~12.
- "**z**" is the hour number in the day. Its value is 0~23.

sntp end-time w/x/y/z command is used to set the end time of Daylight Saving Time.

- "**w**" is the week number in the month. Its value is 1~5.
- "**x**" is the day number in the week.   Its value is 0~6.
- "**y**" is the month number.   Its value is 1~12.
- "**z**" is the hour number in the day.   Its value is 0~23.

19 **username** command

This command is used to set the username and password for administrator and guest.

username admin www xxx yyy zzz command is used to set the username and password for administrator.   "**www**" is the old username.   "**xxx**" is the old password.   "**yyy**" is the new username.   "**zzz**" is the new password.

username guest yyy zzz command is used to set the username and password for guest.   "**yyy**" is the new username.   "**zzz**" is the new password.

Administrator is the user who has the right to do configuration modification.   Guest is the user who has the right to view configuration only.

7.2.4 Interface Configuring Commands

Commands in Configuring Mode are for general device settings.   And its prompt is "(config)#".

The port interface function and VLAN interface function are set with "interface" command.
(config)# interface ?
  ethernet   Ethernet port
  vlan   Virtual LAN interface

interface ethernet 1/x command is used to configure settings for **Port x**. Please refer to section **7.2.4.1 Interface Configuring Commands for Port** for the details.

interface vlan x command is used to configure **VLAN x** ("x" is the VLAN ID).   Please refer to section **7.2.4.2 Interface Configuring Commands for VLAN** for the details.

Both commands will change the prompt from "(config)#" to "**(config-if)#**".

7.2.4.1 Interface Configuring Commands for Port

Commands in Configuring Mode are for general device settings.   And its prompt is "(config)#".

If the settings are for ports, it is done in port interface configuring mode. Port interface configuring mode is entered with "**interface ethernet 1/x**" command in configure mode.   For example, "interface ethernet 1/5" is for settings on Port 5.

Some syntax are supported for port selection.

1. **interface ethernet 1/x** and "**x**" is port number. All the settings after this command will be applied to this port.   For example, "interface ethernet 1/5" and all the settings after this command will be applied to Port 5.
2. **interface ethernet 1/x,y,z,...** and "**x**", "**y**", "**z**",.. are port number.   All the settings after this command will be applied to these ports.   For example, "interface ethernet 1/2,4,7" and the settings after this command will be applied to Port 2, Port 4, and Port 7.
3. **interface ethernet 1/x-y** and "**x**","**y**" are port number.   All the settings after this command will be applied to ports in this range.   For example, "interface ethernet 1/4-7" and the settings after this command will be applied to Port 4, Port 5, Port 6, and Port 7. (Port 4~7)
4. **interface ethernet 1/w,x,..,y-z** and "**w**","**x**","**y**","**z**" are port number.   All the settings after this command will be applied to those ports.   For example, "interface ethernet 1/1,2,4-7" and the settings after this command will be applied to Port 1, Port 2, Port 4, Port 5, Port 6, and Port 7. (Port 4~7)

Entering "interface ethernet 1/5", and its prompt will become ...
(config)# interface ethernet 1/5
(config-if)#

Enter "?" at the prompt, the sub-command list will be shown.

```
---------------------------------------------------------------------------------------
(config-if)# ?
   exit                 Exit from current mode
   help                  Show available commands
   history              Show a list of previously run commands
   logout                Disconnect
   quit                 Quit commands
   description          Interface specific description
   end                   Exit from interface mode
   interface            Enters privileged interface configuration
   lpt                  Enable link Pass-through
   no                    Negates a command or sets its defaults
```

```
        shutdown                Shuts down the selected interface
        speed                   Configures speed operation
-----------------------------------------------------------------------------------------
```

1 **exit** command
   This command is used to leave current operation mode.   Go back to
   last mode.

2 **help** command
   This command is used to show all the available commands in this
   mode.

3 **history** command
   This command is used to show the history of entering commands.

4 **logout** command
   This command is used to logout from console interface.

5 **quit** command
   This command is used to quit from console interface.   It has the same
   function as logout.

6 **description** command
   This command is used to assign a description string for the port(s).

   description xxx command will assign a description string for the
   port(s).   "**xxx**" is the string.
   no description command will clear the description string.

7 **end** command
   This command is used to exit from interface mode.
   (config-if)# end
   (config)#

8 **interface** command
   This command is used to change the interface port(s) or interface

VLAN for next setup commands.
(config-if)# interface ?
   ethernet   Ethernet port
   vlan   Virtual LAN interface

For example,
"(config)# interface ethernet 1/5" will set current setup interface to Port 5 and all the commands will be applied to Port 5.
"(config-if)# interface ethernet 1/6-7" will change current setup interface to Port 6-7 and all the commands will be applied to Port 6-7.

If "vlan" sub-command is used, current setup interface will be changed to some VLAN.   For example,
"(config-if)# interface vlan 100" will change current setup interface to VLAN 100 and all next commands will be applied to VLAN 100.

The description of commands in interface configuring mode is put in Section **7.2.4 Interface Configuring Commands**.   Please refer to the section for the details.

9 **lpt** command
This command can be used to enable link pass-through function of the TX-SFP pair.   Link pass-through function can make the link status of TX port and SFP port follow each other.   Only both of them are link up, then they will be link up.   That will make the link status being transparent after media conversion.
no lpt command can be used to disable it.

10 **no** command
This command can do the following settings.   And it depends on the command after it.

1) Disable a function.
2) Restore a setting to factory default of the device.
3) Clear a setting.   For example, "description abc" will set the description of the port(s) as "abc".   And "no description" will clear this setting.
4) Remove port(s) from a function.

