HNDE Modules of H3C Series Routers

赵刚 2007-09-27 发表

HNDE Modules of H3C Series Routers

I. Preface

Encryption card module is used for router data flow encryption, supporting:

IPSec/SSL security;

Hardware encryption/decryption and Hash algorithm;

Up to 2048 IPSec connections simultaneously;

High-speed forwarding, system ESP（3DES+HMAC-SHA1）:300Mbps

Several encryption cards, but does not support processing the same data flow on several encryption cards

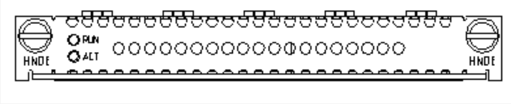
II. Introduction

HNDE is the short of High Network Data Encryption modules. HNDE supports IPsec/SSL protocol with high performance data encryption function. The hardware supports encryption/decryption and hash algorithm, providing a high performance and high reliable encryption feature for routers.

HNDE resides on the PCI slot of medium/low end modularized routers. When inserting HNDE modules, the main board of router will handle the IP packet routing forwarding and enable VPN with encryption feature, in which encryption/description is performed by encryption card.

III. Module Appearance

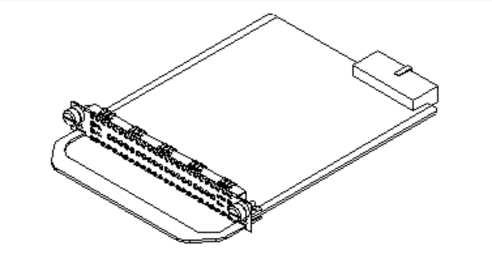
The HNDE module appearance is shown as follows:



HNDE module appearance

Module Interface Indicator

The front panel of HNDE module is shown as follows:



HNDE module panel

HNDE module indicator implication

Indicator	Implication
STATUS	Lighting frequently (Green) represents the module powers on well. Extinguished represents the module does not power on, the module power does not work or severe hardware failure.
ACTIVE	Extinguished after flashing (Yellow) 2s represents the module initiation completed. Flashing consecutively represents the module works well and some data has been received/sent with the host. Extinguished represents the module works well and no data has been received/sent with the host.

IV. Module Interface Cable

HNDE has no foreign interface and no cable.

V. Module Interface Attribute

HNDE module attribute

Attribute	Description
Supported protocols	IPSec/SSL, AH protocol ,ESP protocol, handling of AH+ESP protocols binding

Attribute	Description
Hardware enablement algorithm	Key algorithm (DES/3DES, AES, AES128) Authentication algorithm (MD5, SHA-1, HMAC-MD5, HMAC-SHA-1)

VI. Module Troubleshooting

Fault 1: STATUS indicator extinguished frequently after started.

Troubleshooting: The STATUS indicator should light frequently after started. If not, this means that the module or some hardware on the module did not work well. Please check whether the power is connected correctly. If the power worked, there may be the power chipset of the module damaged, it also may be CPLD（Complex Programmable Logic Device）does not work. Please contact Hauwei-3COM agent.

Fault 2: ACTIVE indicator extinguished frequently during start.

Troubleshooting: During start, the ACTIVE indicator should flashing 2s and then extinguished. This indicated that the encryption processor of the module is configured for operation. If the ACTIVE indicator extinguished frequently during start, that is the initiation configuration of module processor failed, this means that system bus may not work. Please check whether the module is connected to the host perfectly. If so, there may be the host or the module failed. Please contact Huawei-3COM agent.

Fault 3: ACTIVE indicator lights or extinguished frequently in running module.

Troubleshooting: The ACTIVE indicator should flash when the module runs encryption operation. Light or extinguished means system bus may not work. Please check whether the module is connected to the host perfectly. If so, there may be the host or the module failed. Please contact Huawei-3COM agent.