SafeNet Ethernet Encryptor

Version 4.0.0

User’s Guide

Software Version 4.0.0 (Sep 2010)

Documentation Part Number 007-011114-001 Revision C_2

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland 21017
USA

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information

Phone: 800-545-6608
Email: support@safenet-inc.com

www.safenet-inc.com

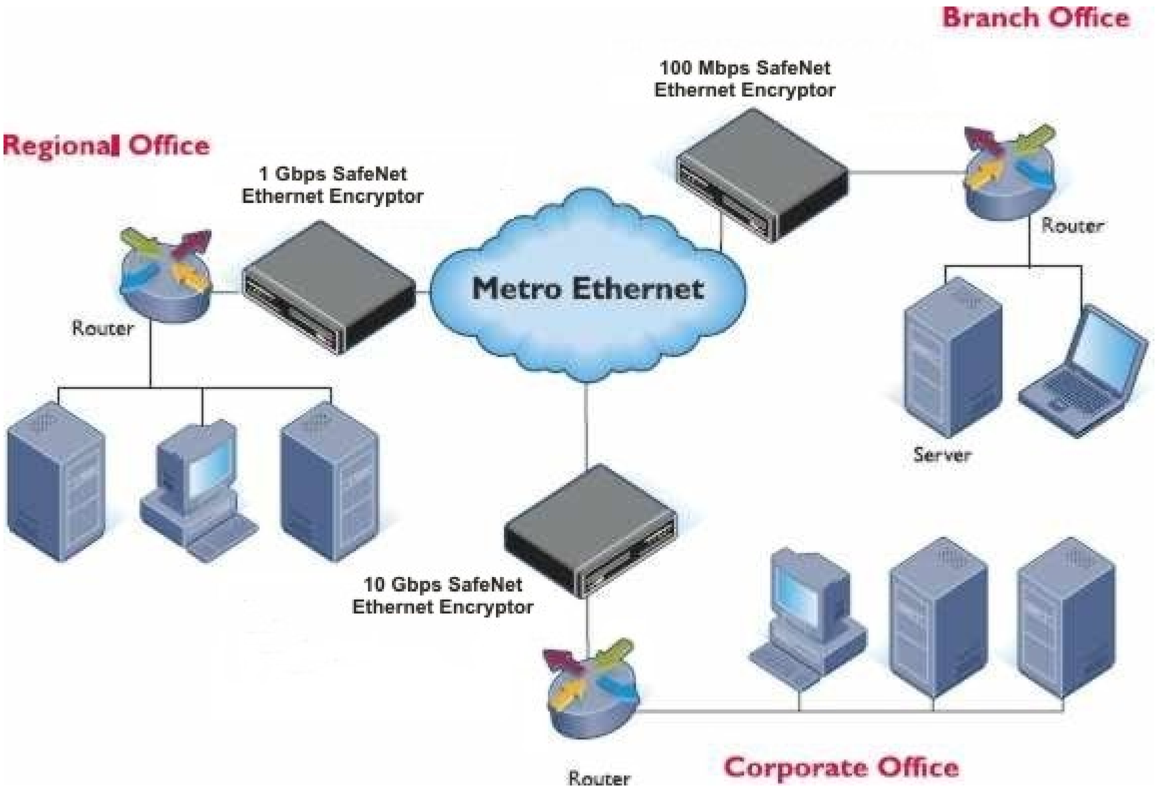
Table of Contents

Welcome

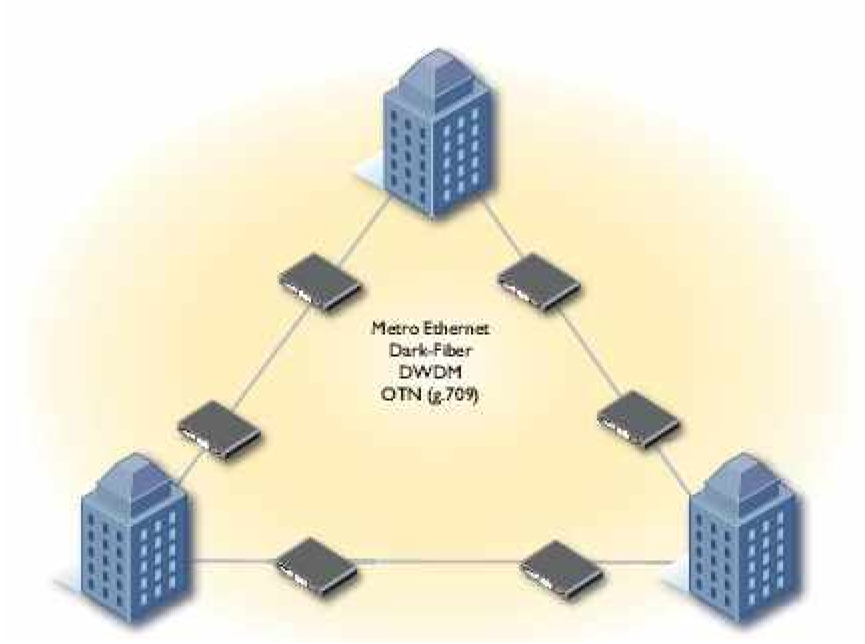
Welcome to the *SafeNet Ethernet Encryptor User's Guide*.

The SafeNet Ethernet Encryptor (SEE) is a Layer 2 security device designed to protect high-speed Ethernet networks at speeds up to 1Gbps and at 10 Gbps. With seamless end-to-end integration, the SEE delivers instant protection across the network.

The SEE is managed by SafeNet's Security Management Center II (SMCII), a robust web-based management application with secure, flexible, and transparent SNMP-based control and monitoring capabilities. The SMCII provides the ability to define integrated security policies that can be centrally and remotely distributed across multiple devices.


Branch Office
100 Mbps SafeNet Ethernet Encryptor
Regional Office
1 Gbps SafeNet Ethernet Encryptor
Router
Metro Ethernet
Router
Server
10 Gbps SafeNet Ethernet Encryptor
Router
Corporate Office

Mesh Network Configuration Diagram



10 GbE Line Mode Configuration Diagram

Product Overview

Features

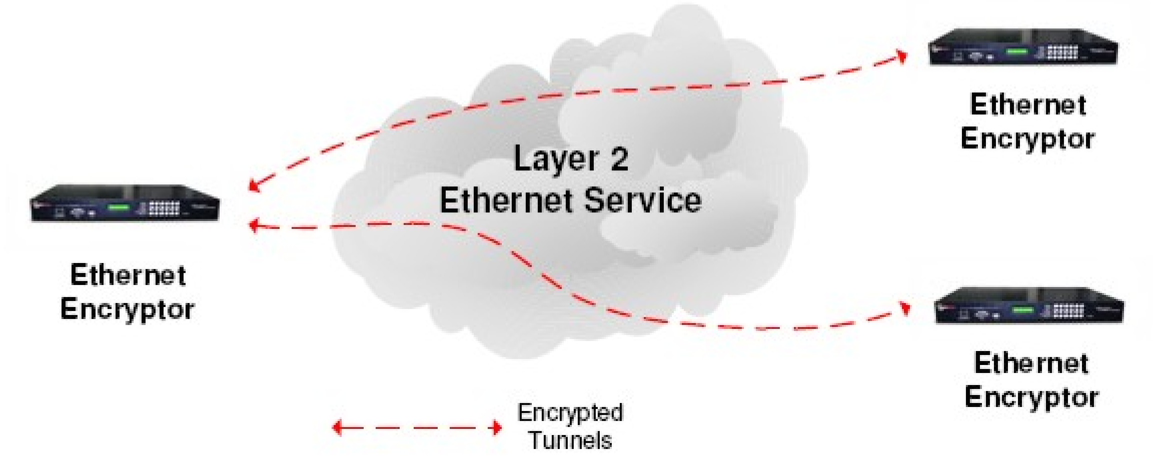
- Full-duplex line rate AES encryption for FastEthernet (100 Mbps), GbE (1 Gbps), and 10 GbE (10 Gbps) networks
- Standards-based authentication, digital certificates, and key management
- Bump-in-the-wire design for easy installation into existing network environments
- Designed to international Common Criteria and U.S. Government FIPS security standards
- Central remote configuration, monitoring, and management through SafeNet Security Management Center II (SMCII)

SafeNet Ethernet Encryptor - 100 and 1000 Mbps (Model 600)

SafeNet Ethernet Encryptor - 10 Gbps (Model 650)

Operations

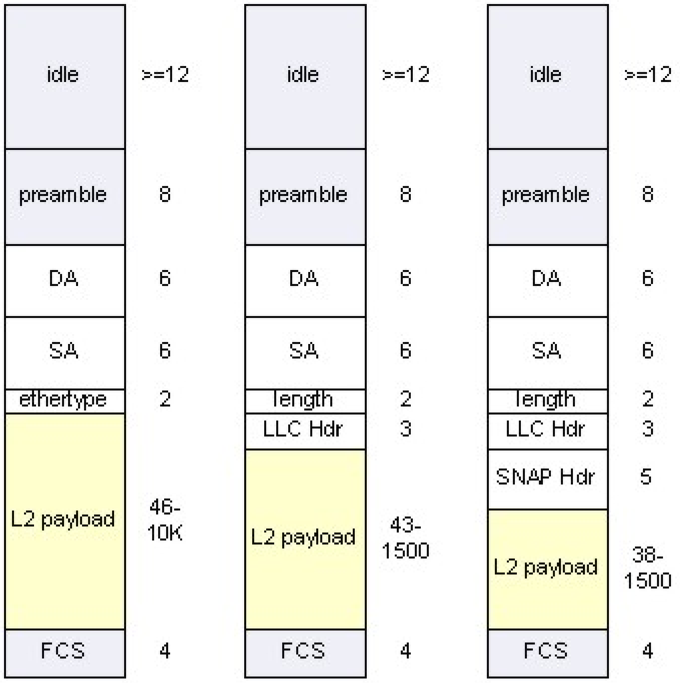
The SEE connects between a local (protected) network and a remote (protected) network across a public (unprotected) network. As shown in the following figure, an encryptor is paired with one or more remote encryptors to provide secure data transfer over encrypted connections.