Here is the sub-commands.
(config-if)# no ?
   description   Interface specific description

11 **shutdown** command
This command is used to disable the interface port(s).

shutdown command is used to disable the interface port(s).
no shutdown command is used to enable it.

12 **speed** command
This command is used to set the operation speed of the interface port(s).

```
(config-if)# speed ?
  auto                 Set port speed to be auto
  100                  Set port speed to be 100M
  1000                 Set port speed to be 1G
```

speed auto command will set the interface port(s) to auto-detect 100M or 1000M operation speed.
speed 100 command will set the interface port(s) to 100M speed.
speed 1000 command will set the interface port(s) to 1000M(gigabit) speed.

7.2.4.2 Interface Configuring Commands for VLAN

Commands in Configuring Mode are for general device settings.   And its prompt is "(config)#".

If the characteristics are for VLAN, it is done with "**interface vlan x**" command in configure mode.   For example, "interface vlan 1" is for characteristics settings on VLAN 1.

Entering "interface vlan 1", and its prompt will become ...
(config)# interface vlan 1
(config-if)#

Enter "?" at the prompt, the sub-command list will be shown.

```
--------------------------------------------------------------------------------------
(config-if)# ?
   exit                     Exit from current mode
   help                      Show available commands
   history                  Show a list of previously run commands
   logout                    Disconnect
   quit                      Quit commands
   interface                Enters privileged interface configuration
   ip                         Internet protocol
   no                          Negates a command or sets its defaults
--------------------------------------------------------------------------------------
```

1. **exit** command
   This command is used to leave current operation mode.   Go back to last mode.

2. **help** command
   This command is used to show all the available commands in this mode.

3. **history** command
   This command is used to show the history of entering commands.

4. **logout** command
   This command is used to logout from console interface.

5. **quit** command

   This command is used to quit from console interface.   It has the same function as logout.

6. **interface** command

   This command is used to change to interface port(s) or another interface VLAN for next setup commands.

   (config-if)# interface ?
      ethernet   Ethernet port
      vlan   Virtual LAN interface

   For example,
   "(config)# interface ethernet 1/5" will change the setup interface to Port 5 and all the following commands will be applied to Port 5.
   "(config-if)# interface ethernet 1/6-7" will change the setup interface to Port 6-7 and all the following commands will be applied to Port 6-7.

   If "vlan" sub-command is used, the setup interface will be changed to some VLAN.   For example,
   "(config-if)# interface vlan 100" will change the setup interface to VLAN 100 and all following commands will be applied to VLAN 100.

   The description of commands in interface configuring mode is put in Section **7.2.4 Interface Configuring Commands**.   Please refer to the section for the details.

7. **ip** command

   This command is used to set IP address of the device on this VLAN interface.   And only users in this VLAN can access this device with the IP address remotely.

   (config-if)# ip address ?
      dhcp   Dynamic host configuration protocol
      A.B.C.D   IP address
      renew   Renew IP
      release   Release IP

   ip address dhcp command is used to enable DHCP client function. DHCP client function will try to get IP configuration from DHCP server in network.   And **no ip address dhcp** command can be used to disable it.

ip address x.x.x.x y.y.y.y command is used to set IP address of the device on this VLAN. "**x.x.x.x**" is the IP address. "**y.y.y.y**" is the subnet mask.

For example, "ip address 192.168.1.12 255.255.255.0" will set the IP address of the device on this VLAN group for remote management.

ip address renew command is used to refresh the lease time of the IP address got by DHCP. If IP configuration is not got when boot-up, this command will try to get IP configuration again.

ip address release command is used to release current IP address got by DHCP. Then, you can try to get the IP configuration again by "ip address renew" command.

8. **no** command

This command is used to disable a function or restore a setting to factory default of the device.

(config-if)# no ?
  ip   Internet protocol

For example,

"**ip address dhcp**" command can enable DHCP client function on the VLAN group interface and "**no ip address dhcp**" command can disable it.

"**ip address x.x.x.x y.y.y.y**" command can set the IP address x.x.x.x on the VLAN group interface and "**no ip address**" command can set it to default settings - "192.168.1.1".

7.2.5 Show Commands

Show command is put in General Basic Commands for viewing system configuration and information.

Enter "show ?" at the prompt, the sub-command list will be shown.

```
-----------------------------------------------------------------------------------------
# show ?
    aaa                     Show AAA service configuration
    calendar                Date and time information
    history                 History information
    interface               Interface information
    ip                      IP information
    line                    TTY line information
    log                     Log records
    management              Management IP filter
    radius-server           RADIUS server information
    running-config          Information on the running configuration
    snmp                    Simple Network Management Protocol statistis
    sntp                    Simple Network Time Protocol configuration
    system                  System information
    version                 System hardware and software versions
-----------------------------------------------------------------------------------------
```

1. **show aaa authentication login** command
   This command will show the authentication settings for admin of the device when login for management.   It could be authenticated by local or RADIUS Server, or local first RADIUS Server next.
   For example,
   # show aaa authentication login
   Authentication:
            local

2. **show calendar** command
   This command will show current system time.
   For example,
   # show calendar
   Current Time : 2008/08/29-11:27:12

3. **show history** command
   This command is used to show the history of input commands.
   # show history
      0. show

1. show history

4. **show interface** command
   This command is used to show port information and status.

