Login OLT

- About User Logins, on page 1
- How to Configure Different Methods of User Logins on an OLT, on page 2

About User Logins

You can use one of the following methods to log in to an Optical Line Terminal (OLT):

- Console port: You can log in to an OLT directly through the console port.
- Telnet: You can configure an OLT as a Telnet server. By default, the Telnet Server feature is enabled on an OLT but without an IP address, the client OLT cannot log in to the server OLT. To set up a login through Telnet, configure the IP address on the OLT through the console port. After the IP address is configured on the OLT Telnet server, you can configure other OLTs as Telnet clients.
- SSH: You can configure an OLT as an SSH server, but not an SSH client. The SSH Server feature is disabled on the OLT by default. Log in to the OLT through the console port to enable the SSH Server feature and configure the SSH settings.

  To set up SSH login on an OLT, perform the following steps:

  1. Open SSH.
  2. Configure the default key.
  3. Activate the default key.

  Note The key file and configuration are saved on the flash drive and are not decompiled.

- Network Management Software (NMS): The OLT supports login management through the NMS software.

  The SNMP server function is required for the operation of the NMS. The SNMP server function is not supported on certain OLTs. For certain OLTs, the SNMP server is enabled by default after the corresponding device is switched on; the SNMP server cannot be disabled.

  By default, the SNMP server has the following communities configured:

  - Private community with read-write authority.

• Public community with read-only authority.

How to Configure Different Methods of User Logins on an OLT

The following sections provide information on how to configure different methods of user logins on an OLT.

Setting Up Console Port Login on an OLT

To login in to an OLT through the console port, perform this procedure.

Step 1 Connect the DB-9 connector of the serial cable into the 9-pin serial port of the PC, and the RJ-45 connector into the console port of the OLT.

Step 2 Run a terminal software, such as Windows HyperTerminal.

Configure the following parameters through the terminal software:

- Configure the baud rate as 9600
- Configure the data bits as8
- Configure the parity as none
- Configure the stop bits as 1

The serial parameters are configured.

Step 3 Follow the prompts to key in the username and password to log in into the OLT. The default username is admin, and the default password is 123456. You must change the password after logging in to the device (For information on how to modify the password, see User Management Configurations).

Setting Up Telnet Login on an OLT

To set up Telnet login on an OLT, you must perform the following configurations.

Configuring an OLT as the Telnet Server

To configure an OLT as the Telnet server, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**telnet enable** **Example:** `Device(config)# telnet enable`	Enables Telnet on the OLT and configures the OLT as the Telnet server.
Step 4	**telnet disable** **Example:** `Device(config)# telnet disable`	(Optional) Disables Telnet on the OLT.
Step 5	**telnet limit** *value* **Example:** `Device(config)# telnet limit 10`	(Optional) Limits the number of users who can log in to the Telnet server. *value*: The number of users. The range is from 0 to 5.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.
Step 7	**stop telnet client** {**all** | *terminal_id*} **Example:** `Device# stop telnet client`	(Optional) Removes logged-in Telnet clients. • **all**: All the Telnet clients. • *terminal_id* : Telnet clients logged in through a particular terminal. The range is from 0 to 5.
Step 8	[**no**] **timeout** **Example:** `Device# timeout`	(Optional) Enables client timeout. Use the **no timeout** command to disable client timeout.
Step 9	**timeout** *value* **Example:** `Device# timeout 10`	(Optional) Configures the client timeout period. *value*: The period of inactivity, after which the client is logged out. The default is 20. The range is from 1 to 480.

Logging in to the Telnet Server Through an OLT

To log in to the Telnet server through an OLT, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	{**telnet**|**telnet6**} *server-ip* [*port-number* | **/localecho**] **Example:** `Device# telnet 192.0.2.1`	Logs in into the Telnet server.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	[**no**] **telnetclient timeout** **Example:** `Device(config)# telnetclient timeout`	(Optional) Enables timeout. Use the **no telnetclient timeout** command to disable timeout.
Step 5	**telnetclient timeout** [*value*] **Example:** `Device(config)# telnetclient timeout 10`	(Optional) Configures the Telnet client timeout period. *value*: The period of inactivity, after which the client is logged out. The default is 20 mins. The range is from 1 to 480.

Setting Up SSH Login on an OLT

To set up SSH login on an OLT, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **ssh** **Example:** `Device(config)# ssh`	Enables SSH. Use the **no ssh** command to disable SSH.
Step 4	[**no**] **ssh limit** *value* **Example:** `Device(config)# ssh limit 10`	(Optional) Limits the number of user logins on SSH. *value*: The user login limit value. The range is from 0 to 5.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

	Command or Action	Purpose
Step 6	**stop vty** {**all** | *vty_list*} **Example:** `Device# stop vty all`	(Optional) Removes logged-in users. • **all**: All logged-in users. • *vty_list*: Users on the VTY list only. The range is from 1 to 64.
Step 7	**crypto key generate rsa** **Example:** `Device# crypto key generate rsa`	Configures the default key.
Step 8	**crypto key zeroize rsa** **Example:** `Device# crypto key zeroize rsa`	(Optional) Removes the key file.
Step 9	**crypto key refresh** **Example:** `Device# crypto key refresh`	(Optional) Activates the key.
Step 10	Use one of the following: • **load keyfile** {**public** | **private**} **tftp** {**inet** | **inet6**} *server-ip filename* • **load keyfile** {**public** | **private**} **ftp** {**inet** | **inet6**} *server-ip filename username password* **Example:** `Device# load keyfile public ftp inet FE80::20A:5AFF:FE9B:1815%sw0`	(Optional) Downloads the key from the external key server to this machine.
Step 11	Use one of the following: • **upload keyfile** {**public** | **private** } **tftp** {**inet** | **inet6**} *server-ip filename* • **upload keyfile** {**public** | **private** } **ftp** {**inet** | **inet6**} *server-ip filename username password* **Example:** `Device# upload keyfile public ftp inet FE80::20A:5AFF:FE9B:1815%sw0`	(Optional) Uploads the local key to the key server.

Setting Up NMS login on an OLT

To set up NMS login on an OLT, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server** {**enable** | **disable**} **Example:** `Device(config)# snmp-server enable`	Enables the SNMP server. To disable the SNMP server, run the **snmp-server disable** command.

Monitoring Device Logins

Use the following commands to monitor device logins.

Table 1: Commands to Monitor Device Logins

Command	Purpose
show telnet	Displays the limit value of logged-in users.
show telnet client	Displays the login client.
show arp anti interface	Displays the state of the inteface.
show ssh	Displays SSH configuration.
show ssh limit	Displays the number of users.
show keyfile {**public** | **private**}	Displays the key file.