The SEE supports LAN, VLAN, Ethernet over SONET, L2 MPLS networks, and any transmission of layer 2 non-routed Ethernet traffic. Any modification, discard, reordering of frames, or routing based on encrypted data within the network is not supported in the layer 2 encryption model when in line mode or multipoint MAC mode. The exception is multipoint VLAN mode where packet reordering is permissible.

The SEE encrypts the payload data of the frame with no frame expansion in AES CFB mode. In AES CTR mode, SHIM headers are added. See SHIM Command for further details.

The encryption method used is AES with a 256-bit key utilizing a self synchronizing Cipher Feedback Block (CFB) mode or Counter (CTR) mode. The only exception is the 10 GbE device in multipoint mode which uses Counter mode and does not support CFB mode.



idle	>=12
preamble	8
DA	6
SA	6
ethertype	2
L2 payload	46-10K
FCS	4

idle	>=12
preamble	8
DA	6
SA	6
length	2
LLC Hdr	3
L2 payload	43-1500
FCS	4

idle	>=12
preamble	8
DA	6
SA	6
length	2
LLC Hdr	3
SNAP Hdr	5
L2 payload	38-1500
FCS	4

Each connection between encryptors has its own key pair. Key updates occur seamlessly without interrupting user data. Connections between encryptor peers are based off the frames 'remote MAC address'. A 'remote MAC address' is defined as follows:

- if the frame is received on the local port, the destination MAC address is labeled as remote MAC address.
- if the frame is received on the network port, the source MAC address is labeled as the remote MAC address.

Therefore, it is a requirement that the network between encryptors does not modify the Ethernet addresses.

Frames

Encrypted Frames

An encrypted frame is encrypted according to the AES algorithm using a 256-bit key. The Ethernet frame payload is encrypted. If padding is present on the received frame, a value of zero is used to pad the transmitted frame, i.e., padding is not encrypted.

Bypassed Frames

A bypassed frame is transmitted without alteration, except for Frame Check Sequence (FCS) and padding regeneration.

Discarded Frames

A discarded frame is dropped (blocked) by the encryptor.

Rx Invalid FCS Frames

Frames received with an invalid FCS are transmitted with an invalid FCS.

Padded Frames

Padding is inserted to ensure the minimum frame size of 64 bytes. It is only present on 802.3 LLC SNAP and 802.3 SAP frame types when the length field indicates that the payload data is less than 46 bytes in length.

Address Resolution Protocol

Address Resolution Protocol (ARP) is used to map an IPv4 address with a MAC address. The Address Resolution Protocol is defined in RFC 826.

> *ARP is only relevant for IPv4. IPv6 nodes on the same link use the Neighbor Discovery Protocol (NDP) to discover each other's presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors.*

Ethernet Addressing

Ethernet is a transport protocol defined at the layer 2 of the Open Systems Interconnection (OSI) model. It has progressed from a low bandwidth LAN technology to a High bandwidth MAN and WAN technology. Ethernet uses a frame-based communications method.

An Ethernet (or MAC) address is 6 bytes long and has 2 portions of significance:

- Organizationally Unique Identifier (OUI) (first 3 bytes)
- Organization Assigned Portion (last 3 bytes)

There are 3 types of addresses:

- Unicast - addresses a single network device
- Multicast - addresses a logical group of network devices
- Broadcast - addresses all devices on a particular LAN segment

A multicast addressed Ethernet frame is defined by the least significant bit of the most significant byte of the destination address.

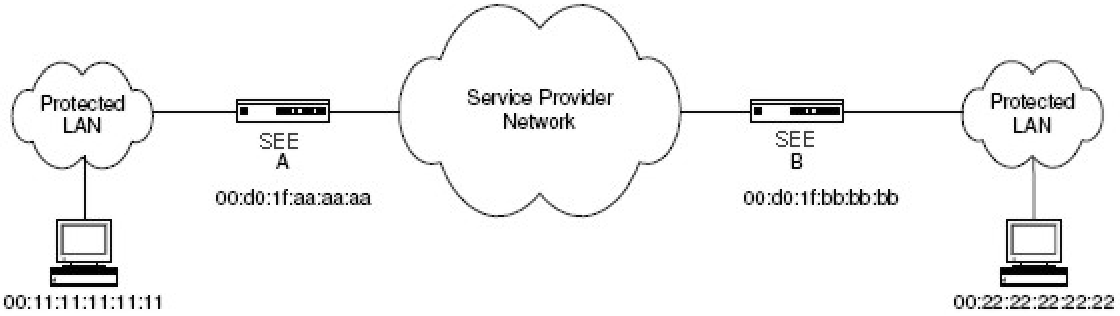
A broadcast addressed Ethernet frame is defined by a destination address of all 1's (FF:FF:FF:FF:FF:FF).

Modes

The SEEs operate in line mode or multipoint mode. When in multipoint mode, the SEE can be in either MAC mode or VLAN mode.

Line Mode

Line mode is designed for point-to-point connections with little or no ethertypes injected on the network side. Point-to-point line mode deployments can encrypt multicast and broadcast addressed frames in some configurations. Line mode is not applicable for meshed networks. The network topology is shown in the following figure.

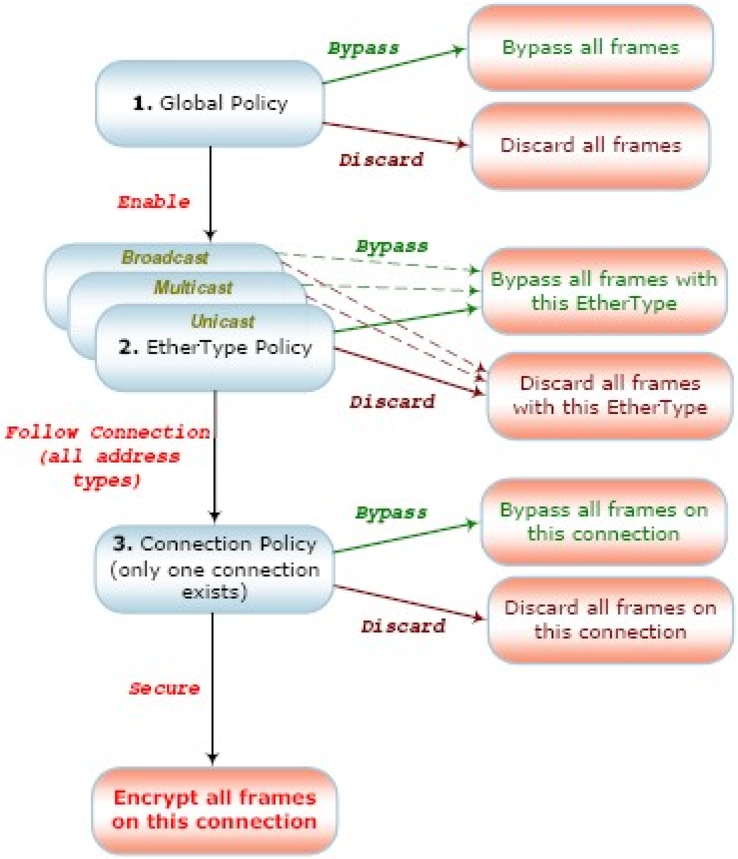


MAC address configuration is not available when the device is operating in line mode.

