

Encryption Settings

Table of Contents

Chapter 1 Encryption Settings.....	1
1.1 Setting Encryption.....	1
1.1.1 Encryption Principle	1
1.1.2 Encryption Settings on OLT	1

Chapter 1 Encryption Settings

1.1 Setting Encryption

1.1.1 Encryption Principle

At the downlink direction the EPON system adopts the broadcast mode and vicious users are easy to capture the information about other users in this system. In order to improve the safety of user's data, you can adopt the encryption algorithm to encrypt the data. OLT can meet users' requirement at this respect for it supports triple churning.

OLT supports the churning for each LLID and each LLID has independent key. OLT prompts the requirements of updating keys, ONU provides a 3-byte churning key and OLT uses this key to finish the churning function. After the churning function is enabled, all the data frames and the OAM frames will be churned.

The update and synchronization of the key is based on the OAM PDU mode of Organization-Specific Extension.

1.1.2 Encryption Settings on OLT

OLT supports three encryption modes: aes-32, aes-48 and triple churning, among which the update of the keys, Tkey, can be flexibly set and its default value is 10 seconds.

Perform the following steps to conduct the encryption settings towards the downlink packets.

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon encryption triple-churning 10000	Sets the encryption mode of the downlink packets to triple churning, and the key update period to 10000ms.
Interface slot/port:llid	Enters the LLID interface configuration mode.
epon encryption enable	Enables the encryption function of the LLID port.
exit	Exits from the LLID interface configuration mode.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.