   ```
   # show interface ?
     counters              Interface counters information
     mgmtport              Interface management port information
     status                Interface status information
     switchport            Interface switchport information
   ```

   show interface counters command will show total statistics counters for all ports.
   show interface counters ethernet 1/x command will show statistics counters for Port x. ("**x**" is the port number).
   For example,
   ```
   # show interface counters ethernet 1/3
   Port: 1/3
   ========================================
   TX Port Counter                 Statistics
   Receive Good Packet                 0
   Receive CRC Error Packet            0
   ========================================
   SFP Port Counter                Statistics
   Receive Good Packet                 0
   Receive CRC Error Packet            0
   ```

   show interface mgmtport command will show current management LAN port link status.

   show interface status command will show port status of all ports (one after another).
   show interface status ethernet 1/x command will show port status of Port x.   ("**x**" is the port number).
   For example,
   ```
   # show interface status ethernet 1/3
   Information of Eth 1/3
     Name:               Port 3
     Admin:              Enable
     Speed:              Auto
     Link Pass-through:  Enable
     TX-Link:            DOWN
     SFP-Link:           DOWN
   ```

show interface switchport command will show DDMI information /status of all ports (one after another).

show interface switchport ethernet 1/x command will show DDMI information/status of Port x. ("**x**" is the port number).

For example,

```
# show interface switchport ethernet 1/1
 Digital Diagnostics Monitoring Interface of Eth 1/1
 Serial Info Table
 Status:                    ok_with_DDM
 Vendor:                    xxxxxxxx
 PartNo:                    xxxxxxxx
 SerialNo:                  xxxxxxxx
 Revision:
 DateCode:                  xxxxxxxx
 Transceiver:               1000BASE-SX
```

```
 Ddm Info Table
```

Type	AlarmMax	AlarmMin	WarnMax	WarnMin	Current
Temperature(0.01℃)	9500	-3200	9000	-2500	4212
Voltage(0.01mV)	363	297	356	304	331
TxBias(0.01mA)	1300	200	1200	300	816
TxPower(0.01mW)	79	12	63	14	35
RxPower(0.01mW)	100	2	79	3	0

5. **show ip** command

This command is used to show current device IP configuration.

```
# show ip ?
  interface              Interface information
  redirects              Default gateway configured for this device
```

show ip interface command will show current device IP configuration.

For example,
```
# show ip interface
IP address and netmask: 192.168.1.12 255.255.255.0 on VLAN 1
```

show ip redirects command will show current IP gateway setting of the device.

For example,
```
# show ip redirects
gateway: 192.168.1.254
```

6. **show line** command

This command is used to show current console line configuration.

show line console command is used to show current console line configuration.
```
# show line console
Password threshold: open-end time
Baudrate: 9600
Databits: 8
Parity   : 0 [0|1|2|3][NONE|EVEN|ODD|MARK|SPACE]
Stopbits: 1
```

7. **show log** command

This command is used to show current system log and system log configuration.

```
# show log ?
  configuration          logging configuration
  <cr>
```

show log command is used to show current system log content.
For example,
```
# show log
[5]  Sat Jan 01 10:20:31 2011
     Level: 6 User admin login from console
[4]  Sat Jan 01 10:17:29 2011
     Level: 6 User admin login from console
[3]  Sat Jan 01 10:14:29 2011
     Level: 6 User admin login from console
[2]  Sat Jan 01 10:14:23 2011
     Level: 6 Authentication Failure from console
[1]  Sat Jan 01 10:10:00 2011
     Level: 4 System Started
```

show log configuration command is used to show current system log configuration.
For example,
```
# show log configuration
 [System Log]
System Log Status      : Enable
Log Level(0-7): 7
Remote Log             : Disable
Remote Log Server IP : Empty
Remote Log Server IP : Empty
Remote Log Server IP : Empty
Remote Log Server IP : Empty
Remote Log Server IP : Empty
```

8. **show management** command
   This command is used to show device management security settings. The IP/subnet, access mode, and protocol functions security settings will be shown.

   For example,
   # show management
   [Management IP configuration]

Index	Enabled	Address / Net Mask	Mode	Http	Telnet	SNMP
1	Yes	0.0.0.0/0.0.0.0	Modify	Yes	Yes	Yes
2	No	0.0.0.0/255.255.255.255	View	No	No	No
3	No	0.0.0.0/255.255.255.255	View	No	No	No
4	No	0.0.0.0/255.255.255.255	View	No	No	No

9. **show radius-server** command
   This command is used to show settings of RADIUS Server for administrator authentication operation.

   For example,
   # show radius-server
   Server 1*
    Active   : Yes
    IP Address   : 192.168.1.222
    Port Number : 1812
    Security Key: 12345678

   Server 2*
    Active   : Yes
    IP Address   : 192.168.1.222
    Port Number : 1812
    Security Key: 12345678

10. **show running-config** command
    This command is used to show current running configuration of the device.

    For example,
    # show running-config
    !building running-config, please wait.....
    !
    sntp server 220.130.158.54
    !
    sntp zone japan
    !
    !

```
interface ethernet 1/1
!
!
interface ethernet 1/2
!
!
interface ethernet 1/3
!
!
interface ethernet 1/4
!
!
interface ethernet 1/5
!
!
interface ethernet 1/6
!
!
interface ethernet 1/7
!
!
interface ethernet 1/8
!
!
interface ethernet 1/9
!
!
interface ethernet 1/10
!
!
interface ethernet 1/11
!
!
interface ethernet 1/12
!
!
interface ethernet 1/13
!
!
interface ethernet 1/14
!
!
interface ethernet 1/15
!
!
interface ethernet 1/16
!
!
!interface vlan 1
ip address 192.168.1.1 255.255.255.0
```

```
!
!
!end
```

11. **show snmp** command

This command is used to show SNMP configuration of the device.