Enabling or disabling line mode causes an intentional reboot and re-initialization of the device as follows:

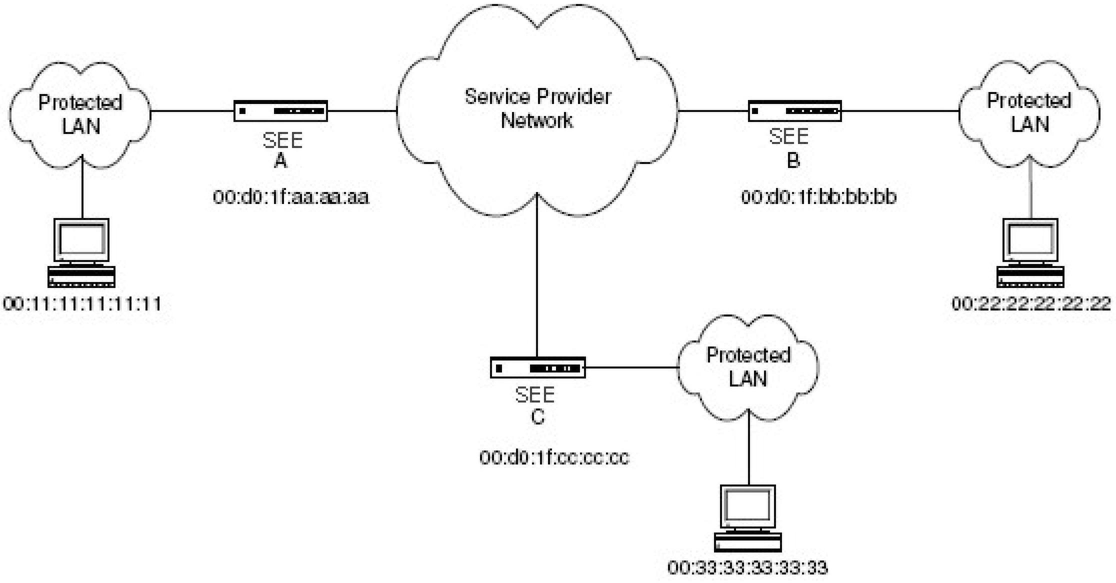
- Local and Network Ethernet MAC Address tables are cleared.
- The Connection Identifier (CI) table is re-initialized.
- The Ethertypes table is re-initialized.

Line mode is supported beginning with version 3.2.1. The basic frame processing policy for an encryptor in line mode is shown below.


1. Global Policy
Bypass
Bypass all frames
Discard
Discard all frames
Enable
Broadcast
Multicast
Unicast
2. EtherType Policy
Bypass
Bypass all frames with this EtherType
Discard
Discard all frames with this EtherType
Follow Connection (all address types)
3. Connection Policy (only one connection exists)
Bypass
Bypass all frames on this connection
Discard
Discard all frames on this connection
Secure
Encrypt all frames on this connection

Multipoint Mode

Multipoint mode is designed for point to multipoint connections. The network topology is shown in the following figure.



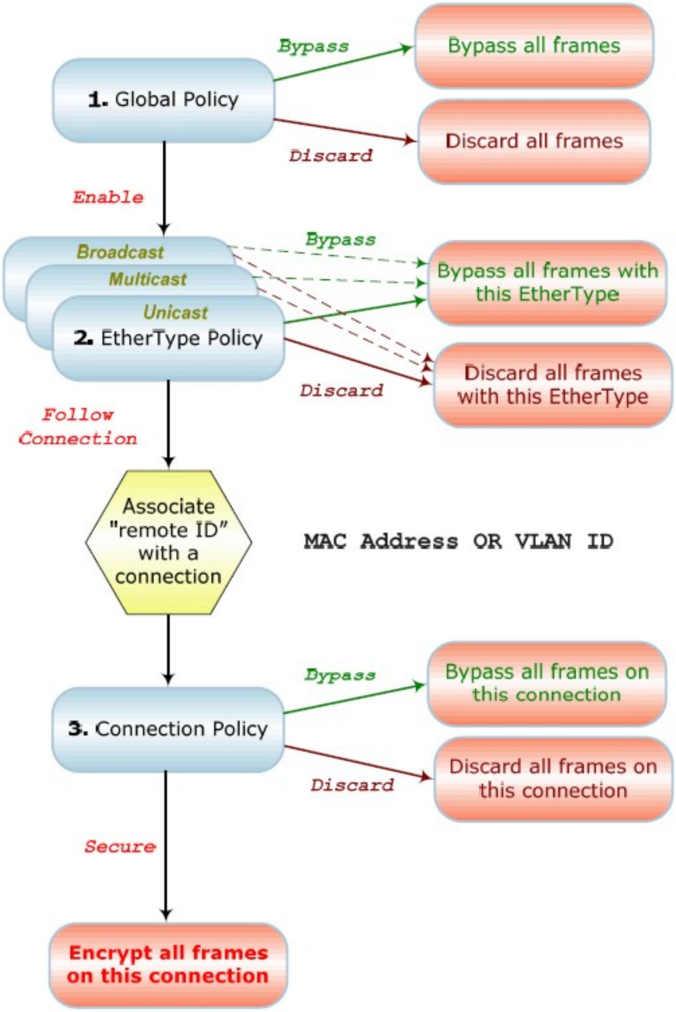
One of the principal differences in multipoint mode when compared to line mode is that security policy is extended to allow it to be based on the remote MAC addresses or VLAN ID of transmitted frames. For discussion we will refer to this as the 'Remote ID'.

To implement policy, the encryptor associates the Remote ID of each received frame with a configured connection policy. This association can occur in one of two ways:

- Automatic discovery of MAC addresses or VLAN IDs
- Manual entry of MAC addresses or VLAN IDs

The auto-discovery configuration option instructs the encryptor to learn Remote IDs from the network traffic and automatically establish secure connections with peer encryptors. Where policy is based on the MAC address, separate auto-discovery mechanisms are provided for unicast and multicast traffic. Where the policy is based on VLAN ID, a single group auto-discovery mechanism is provided.

The basic frame processing policy for an encryptor in multipoint mode is shown below.


1. Global Policy
Bypass
Bypass all frames
Discard
Discard all frames
Enable
Broadcast
Multicast
Unicast
2. EtherType Policy
Bypass
Bypass all frames with this EtherType
Discard
Discard all frames with this EtherType
Follow Connection
Associate "remote ID" with a connection
MAC Address OR VLAN ID
3. Connection Policy
Bypass
Bypass all frames on this connection
Discard
Discard all frames on this connection
Secure
Encrypt all frames on this connection

Differences Between Line Mode and Multipoint MAC Mode

In line mode:

- MAC addresses are not observed or learned.
- The local and network MAC address tables are not applicable.
- The automatic connection discovery feature is not applicable.
- Only one tunnel is established.
- The tunnels add/delete feature is not applicable.

Differences Between Line Mode and Multipoint VLAN Mode

In line mode:

- The automatic connection discovery feature is not applicable.
- Only one tunnel is established.
- The tunnels add/delete feature is not applicable.

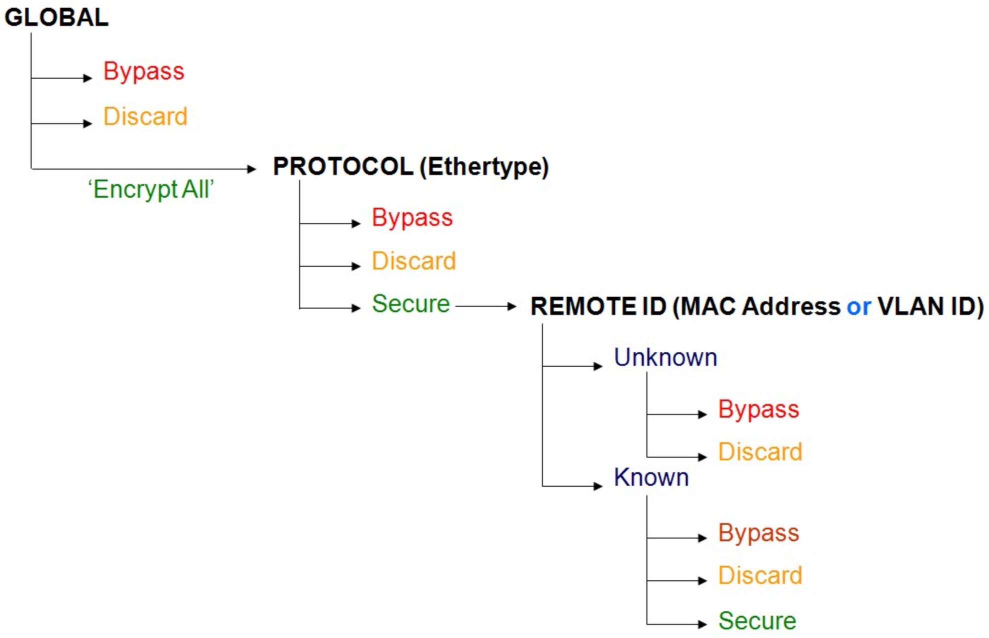
Differences Between Multipoint MAC Mode and Multipoint VLAN Mode

In multipoint VLAN mode:

- MAC addresses are not observed or learned.
- The local and network MAC address tables are not applicable.

Frame Processing Policies

Policy is performed in a hierarchical process as shown in the following diagram.



Global Policy

First, the GLOBAL policy setting is checked. The Global policy is set to either bypass, discard, or encrypt all (enable). Setting the global policy to bypass or discard provides a quick way of bypassing or discarding all traffic passing through the encryptor regardless of VLAN ID, MAC address, or ethertype. If the Global policy is set to encrypt all, then the following transitions occur:

1. Tunnel or group connection discovery begins if auto-discovery is enabled.
2. MAC address learning begins if auto-discovery is enabled in MAC mode, or VLAN ID learning begins if auto-discovery is enabled in VLAN mode.
3. The Protocol level is followed using the Ethertype table.