For example,
```
# show snmp
[SNMP Configuration]
Object ID      : 1.3.6.1.4.1.655.80.21
System up Time: 9248 (seconds)
System Name    :
Location       :
Contact name   :
Get Community : public
Set Community : private
[Trap Community]
ID   Status    Community          IP Address
1    Disabled  public             0.0.0.0
2    Disabled  public             0.0.0.0
3    Disabled  public             0.0.0.0
4    Disabled  public             0.0.0.0
5    Disabled  public             0.0.0.0
Version: V3V2cV1
Username: admin
SnmpSecurityLevel: noauth
Authentication: MD5
Privacy: Des
```

12. **show sntp** command

This command is used to show system time settings of the device.
(D.S.T. means Daylight Saving Time)

For example,
```
# show sntp
===================================
[Time Configuration]
===================================
Get Time By  : Manually
Time Server  : 220.130.158.54
Time Zone    : Japan(+9)(37)
Current Time : 2011/01/01-12:45:12
D.S.T. status: Disable
D.S.T. start : 1st/SUN/JAN/0:00
D.S.T. end   : 1st/SUN/JAN/0:00
```

```
===================================
```

13. **show system** command

This command is used to show general system information/configuration of the device.

```
For example,
# show system
System Configuration
Main Board Information:
Firmware Version:        1.00.01 (built at Jun   2 2011 10:50:54)
Mac Address:             00:00:00:00:00:88
Number of Ports:         16
DHCP Client:             Disable
Time Server:             Disable
System Log Status:       Enable
Remote Log:              Disable
Web server:              Enable
Web server port:         80
Web secure server:       Disable
Web secure server port:  443
```

14. **show version** command

This command is used to show system version information and model information.

```
For example,
# show version
Firmware Version:    1.00.01 (built at Jun   2 2011 10:50:54)
Number of Ports:     16
Model Name:          CL-MCSFP-16M
```

7.3 About Telnet and SNMP Management Interfaces

7.3.1 About Telnet Management Interface

If you want to use Telnet to manage the device from remote site, you have to set the IP/NetMask/Gateway address to the device first from console. Then use "**telnet <IP>**" command to connect to the device. Its operation interface is the same as console interface.

7.3.2 About SNMP Management Interface

If you want to use NMS to management the device from remote site, you have to set the IP/NetMask/Gateway address to the device and configure the SNMP setting of the device from console first. Then you can use SNMP management program to manage this device.

This device supports SNMP v1, v2c, and v3 agent function and MIB II(Interface), Private MIB. The default GET community name is "public" and SET community name is "private".

This device supports up to five trap receivers with different trap community names.

7.4 Management with Http Connection

Users can manage the device with Http Web Browser connection.   The default IP setting is **192.168.1.1** and NetMask **255.255.255.0**.   The default IP Gateway is **192.168.1.254**.   Before http connection, IP address configuration of the device could be changed first.

1 Please follow the instruction in Section 7.2 to complete the console connection.
2 Login in with "**admin**" (password is also "**admin**" by default.)
3 Use "**show ip interface**" command to check IP address of the device first.
4 If IP address needs to be changed, follow the steps ...
   4.1 Enter "**config**" command, and the prompt will become "(config)#".
   4.2 Enter "**interface vlan 1**" command, and the prompt will become "(config-if)#".
   4.3 Enter "**ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy**" command (**xxx.xxx.xxx.xxx** is the IP address and **yyy.yyy.yyy.yyy** is the netmask) to modify IP address of the device.
   4.4 Enter "**exit**" command to go back to "(config)#" prompt.
   4.5 If IP Gateway will be set, enter "**ip default-gateway xxx.xxx.xxx.xxx**" command to set the IP gateway of the device. (**xxx.xxx.xxx.xxx** is the IP address.)
   4.6 Enter "**exit**" command to go back to "#" prompt.
   4.7 Enter "**show ip interface**" to check the IP settings.
   4.8 Enter "**show ip redirects**" to check IP gateway setting.

After IP address configuration done and the management port of the device is connected to network, users can start Http connection by entering IP address of the device to the web address line in Web Browser.   A login screen will be prompted for user name and password. The default user name and password is **"admin"** / "**admin**".   Then the management homepage will appear.

CL-MCSFP-16M
1.00.01 (built at Jun 2 2011 10:50:54)

- Home
- System
- SNMP
- Security
- Port
- Tools

System Information

Main Board Information	
Firmware Version	1.00.01 (built at Jun 2 2011 10:50:54)
Mac Address	00:00:00:00:00:88
Number of Ports	16
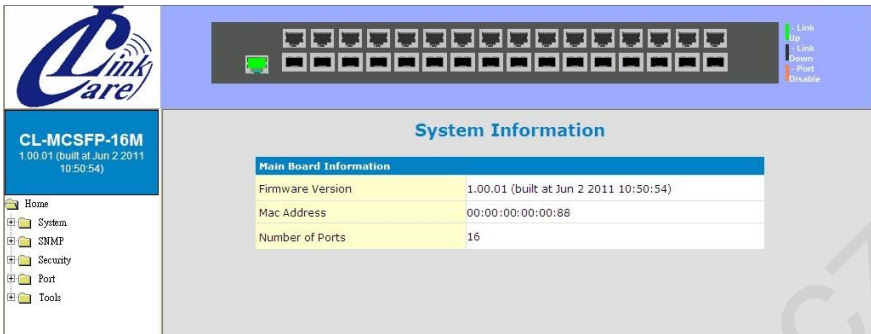
Left part of the homepage is a function list. Users can select one of them for status monitoring or device configuration.
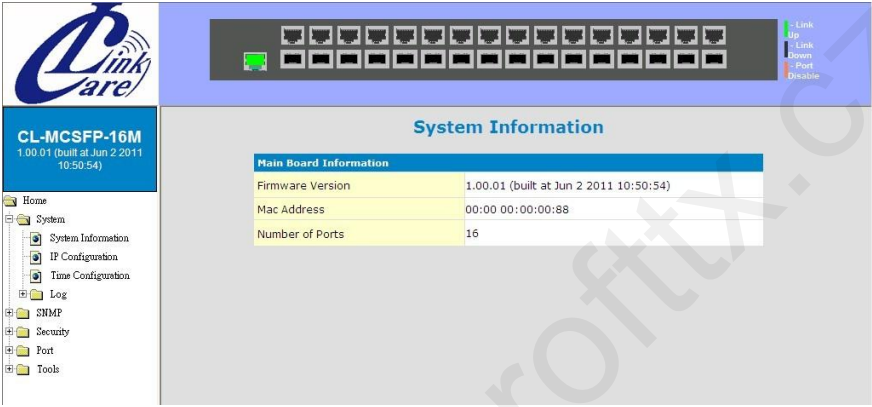
Upper part of the homepage is the link status of the device. Three different colors are used to show different status of ports – Link Up, Link Down and Port Disable.