Ethertype Policy

The second policy level is the PROTOCOL level, which is the ethertype policy of the encryptor. The Ethertype table gives control over frame processing by ethertype and allows policy actions to be specified for up to 15 ethertypes. The set of policies are defined for each destination ethertype based on MAC address (unicast, multicast, or broadcast) and is set to either bypass, discard, or follow CI. A group of default entries are provided and are listed here:

- Length encoded (0x05ff)
- IPv4 (0x0800)
- ARP (0x0806)
- IPv6 (0x86dd)
- MAC Control Frames (0x8808)
- Link Aggregation (0x8809)
- Link Layer Discovery Protocol Frames (0x88CC)
- Loopback (0x9000)
- Other

Setting the ethertype policy to bypass or discard instructs the encryptor to bypass or discard all traffic passing through the encryptor regardless of VLAN ID or MAC address.

An optional encryption offset should also be applied to frames. The offset delays the encryption start point in the frame by the specified number of bytes and allows a portion of the frame to be sent in the clear.

The encryption offset may be necessary if intermediate equipment between a pair of encryptors needs visibility of the frame payload after the Ethernet header. For example, a layer 2 service that requires a valid IP header to be present. This type of behavior should never be observed on a true layer 2 network. However, the encryption offset provides a flexible solution for unexpected network problems.

If the ethertype policy for the frame is follow CI, the the Connection Identifier table is followed based on remote ID (MAC Address or VLAN ID).

MAC Address or VLAN ID Policy

The final policy level is the REMOTE ID (MAC Address or VLAN ID) level found in the Connection Identifier table. The Connection Identifier table contains the following entries:

- a single system pending connection
- a single bypass connection
- a single discard connection
- zero or more unicast connections to remote encryptors
- zero or more multicast or VLAN group connections

The first three entries are default. All others are created through automatic discovery or added manually.

If the remote ID (MAC Address or VLAN ID) is known, then the connection to which the frame belongs is known. The connection policy can be set to either bypass, discard, or secure. If the policy is set to secure, then the frame is encrypted according to the cryptographic mode of the device. If a unicast frame is received with an unknown remote MAC address and auto discovery is enabled, the MAC address is initially associated with the system pending connection.

Ethernet Session Establishment for Unicast Frames

In MAC Mode, the SEE maintains internal tables of local and network MAC addresses for frames that pass through it. Addresses listed in the local MAC table are those of devices protected behind the encryptor's local port. Addresses in the network MAC table are those of devices that exist somewhere on the network side of the encryptor. Each address in the network MAC table is associated with a Connection Identifier (CI) table entry.

The tables can be automatically populated by the encryptor as frames are received if the automatic discovery option is enabled. When enabled, the encryptor parses all frames received on both local and network interfaces and adds the frame's MAC addresses to the internal MAC tables.

When a newly discovered remote MAC address is assigned to the system pending CI table entry, the local encryptor will try to establish whether there is a remote peer encryptor protecting the new address. If a remote peer is found and an existing connection exists between the two encryptors, the new MAC address will be assigned to this connection. If there is not an existing connection, the local encryptor will then attempt to establish a secure connection with the remote peer. Once this has been established, a new CI entry will be created with the Origin field set to automatic. The remote MAC address will then be assigned to the new connection. If a peer encryptor cannot be found the remote MAC address will be left in the system pending entry and the process will be repeated.

The local encryptor will use management frames when trying to locate a peer encryptor for MAC addresses in CI 1. These management frames are transmitted using the Ethernet II format with a proprietary ethertype of 0xFC0F.

The local encryptor will send out management frames every 5 seconds to all MAC addresses associated with system pending entry CI 1. If a remote peer encryptor cannot be found for the MAC addresses, this process will continue forever and may not be desired. There may be MAC addresses of devices associated with CI 1 that are not intended to be placed in the protected network. When this is the case, these MAC addresses can be manually moved to either the discard entry CI 2 or the bypass entry CI 3 by using the **netmacs** command. This will prevent management frames from being sent out every 5 seconds.

There is only one tunnel ever established between a given pair of SEEs. All unicast frames passing through the encryptor are processed according to the specified action for that tunnel.

Ethernet Session Establishment for Group Connections

Multicast encryption and VLAN based encryption within a multipoint network requires a group key management infrastructure to ensure that each encryptor can share individual encryption keys per multicast MAC address.

The group key management scheme is responsible for ensuring group keys are maintained across the visible network, and survive network outages and topology changes automatically. The group key management scheme automatically elects a group key master amongst the visible encryptors within a mesh, and re-election of the group key master is automatically negotiated upon network topology changes.

In the event of a temporary isolation of network segments, the group key management scheme will maintain/establish new group key managers per group of visible peers. Subsequent rejoining of these network segments will instigate a transparent re-electing of a single group key manager.

Inband Management

SMCII servers can be used to monitor and manage the SEE appliances and the secure Ethernet network. The SEEs can be managed locally or remotely over an IP network using out-of-band communication. Out-of-band communication uses the Ethernet port on the front panel.

Remote encryptors can also be managed via inband management as long as there is a layer 2 network between the local and remote encryptors. Inband management uses internal mechanisms to send management IP packets over the network port to remote encryptors.

To provide the IP connectivity over the network, one encryptor must be configured as an inband management gateway. The gateway encryptor receives inband management traffic from the front panel Ethernet port and forwards it over the network to the remote encryptors being managed. This inband traffic is encapsulated in a proprietary ethertype (FC0F), which allows the traffic to be inline with the user data while consuming only a minimal amount of bandwidth.

Up to 16 remote encryptors can be reached through a gateway. Multiple gateways can be used for larger networks.

Inband management IP addresses of remote encryptors must be on the same IP network. A static route must be added on the SMCII workstation to route inband IP packets to the Ethernet port on the local encryptor acting as a gateway. See IP Command or the *Security Management Center II User's Guide* for information on inband parameters that can be configured.

Inband Management Settings

Inband management is disabled by default. The inband management IP address and IP network mask can also be set.

All encryptors on a managed network must use the same IP subnet for inband interfaces (distinct from the out-of-band management IP subnet).

See IP Command for examples on configuring inband management.

Gateway Encryptor Settings

The gateway encryptor is managed directly via the front panel Ethernet port. It requires the following settings:

- The Management IP Address must be set to a valid IP address reachable from the SMCII.
- The Inband Mgmt IP Address must be set to an address on the same inband network as the remote SEE.
- For the encryptor acting as the gateway, the 'Inband Management Gateway Enabled' should be set to 'Yes.'
- The IP Gateway is set to the gateway for the management IP address.

Remote Encryptor Settings

The remote encryptor(s) is logically connected to the gateway encryptor through the data network. It requires the following settings:

- For the remotely managed encryptor, the 'Inband Management Gateway Enabled' should remain the default of 'No.'
- The Inband Mgmt IP Address must be set to an address on the same inband network as the gateway SEE.
- The IP Gateway is set to the Inband IP Address of the SEE acting as the gateway.

Router Settings

A route must be added to the router or the SMCII manager (if the SMCII manager is on the same subnet as the gateway SEE) that directs traffic to the inband network through the gateway SEE's IP address.

Using Windows, an example is:

```
route add network 192.168.0.0 mask 255.255.255.0 10.0.100.179
```

Using Solaris, an example is:

```
route add -net 192.168.0.0 netmask 255.255.255.0 gw 10.0.100.179
```

This will allow the SMCII to be able to reach the inband address of 192.168.0.xxx (on the remote SEE) by going through the gateway SEE which is 10.0.100.179.

Certificates and Certifying Authority

In order for two encryptors to exchange master and session keys and secure a virtual connection it is necessary for a level of trust to exist between them. Trust is achieved by means of certificates.

Certificates are a form of electronic passport that contain an identifying name, unique serial number, expiration date, and public key. Certificates are issued and tied to each encryptor by a trusted authority called a Certifying Authority (CA).

SEEs use RSA public key encryption during secure connection establishment. Each SEE is responsible for generating its own key pair consisting of a public and private key. The private key is held internally in the unit and is automatically erased when the interface card is removed allowing the cover to be taken off.

When two encryptors establish a secure session they exchange certificates. Both encryptors must confirm that the other's certificate was issued by the same trusted CA (confirmation is achieved by public key encryption methods) and if so the secure connection establishment may proceed. A certifying authority is provided by SafeNet as part of Security Management Center II and can be used to issue certificates to all the encryptors in the network.

Although there may be multiple SMCII servers being used on a given network, it is essential that the same SMCII server be used as the Certifying Authority. This is because all encryptors that need to establish secure logical connections must have certificates issued from the same trusted CA.

SEEs support both 1024 bit (V1) and 2048 bit (V2) certificates. V1 certificates are supported for interoperability with devices running software versions prior to 3.3.0. The V1 certificates employ 1024 bit encryptor RSA keys and are signed with 1024 bit CA RSA keys. V2 certificates provide stronger security when interoperating with devices running software versions 3.3.0 and higher. Following current best practices, V2 certificates employ 2048 bit encryptor RSA keys and are signed with 4096 bit CA RSA keys. Upgrades from software versions prior to 3.3.0 maintain the existing V1 certificate.

Upgrades from 3.3.0 or later maintain the existing V2 certificate. When establishing secure connections, the unit automatically determines which certificate to use on each connection based on the available certificate(s) on the far end device. When two systems have both V1 and V2 certificates, the V2 certificates are used in preference to the v1 certificates.

Secure negotiation for GbE devices fail if the certificate has a subject name (DN) longer than 32 characters. Limit the subject name to 32 characters or less.

MAC Migration

MAC address migration is a feature supported by the SafeNet Ethernet Encryptors when in multipoint MAC mode and secure sessions have been established.

When an auto-discovered device listed in the local MAC address table is moved to a peer encryptor network, the device's MAC address is cleared from the local MAC address table and moved to the network MAC address table. The table updates take approximately two minutes or less to complete. Audit log entries are recorded for MAC address table additions and deletions.

Miscellaneous Policy Settings

The encryptor has several miscellaneous policy settings, which include:

- bypass reserved multicast addresses
- enable Spanning Tree Protocol (STP) monitoring (multipoint MAC mode only)
- enable Tunnel Keep Alive Monitoring (TKAM) (multipoint MAC mode only)
- observe pending action for unknown DA on ingress

For information regarding the configuration of these features, see Policy Command.

Bypass Reserved Multicast Addresses

Some multicast addresses are reserved and may need to be bypassed by the encryptor to allow certain network protocols to function correctly. The following group of addresses is bypassed if the reserved multicast address bypass feature is enabled.

Multicast Address Type	**Address**
Link constrained protocol	01:80:c2:00:00:0*
STP	01:80:c2:00:00:00
MAC Pause Frame	01:80:C2:00:00:01
Slow Protocols	01:80:C2:00:00:02
Port Access protocol	01:80:C2:00:00:03
LLDP	01:80:C2:00:00:0e
Routing protocols	01:00:5e:00:00:**
Cisco VTP/DTP/CDP	01:00:0c:cc:cc:cc
Cisco L2TP	01:00:0c:cd:cd:d0
Cisco CGMP	01:00:0c:dd:dd:dd
Cisco SSTP	01:00:0c:cc:cc:cd

Enable STP Monitoring

The SEE STP monitoring feature allows the encryptor to observe Spanning Tree Protocol operations on networks to provide failover for redundant links in the event of an active link failure. Layer 2 switch devices use STP to provide path redundancy while preventing undesirable loops in the network. This is done via STP by providing a tree that spans all switches in a meshed network and forces certain redundant paths into a blocked state. If one network segment becomes unreachable the algorithm reconfigures the topology and activates the standby path.

To maintain an STP topology, all switches advertise their knowledge via configuration messages. When a topology change occurs, a topology change message is sent on the affected links which informs the switches of the change and a new path is selected. STP monitoring by the encryptor makes use of this information to enable failover between encryptors.

The SEE can be connected to any switch or port within an STP topology. There are no limitations on the type of the spanning tree port type connected to the encryptor. That is, it can be connected to a root, designated, alternate or backup port.

When STP monitoring is enabled, the encryptor will detect STP configuration and topology change messages and purge the local MAC address table. This means that when the Spanning Tree Topology reconverges and starts forwarding data, new MAC addresses will be identified on the local port of the encryptor. The auto-discovery feature will cause the encryptor to notify all other encryptors that it is protecting these MAC addresses, which completes the failover process.

- STP monitoring requires auto-discovery to be enabled so new MAC addresses can be learned.

- STP monitoring only applies when the switch devices connected to the SEE device local and network ports are configured for per VLAN spanning tree (PVST).

The SEE detects a topology change on the following conditions:

- Bridge Protocol Data Unit (BPDU) topology change message
- BPDU configuration message with topology change flag set
- BPDU configuration message with topology change acknowledge flag set
- BPDU configuration message absence at least 3 hello time periods followed by BPDU configuration message reception

STP Monitoring does not have any adverse effects on the SEE throughput or latency. STP monitoring only operates in multipoint MAC mode as there is no dependency on MAC addresses in line mode.

Local MAC Address Table Purging

Typical operation of the SEE is to preserve MAC addresses. When STP monitoring is enabled and an STP topology change is identified the local MAC address table is purged. The table is purged repeatedly for a finite period to account for the delay required for the STP topology to reconverge to a forwarding state.

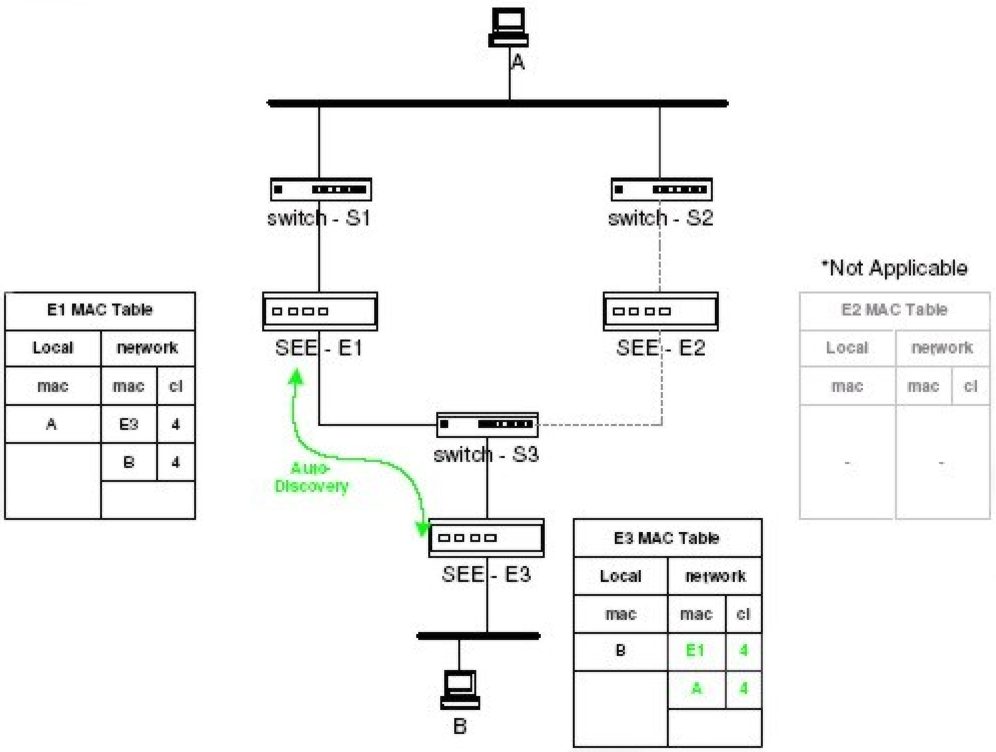
The SEE purges the local MAC address table four times, every forward delay. The forward delay is measured by counting STP configuration messages.

Purge Frequency = 4 x (Forward Delay)/(Hello Time) Configuration Messages

As a result of purging, there may be some minimal frame loss just after a topology reconvergence.

STP Monitoring Example

In this example, the SEE-E1 is on the active path within the spanning tree. SEE-E2 is on a blocked/alternate segment and is not visible to the other encryptors. SEE-E1 and SEE-E3 identify each other and establish a connection via auto-discovery.