Middle part of homepage is the main operation area for each function.
The details about management with http connection will be shown in the following sub-sections.

7.4.1 System

"System Information" is the homepage of the device.   And there are four sub-functions for it.

7.4.1.1   System Information

This function lists the system information about the device.   You can find the firmware version, Mac address, and connection port number here.

7.4.1.2 IP Configuration
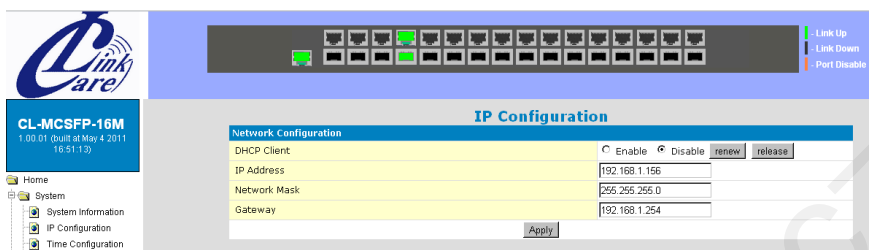
This function is used to setup IP configuration of the device.
You can enable DHCP client function to get IP configuration from DHCP server automatically.   Or, disable DHCP client function and set IP configuration manually.

About DHCP Client [renew] and [release] button ...
[renew] button: If DHCP client function is enabled, you can click [renew] button to refresh the lease time of the IP address.   If IP configuration is not got when boot-up, clicking [renew] button will try to get IP configuration again.
[release] button: If DHCP client function is enabled and IP configuration is got, clicking [release] button will release current IP configuration.   After that, you can click [renew] button to get the IP configuration again.

7.4.1.3 Time Configuration
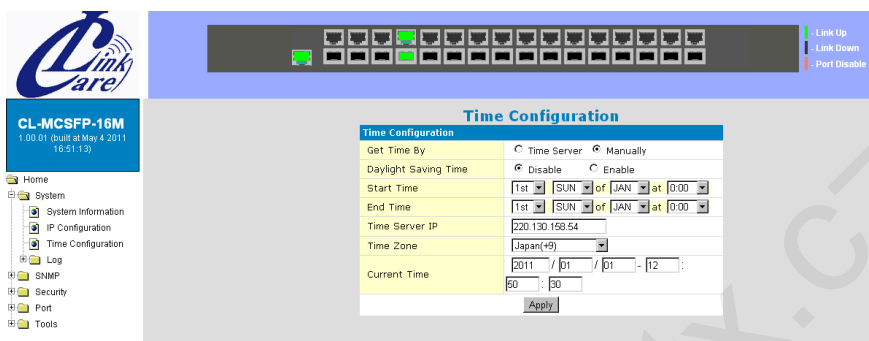
There are two ways to get the system time.

a). Get time from Time Server
This device support NTP protocol to get time from Internet time server. For such application, you have to select Get Time by "Time Server", input the IP of Time Server, and select the Time Zone of your location.   Then click [Apply]
If time is got from Time Server, it will be shown at "Current Time".
For such application, you have to get the IP of Time Server from your network administrator first.

b). Set time manually
This device can count time internal.   You can select Get Time by "Manually", and input current time manually.   Then click [Apply].

About [Daylight Saving Time] ...
Daylight Saving Time function will set the system time one-hour early than normal time in a period of time.   [Start Time] and [End Time] can be used to set the time period.

7.4.1.4 Log

[Configuration]

Users can configure System Log function and view log records here. If this function is enabled, the device will record events to a log file in flash.

Up to 512 records are allowed for local logging. If more than 512 events happen, the records will be overwritten from beginning. And if remote syslog server is applied, the device will also send event record to the syslog server.

About log function configuration ...
System Log Status : This can enable/disable system logging function.

Log Level (0~7) : Log levels 0~7 are defined as below. And events with lower log level than this number will be recorded.

Level	Name	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Informational	Informational messages
7	Debug	Debug-level messages

Remote Log : This can enable/disable remote syslog function.
Remote Log Server IP : This is the syslog server IP for remote logging. Up to five syslog servers is supported. Event logs will be sent to those

syslog servers at the same time.

[Log Table]

You can view log table content here.

There could be more than one page.   You may change the page or go to a page by its operation icons.

Clicking [clear log] button will clear the local log table.