E1 MAC Table

Local	network	
mac	mac	cl
A	E3	4
	B	4

*Not Applicable

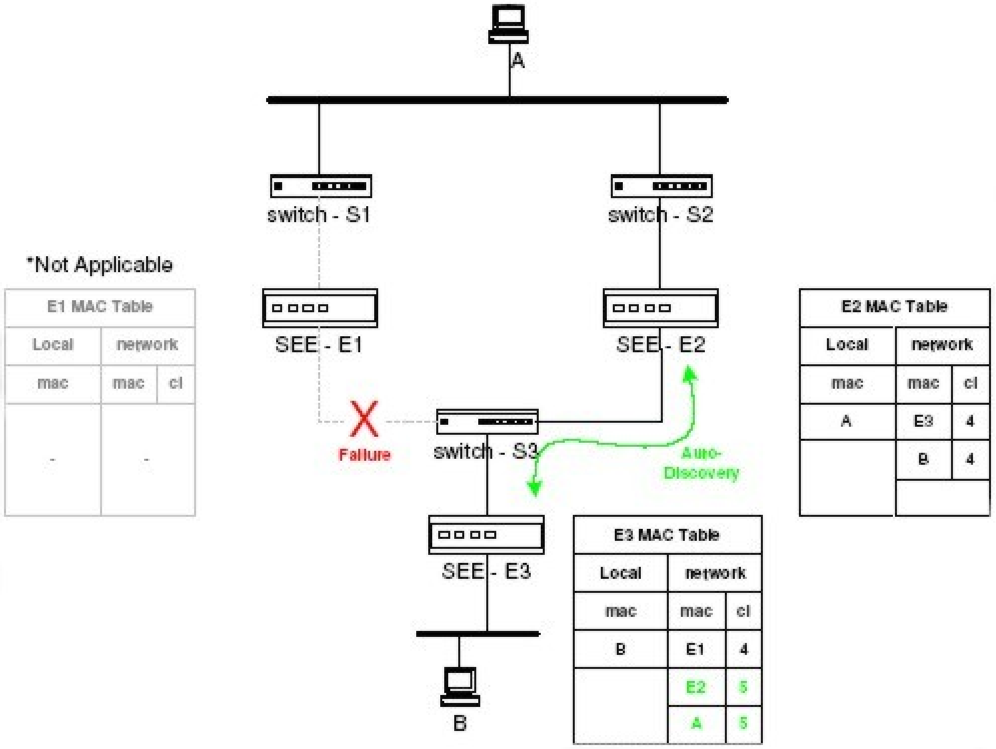
E2 MAC Table

Local	network	
mac	mac	cl
-	-	

E3 MAC Table

Local	network	
mac	mac	cl
B	E1	4
	A	4

If a failure occurs on the active path, the spanning tree detects the failure and performs a topology change to use the inactive/alternate path. SEE-E2 and SEE-E3 identify each other and establish a connection via auto-discovery if they have not previously communicated. Note that SEE-E3 is notified of the change and the remote MAC address A is moved from connection 4 to connection 5.

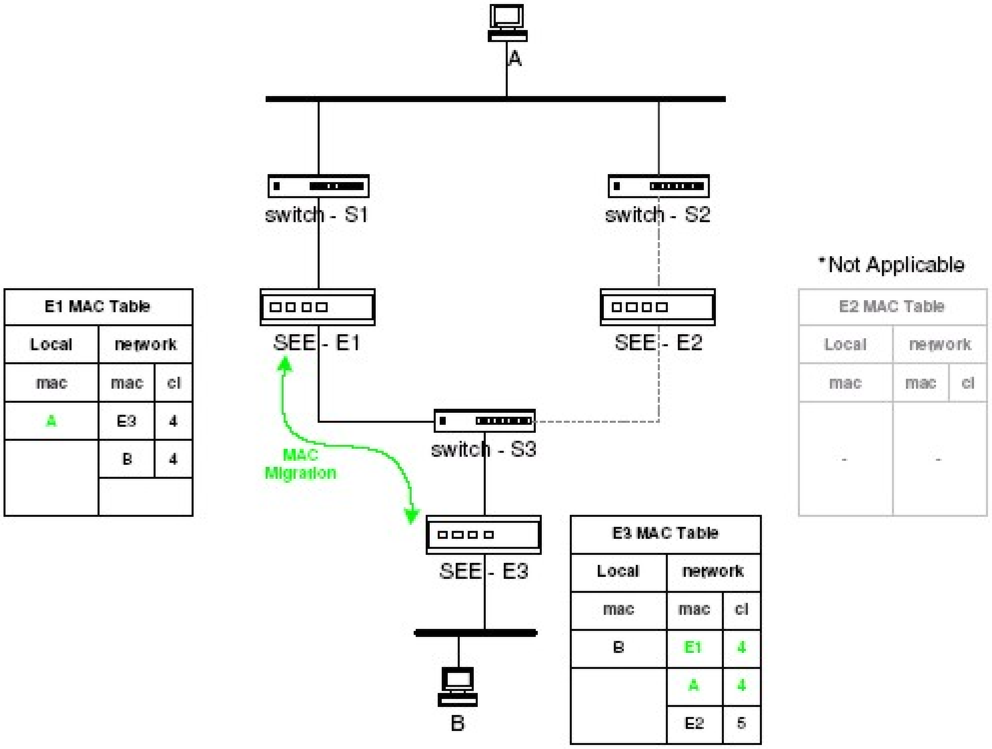


E1 MAC Table		
Local	network	
mac	mac	cl
-	-	

E2 MAC Table		
Local	network	
mac	mac	cl
A	E3	4
	B	4

E3 MAC Table		
Local	network	
mac	mac	cl
B	E1	4
	E2	5
	A	5

Once the failure is removed the root path is restored. The spanning tree generates a topology change and the local MAC address table in SEE-E1 is purged. As traffic is forwarded, the MAC discovery mechanism SEE-E1 learns MAC address A and notifies SEE-E3. SEE-E3 adjusts its network MAC table accordingly to map MAC address A back to connection 4.



E1 MAC Table		
Local	network	
mac	mac	cl
A	E3	4
	B	4

E2 MAC Table		
Local	network	
mac	mac	cl
-	-	

E3 MAC Table		
Local	network	
mac	mac	cl
B	E1	4
	A	4
	E2	5

To configure the device for STP monitoring, see Configuring STP Monitoring.

Enable Tunnel Keep Alive Monitoring

TKAM is a protocol independent mechanism for detecting network failover. When TKAM is enabled the encryptors periodically send (and receive) keep alive messages to the peer encryptor on each encrypted tunnel.

If keep alive messages fail to be received on a tunnel for any thirty second period (for example, due to failover to a redundant path) then the encryptor will automatically purge its network MAC table and allow new MAC addresses to be learned.

TKAM only operates in multipoint MAC mode and requires auto-discovery to be enabled.

Observe Pending Action for Unknown DA on Ingress

When a frame is received on the network port of the encryptor, the destination MAC address is compared with the known addresses in the discovered local MAC address table.

If the destination address is not known then the frame is discarded by default. The 'Observe pending action for unknown DA on ingress' option specifies that frames with unknown destination addresses should observe the pending action instead of being automatically discarded.

Link Control

Electrical Link Loss Forwarding

Unidirectional electrical LLF (eLLF) in both line mode and multipoint mode is possible under specific operations.

The concept behind electrical Link Loss Forwarding is to propagate changes in link status of the network port (and optionally tunnel status) by administratively controlling the local port link status. If the local port is 'administratively down' due to eLLF, the LOCAL LED will be solid RED.

If a mix of SFPs is used (for example, optical SFP on network port and copper SFP (or RJ45 connector used in the case of a 2086/7) on local port), eLLF shall not be performed, even if the electrical Link Loss Forwarding feature is enabled. If the local port is 'administratively down' due to eLLF at the time the mix of SFPs is used, the local port will be re-enabled and alarms cleared.

Laser levels on both ports can be checked using the **sfp** command. This event can be verified by both audit and alarm log messages. Electrical LLF can be configured to propagate network to local loss with the **linkspeed** command.

Line Mode

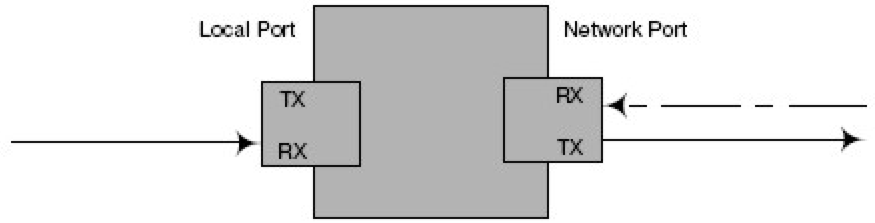
With eLLF enabled while in line mode, any loss of link on the network port will force the local port to be 'administratively down'. Additionally, the local port can be made to also follow the encrypted tunnel (CI) status. For line mode, the tunnel is fixed to tunnel (CI) 1.

If the device’s mode is changed from line mode to multipoint mode, eLLF tied to connection shall automatically be disabled. A message will be added in the audit log when this occurs.

Multipoint Mode

With eLLF enabled while in multipoint mode, any loss of link on the network port will force the local port to be 'administratively down'. Additionally, the local port can be made to also follow the status of a single nominated tunnel (CI) status. Users must nominate a specific tunnel identifier for this function to monitor. Current valid tunnels (CI) are in the range 4 to 512 and the tunnel must exist in order for it to be selectable.

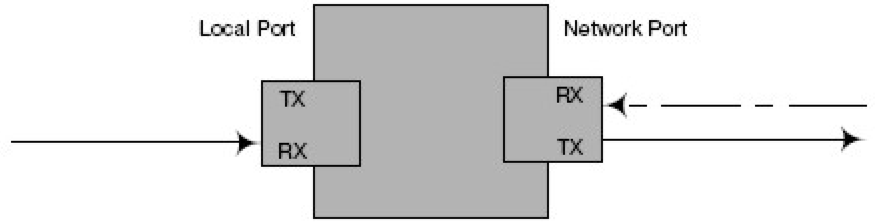
If the device’s mode is changed from multipoint mode to line mode, eLLF tied to connection shall automatically be disabled. If the user deletes the connection that has been nominated to tie eLLF to connection status, then eLLF tied to connection shall automatically be disabled. A message in the audit log shall be added when either of these cases occur.



Optical Link Loss Forwarding

When using optical SFP devices, both the RX and TX directions can be viewed and controlled in isolation. This permits the implementation of full bidirectional optical Link Loss Forwarding (oLLF).