7.4.2 SNMP

This function is used to configure SNMP function of the device. This device supports SNMP v1, v2c, and v3 agent function and MIB II(Interface), Private MIB.
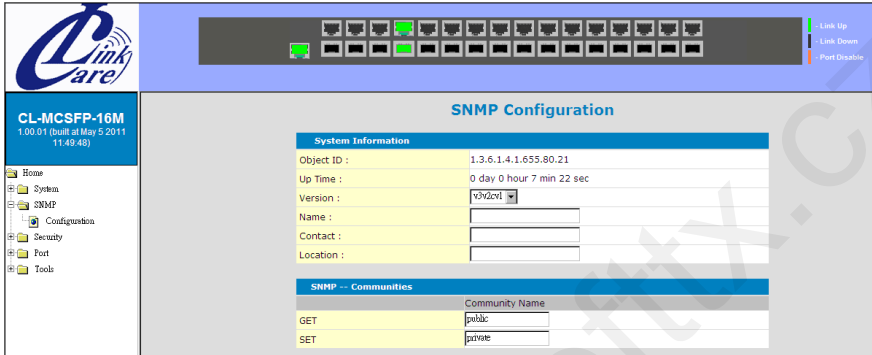
[System Information]
Object ID: this is the SNMP Object ID of the device for SNMP management.
Up Time: this is the power-up running time of the device.
Version: this is used to select SNMP agent operation version.
Name: this the host name of the device.
Contact: this is the contact information for the device.
Location: this is the location information of the device.

[SNMP -- Communities]
Get: this is the community string of GET command for SNMP operation. GET command is used to read device configuration/information.
Set: this is the community string of SET command for SNMP operation. SET command is used to set device configuration.

The switch configuration interface showing:

Name :	
Contact :	
Location :	

SNMP -- Communities

	Community Name
GET	public
SET	private

SNMP -- IP Trap Manager

IP Address		Community Name	Status
0.0.0.0		public	Disable
0.0.0.0		public	Disable
0.0.0.0		public	Disable
0.0.0.0		public	Disable
0.0.0.0		public	Disable

User Information

Index	Username	Security Level	Authentication	Privacy
1	admin	noauth	MD5	DES

Apply

[SNMP — IP Trap Manager]
Trap function will send notice message to SNMP management station when some events happen.   Up to five SNMP management stations are supported for Trap function.

The community string and enable/disable setting for each trap are set here.

[User Information]
This is used to configure SNMPv3 administrator settings.   The default user name is "admin".   The security level and authentication manner could be configured here.   The default encryption for privacy is by DES.

The security level could be ...
- **noauth** : no authentication, no encryption
- **auth** : do authentication, no encryption
- **priv** : do authentication and encryption(by DES)

The authentication manner could be **MD5** or **SHA**.

7.4.3 Security

This function is used to configure security functions of the device. The security functions are Administrator Management Security.

7.4.3.1 User Accounts (Administrator Management Security)
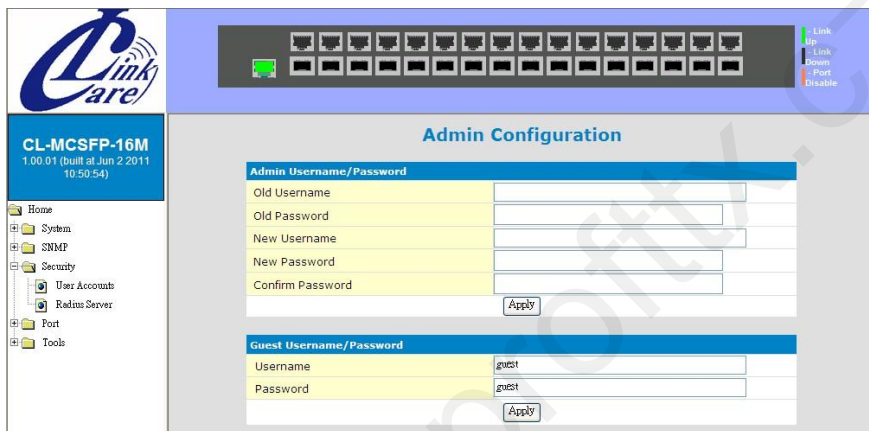
Administrator Username/Password : This is for network administrator to change his/her username and password. (Default is admin/admin.)

Guest Username/Password : This is used to setup the username/password for guest-right user who just can view the setting of the device.

Authentication : This is used to configure authentication for administrator when login.   It could be local, radius, or local-radius.

- local : authentication is done by local.
- radius : authentication is done by RADIUS Server.
- local-radius : authentication is done by local first. Then authentication is done by RADIUS Server if local authentication fails.

[Security Policy]
This is used to setup the IP addresses of administrators that can manage this device.   They have different access rights set in "Mode". And the remote management interfaces (Http/Telnet/SNMP) could be enable/disable for different administrators.   This function is for security policy of device management.

Note: Remember to enable at least one IP/Subnet with Modify right for Http/ Telnet/SNMP interface.   Otherwise, configuring device from remote will become impossible.   In that case, you can manage the device from console only.

7.4.3.2 RADIUS Server
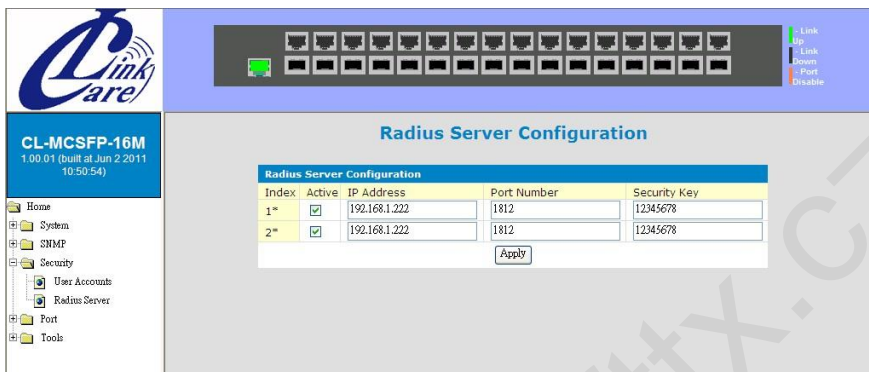
This function is used to configure RADIUS Servers for administrator authentication operation. This device supports two RADIUS Servers for redundant applications.

7.4.4 Port

This section is about configurations for ports.

7.4.4.1 Port Configuration

This function is used to configure port settings of the device.

Port Setting : It is for modifying the settings of port.   Follow the steps to do it.

1. Select the port that you want to modify in "Port#" first.
2. Fill the name of the port.
3. "Admin" is for port enable/disable setup.
4. "Speed" could be auto, 1000M, or 100M.
5. "Link Pass-through" is for link pass-through function enable/disable.
6. Click [Apply] after any modification.

[Current Setting & Link Status]

It is current setting and link status of ports.
- **Name**: The name of the port.
- **Admin**: enable/disable status of the port.
- **Speed**: speed setting of the port.
- **Link Pass-through**: link pass-through function enable/disable status
- **TX-Link**: TX port link status
- **SFP-Link**: SFP port link status

7.4.4.2 Port Statistics

Port statistics counters could be read here.
Select a port to get its counters.

[Refresh]
The counters will be refreshed automatically.   You can modify the refresh interval.
And you can click [Refresh] to refresh the counters immediatelly.

[Reset Counters]
Click [Reset Statistics] can reset all counters to "0".

7.4.4.3 DDMI

SFP Module DDMI information/status can be monitored here.
Select a port to get the SFP Module DDMI information/status.

[Serial Info Table]
This table will show information about the SFP module - like vendor, part number, serial number, revision, date code, and transceiver mode.

[Ddm Info Table]
This table will show current operating voltage, temperature, transmit bias, transmit power, and receive power of SFP module. And the maximum and minimum limit will be shown in the table. If the limit is met, the device will send a SNMP trap for it.
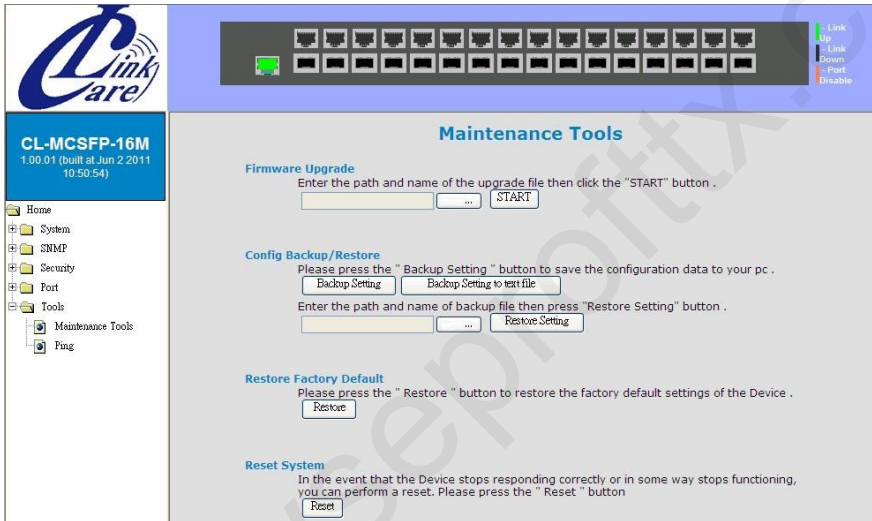
[Refresh]
You can click [Refresh] to refresh the values.

7.4.5 Tools

The follow functions are used for system maintenance. They are Software Upgrade, Configuration Backup/Restore, Restore Factory Default, Reset System, and Ping functions.

7.4.5.1   Tools Information

Four functions are supported as the system maintenance tools.

Firmware Upgrade : This function will upgrade the system operation software from the web management PC.

Config Backup/Restore :
[Backup Setting]: Clicking this button, the device will backup the configuration of the device to the web management PC.
[Backup Setting to text file]: Clicking this button, the device will backup the configuration of the device to the web management PC in text format.
[Restore Setting]: The configuration of the device can be restored to device by clicking this button after the configuration file is selected.

Restore Factory Default : This function will restore the device configuration to factory default setting.

Reset System : This function will cause the device to reboot itself.

7.4.5.2 Ping
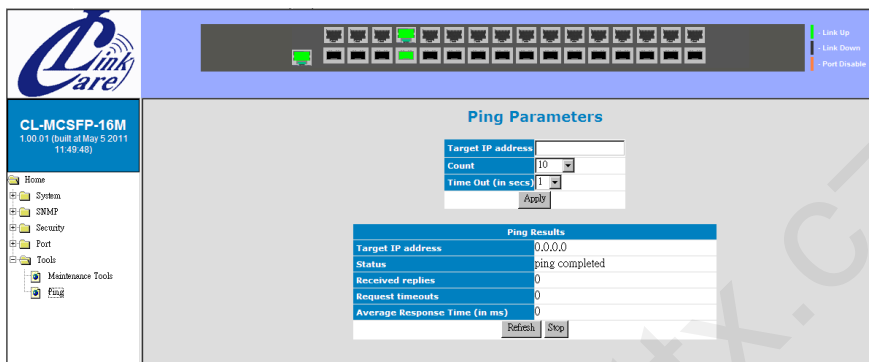
This function is used to ping network devices from the device.   It can be used to verify network connection.

Target IP address : This is the target IP address for the ping operation.
Count : This is the repeat count for the ping operation.
Time Out : This is the timeout value for the ping operation.
After the above items are set, click [Apply] to start the ping operation.

Then the result of ping operation will be shown.

8. Troubleshooting Guide

- ✓ *Power LED is OFF*
  1. Check the power connection.