The concept behind oLLF is to propagate changes in Rx signal to the Tx port of the opposite encryptor port. This has the effect of presenting the Ethernet encryptor as a real ‘bump in the wire.’ The result is that link losses within the network are not hidden between encryption devices, but rather propagated out to local side equipment. In the following figure, a loss of Rx signal on the network port will be forwarded to the local port by turning off the Tx laser on the local port.



Laser levels on both ports can be checked using the **sfp** command. This event can be verified by both audit and alarm log messages. Optical LLF can be configured to propagate local to network loss, network to local loss, or loss in both directions with the **linkspeed** command.

Link Loss Forwarding and Auto-Negotiation

In the example above, the local link Tx laser is disabled due to link loss forwarding. When auto-negotiation is enabled, the following may occur:

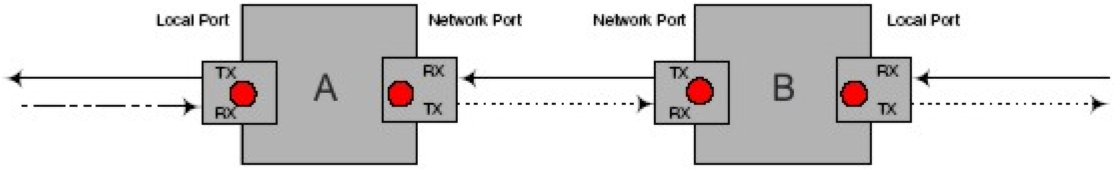
1. Auto-negotiation will be lost on the network side due to loss of the Rx link (NETWORK LED will be solid red).
2. The Tx laser on the local side is disabled due to network Rx loss. This produces an auto-negotiation loss on the local side (LOCAL LED is solid red).

However, when auto-negotiation is disabled, the following may occur:

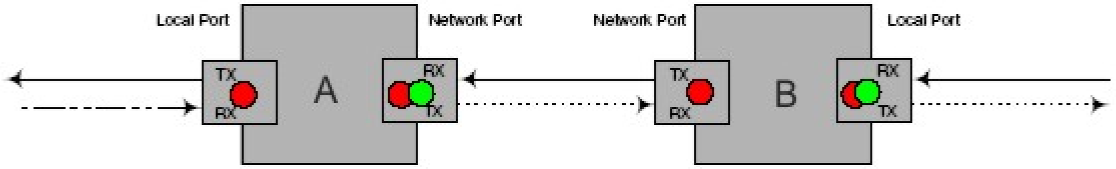
1. The loss of the Rx laser on the network side causes link down on network (NETWORK LED is solid RED).
2. The Tx laser on the local side is disabled due to network Rx loss. Since the Rx laser is still received on the local side the physical link is not seen as down. The Tx laser is disabled (LOCAL LED flashes red/green to indicate the port is administratively down).

Examples

In the following figure, a loss of Rx signal on the local port of encryptor A results in disabling the network Tx laser. This causes propagation of auto-negotiation loss on the network side of encryptor A. Both NETWORK and LOCAL LED indicators on encryptor A will be solid RED indicating loss of link (auto-negotiation) on both ports. The corresponding loss of Rx on the network port of encryptor B results in the propagation of the fault to the local port Tx (disabling the laser). Therefore, auto-negotiation is lost on both ports of the encryptor.



In this example, loss of Rx on the local port of encryptor A results in the Tx laser being turned off on the network side. The result for encryptor A is that the local port is down (solid red LED), but the network is administratively down as the network Rx laser is still being received (flashing green/red LED). Encryptor B detects corresponding loss of network Rx and propagates the loss to the local side by disabling the local side Tx laser. Encryptor B now determines the network port is down (solid red), and the local port is only administratively down (flashing green/red) as it still detects the Rx laser.



More combinations are possible, but the important questions to consider when looking at LLF and auto-negotiation are:

- Which unit is affected by the loss of Rx?
- Is the link completely lost (auto-negotiation is on) or is the link only administratively down (auto-negotiation is off, but the Tx laser has been disabled)?

Link Loss Forwarding Tied to the Connection

With the view that the Ethernet encryptors operate as a bump in the wire, it is conceptually correct that the definition of link loss holds not just for loss of physical connectivity, but also for loss of secure connection establishment.

With this in mind, a further extension for LLF is to tie the concept of connection establishment to the propagation of link loss. This functionality provides for minimal service interruption from the time local side equipment detects link up and the actual passing of secure traffic as the connection is already up prior to re-enabling local side ports.

This operation is only valid in line mode operation. See Linkspeed Command for more information on this command and the link loss forwarding settings.

Local Link Monitoring

Local link loss detection is disabled by default. The SEE can be configured to automatically detect local link loss with the **linkspeed –m –e** command. See Linkspeed Command for more information on enabling local link loss detection.

After detection of link loss on the local (trusted) side, traffic flow must be re-enabled manually. The following actions are automatically taken when local link loss is detected:

- local side traffic is blocked by automatically placing the unit in global discard mode. This is equivalent to performing a **global -d** command via the CLI.
- the event log is updated with a message indicating the reason for the global mode change.

To restore secure traffic flow, type the **global -e** command.

- Auto recovery functionality on the network side of the device is NOT affected by the changes listed above.

Ethertype Mutation

The SEE provides encryption for Transparent Layer 2 LAN Services (TLS). By definition, such services should not inspect the contents of the layer 2 payload. However, this is not always the case.

Typical cases are layer 2 switches that perform checksum/discard operations on IPv4 headers. Other switches have been observed to obey the IPv4 TOS header field under heavy load. In these cases and others, the encrypted data is being interpreted and packet loss or re-ordering may ensue.

Ethertype mutation provides a mechanism where the encrypted packet is translated to a predefined ethertype based on the original ethertype. The goal of this is to shift or mutate a packet to represent an unknown ethertype on the network. This mutation thereby removes the possibility of the network interpreting a particular packet and altering the encrypted payload.

This mutation is particularly useful in instances where packet re-ordering or checksum calculations are being performed. If the network does not understand the higher layer structures of the mutated type, it cannot make any analysis of the packet. Mutation also allows for operation through networks performing QoS.

The selected mutated value should not normally be observed on the network (for example; 0x0800 is mutated to 0xf800, which is generally not present).

The recommended action is to enable mutation to reduce the likelihood of interaction with equipment between the encryptors causing problems. See Ethertypes Command for information on editing an ethertype.

Injected NonMutant Traffic

If mutation is enabled for a given ethertype, the Injected NonMutant policy specifies how the encryptor should process frames received on the network port that are **not** mutated.

For example, if the encryptor is configured to mutate IP frames to 0xf800, then all encrypted IP traffic received from peer encryptors will have an ethertype of 0xf800. However, any IP traffic inserted by network equipment between the encryptors (for example, traffic destined for routers behind the encryptors) will be received by the encryptors with an ethertype of 0x0800.

The Injected Nonmutant policy specifies whether these frames should be bypassed or discarded by the encryptor. The recommended action is to discard these frames to prevent network traffic from interfering with the crypto stream. See Ethertypes Command for information on editing an ethertype.

Messages

The SafeNet Ethernet Encryptor records three types of messages pertaining to the configuration and operation of the unit. These are the alarm, audit, and event messages.

- Alarms are significant conditions that require attention. A flashing amber, flashing red, or solid red ALARM LED on the front panel denotes alarm conditions. There are unique alarm IDs assigned to each alarm type. The alarm table displays unacknowledged faults, either active or inactive. Acknowledging an alarm changes the state signifying knowledge of the alarm. After an alarm has been acknowledged, a corresponding message is entered in the audit log. Messages are entered in the event log when alarms are set and when the alarms are cleared. The alarm table is not preserved across power cycles.
- The audit log contains a record of configuration changes made to the SEE, such as commands that have been issued. The audit log can contain up to 4000 records of the last configuration changes and is preserved across power cycles.
- The event log contains messages on automatic actions taking place within the encryptor. Examples are key updates, enabled sessions, and alarm status. The event log can contain up to 4000 records of the last actions and is preserved across power cycles.

Software Upgrade and Downgrade

A software upgrade is performed to load a more recent version of software on the encryptor. The following concerns should be noted:

- the supported upgrade paths are from 3.4.x or 3.5.x to 4.0.0.
- the certificate is still valid after an upgrade.
- the upgrade does not invalidate configuration information.
- in order for a 1 Gbps device to operate in Counter mode, more than one 1 Gbps device must be upgraded to version 4.0.0 in order for the devices to interoperate.

A software downgrade is performed to return the encryptor to the previous version of software installed on the encryptor. The following concerns should be noted:

- the supported downgrade paths are from 4.0.0 to 3.5.x or 3.4.x.
- the certificate will not have to be reloaded.
- the downgrade can invalidate the configuration. Configuration changes completed while running software version 4.0.0 may not be maintained after the software is downgraded to version 3.5.x or 3.4.x and activated.