- ✓ *SFP port LED is OFF*
  1. SFP module should be inserted correctly.
  2. Check the cable connection and link status at both sides of cable.   The connection of another side of cable should be ready for link up.
  3. Operation mode at both sides should be the same - 1000Mbps or 100Mbps, Single Mode or Multi Mode, and Tx/Rx is pluged correctly.
  4. TX port of the pair should be ready for link up if link pass-through function is enabled.   Link pass-through function could be disabled to verify the connection of SFP port first.   After SFP port connection is verified and TX port is link up, then enable link pass-through function.

- ✓ *TX port LED is OFF*
  1. Check the cable connection and link status at both sides of cable.   The connection of another side of cable should be ready for link up.
  2. Check the connecting Ethernet port.   Fast Ethernet port supports 100Mbps only.   If SFP port will be link up at 1000Mbps, change the connecting Ethernet port to Gigabit Ethernet port.
  3. SFP port of the pair should be ready for link up if link pass-through function is enabled.   Link pass-through function could be disabled to verify the connection of TX port first.   After TX port connection is verified and SFP port is link up, then enable link pass-through function.

- ✓ *Traffic is blocked when both SFP and TX LEDs are ON*
  1. Check the configuration/status of the connecting network devices.   The traffic could be blocked by the configuration/status of the connecting network devices, e.g. VLAN setting, port-disable because of loopback or storm-control, ...

9. Software Update and Backup

This device supports software update and configuration backup/update/restore functions.   It could be done in two ways.

1. **From console when booting**: by Xmodem protocol and doing by terminal program.   This function can be used for run-time code and boot code updating. (Boot code works only at boot time - before the main program starts.)

   Press Ctrl-C when the device is booting, the following message will be shown.

   ```
        Boot Menu
   ============================
   0: Start the Run-time code
   1: Upgrade Run-time code
   2: Upgrade Boot Code

   => Select:
   ```

   a. *Start Run-time code* : This option will continue the booting process.

   b. *Upgrade Run-time code* : This option will try to update run-time code (main code) from terminal program with Xmodem protocol. If this option is selected, the following message will be shown.
   "Waiting to receive file by Xmodem ...."
   Then user can select "Send File" function of terminal program and select Xmodem protocol and the update file, then start the file upgrade.

   c. *Upgrade Boot Code* : This option will try to update boot code from terminal program with Xmodem protocol. User can select "Send File" function of terminal program and select Xmodem protocol and the update file, then start the file upgrade.

2. **From web browser**: Doing by http protocol and by web browser. Please refer to the description of "*Tools*" function in Section 7.4.12.

3. **From console/telnet command**: Doing by tftp protocol and done by "copy" command.   Please refer to the description of "*copy*" command in Section 7.2.2.

A. Product Specifications

Access Method	Ethernet, CSMA/CD
Standards Conformance	
	IEEE802.3u(100Base Fast Ethernet),
	IEEE802.3ab(1000BaseT),
	IEEE802.3z(1000Base)
Number of Ports	16* RJ45 TX ports
	16* SFP ports
	Each TX-SFP pair works individually.
	1* 10/100Mbps RJ45 TX Management Port
Indicator Panel	each unit : Power
	each port : Link/Act/Speed(Green:1000M, Yellow:100M)
	LAN port : Link/Act/Speed(Green:100M, Yellow:10M)
Dimensions	440 x 171 x 43 mm (1U)
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Power Input	AC model: 100~240VAC, 50/60Hz
	DC model: 36~72VDC

Operation Method	Pure converter mode
Link Pass-Through	Yes
Communication Rate	100Mbps or 1000Mbps - depending on link speed on SFP port. (auto-detect)
MDI/MDIX	Auto-detect on TX ports
SFP Interface	Gigabit SerDes or 100BaseFX
Traffic Rate	Line speed

Admin Manage Security	Yes, by IP/Subnet/Protocol-interface limit
Admin Authentication	Yes, by local or Radius Server
System Time	Yes, by NTP protocol, support Daylight-Saving
System Log	Yes, Local and Remote (by syslog) logging. Up to 5 syslog servers are supported
DDMI	Yes, support SFP module DDMI information /status monitor

-----

Out-band Management	Console, Telnet, Http/Https, SNMP
SNMP	Agent Ver 1,2c, 3
	Supports MIB II(RFC1213), Private MIB
Software Update/Backup	by http/TFTP protocols, Xmodem, for firmware/configuration(binary/text)
Configuration File	Support both binary and text format

B.   Compliances

EMI Certification FCC Class A Certification (USA)

Warning: This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications.   It has been tested and found to comply with the limits for a Class A digital device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.   Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are required to correct the interference.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This is to certify that this product complies with ISO/IEC Guide 22 and EN45014.
It conforms to the following specifications:

EMC: EN55022/2006   CLASS A
            EN61000-3-2/2006
            EN61000-3-3/1995   (A1/2001 + A2/2005)
            EN55024/1998   (A1/2001 + A2/2003)
            IEC61000-4-2/2001
            IEC61000-4-3/2006
            IEC61000-4-4/2004   (Corr.1/2006 +Corr.2/2007)
            IEC61000-4-5/2005
            IEC61000-4-6/2006
            IEC61000-4-8/2001
            IEC61000-4-11/2004

This product complies with the requirements of the Low Voltage Directive 2006/95/EC and the EMC Directive 2004/108/EC.

Warning!   Do not plug a phone jack connector into the RJ-45 port.   This may damage this device.

C.   Warranty

We warrant to the original owner that the product delivered in this package will be free from defects in material and workmanship for a period of warranty time from the date of purchase from us or the authorized reseller. The warranty does not cover the product if it is damaged in the process of being installed. We recommend that you have the company from whom you purchased this product install it.