If a device running software version 4.0.0 has Multicast Security enabled or VLAN mode enabled and is downgraded to software version 3.5.x or 3.4.x (a version that does not support these new modes), the device's behavior will be unknown. To prevent this situation, use one of the following workarounds:

- configure/ensure the 4.0.0 device is in a mode supported by the earlier release prior to downgrading to 3.5.x or 3.4.x.
- downgrade the device from 4.0.0 to 3.5.x or 3.4.x and type **erase**.
- downgrade the device from 4.0.0 to 3.5.x or 3.4.x and type **initcfg –a**.

A software upgrade or downgrade is performed using SMCII. See the *SMCII User's Guide* for more information.

USB Port Operation

The USB port is generally reserved for supervised use in special support situations. It provides a means of installing updates locally on the SEE. Locked by default, the USB port may be unlocked or relocked by the CLI using the **usb** command or by SMCII. The USB port is automatically locked any time the unit is power cycled or restarted.

When a USB flash drive is inserted in an unlocked USB port, the device looks for a signed upgrade image. If a properly signed image is available on the flash drive, the user is prompted to enter the assigned 10-digit PIN on the front panel in order to process the image.

FIPS Mode Operation

The SEE uses the SNMPv3 privacy capabilities to secure management traffic between the device and SMCII. In some cases, such as network troubleshooting, the privacy may need to be temporarily disabled. With the SNMPv3 privacy disabled, the device is in a non-FIPS approved mode of operation. To accomplish this, complete the following steps:

1. Turn FIPS mode off
2. Turn SNMPv3 privacy off

To place the device back in a FIPS approved mode of operation, complete the following steps:

1. Turn SNMPv3 privacy on
2. Turn FIPS mode on

The configuration will be erased when FIPS mode is turned on or off.

See FIPS Mode Operation Guidance for full guidance on operating the encryptor in FIPS Mode.

This page intentionally left blank.

Installation

Security Requirements

In order to protect the integrity of your secure network there are a number of security requirements that need to be considered. These requirements are:

- The recommended location to install the SEE is in the same area as other sensitive electronic and communications equipment with access restricted to the network manager.
- Those responsible for IT security:
  - must ensure that the encryptor is delivered, installed, managed, and operated in a manner which maintains the defined network security. See FIPS Mode Operation Guidance for proper configuration and operation in FIPS mode.
  - must ensure that those parts of the encryptor that are critical to security policy enforcement are protected from physical attack which might compromise IT security.
  - must ensure that SMCII is protected from physical attack otherwise the private key used to sign certificates may be compromised.
  - are competent to manage the encryptor and can be trusted not to deliberately abuse their privileges so as to undermine security.
- Those responsible for the management of the encryptor must ensure that the authentication data for each account on the encryptor is held securely and not disclosed to persons not authorized to use that account.

⚠ *The current administrator account name and password must be stored in a secure location. If they are lost or forgotten the device will have to be returned to the factory.*

- Those responsible for the encryptor must ensure that connections are not provided to outside systems or users that would undermine IT security.
- Authorized users of the encryptor must ensure that audit facilities are used and managed effectively.
  - Appropriate action must be taken to ensure continued audit logging; for example, regular archiving of audit logs.
  - Audit and event logs should be inspected on a regular basis. Appropriate action should be taken on the detection of breaches of security or events that are likely to lead to a breach in the future.
- Security Management Center II is the only management station that can be used for remote management. Other SNMPv3 management products cannot provide a secure session and format commands correctly. Other SNMP management products can only receive traps from the SEE.

Network Requirements

The SEE has a very flexible policy that allows it to operate over transparent layer 2 Ethernet services. The encryptor is transparent to MPLS and VLAN services that fit within the definition of transparent Ethernet.

The following are network requirements (network refers to network between encryptor pairs):

- MAC address MUST be preserved.

  The network between encryptors cannot modify the Ethernet MAC addresses.

- Transmission order MUST be preserved for line mode and multipoint MAC mode.
  - QOS - this MUST occur outside of encryptors, not between encryptors. QOS may reorder frames.
  - L2 MPLS VPN - the MPLS control word MUST be enabled to guarantee transmission order.
- L2 payload SHALL NOT be looked into by network between encryptors.
- The network between encryptors may not discard frames based on L3 data (such as IP frame information) as this information is encrypted. Some layer 2 switches or network infrastructures may be designed to look at the IP portion of the header. If this is the case, an additional offset will be needed for the IP ethertype 0x0800. This offset can also be used when sniffing encrypted packets so the source and destination IP addresses are legible. See the *SMCII User's Guide* or this guide for modifying ethertype offsets.
- The network between encryptors cannot pass tag traffic with VLAN IDs to the encryptor network port that are not protected VLAN IDs on the local side of the encryptor.

The L2 payload (IPv4 header) is encrypted. Some L2/L3 devices may check the IPv4 header checksum. Where possible, this must be disabled as the IPv4 header is encrypted. Alternately, a variable encryption offset (20 bytes) for the IPv4 ethertype (0x800) can be used to circumvent this issue.

Choosing a Location

The SEE may be installed in a standard 19-inch rack or placed on a solid surface. Choose a location that is clean and dry. Ensure that the sides of the encryptor are unobstructed to allow air to flow around the vents. The operating and non-operating environmental ranges are specified in the Environmental topic.

Rack Mounting

The SEE is mounted forward facing in a standard 19-inch rack. Consider the following before installing the SEE in a rack:

- Operating Ambient Temperature - If the SEE is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient. Consideration should be given to installing the SEE in an environment compatible with our 40°C recommended maximum ambient temperature.
- Air Flow - Air flow required for safe operation should not be compromised. Maintain a clearance of at least three inches (7.62 cm) on each side of the encryptor to ensure adequate air intake and exhaust.

  An enclosed rack with a ventilation system that is too powerful can prevent proper cooling by creating negative air pressure around the SEE.

- Mechanical Loading - Uneven mechanical loading can produce a hazardous situation. Use the proper mounting hardware to secure the SEE to the rack.
- Circuit Overloading - Consideration should be given to the connection of an SEE to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring.
- Grounding - Maintain reliable grounding of a rack-mounted SEE. Particular attention should be given to supply connections other than direct connections to the branch circuit, such as the use of power strips.

To mount an SEE in a standard 19-inch rack:

1. Attach the right and left mounting brackets to the encryptor using the screws installed on the encryptor.
2. Attach the mounting brackets on the unit to the rack using the screws provided in the mounting bracket kit.

The SEE mounted in a standard 19-inch rack is shown below.

Installing an SFP/XFP

SafeNet tests and provides bail clasp transceivers (SFPs/XFPs) for use with the SafeNet Encryptors.

Prior to installing a transceiver, verify that the SFP/XFP is the correct type for your network. Do not remove the protective caps until you are ready to attach the network cable/optical fiber.

To install the SFP/XFP, complete the following steps:

1. Latch (flip upwards) the bail clasp before inserting.
2. Slide the SFP/XFP into the slot and press in until you feel or hear it click in place.

SFPs/XFPs are keyed to prevent incorrect installation.

Connecting the Cable/Optical Fiber

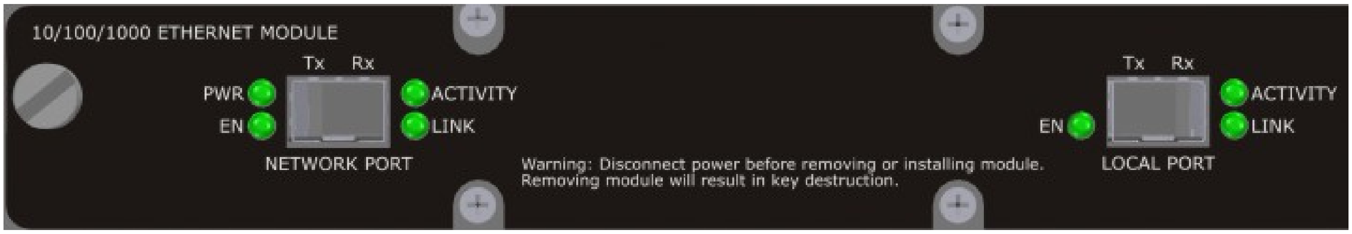
The private (local) port connects to the protected network. All frames received and transmitted on this interface are unencrypted. The public (network) port connects to the unprotected network. All frames received and transmitted on this interface are encrypted unless configured for unencrypted operation. The cables must be connected correctly or secure sessions cannot be established.

Do not remove the interface modules from the encryptor. If they are removed, the unit will have to be returned to the factory for repair.

FastEthernet

The FastEthernet (100 Mbps) unit is available with electrical SFP RJ-45 interface connections. Distances up to 100 meters are supported using Category 5 UTP cable. See Transceiver Specifications for more information.

The Tx and Rx labels on each port of the interface module refer to *transmit* and *receive*, respectively and public (network) and private (local) sides are shown. The following figure is a representation of the interface connections.


10/100/1000 ETHERNET MODULE
Tx
Rx
PWR
EN
ACTIVITY
LINK
NETWORK PORT
Warning: Disconnect power before removing or installing module.
Removing module will result in key destruction.
EN
Tx
Rx
ACTIVITY
LINK
LOCAL PORT

GbE

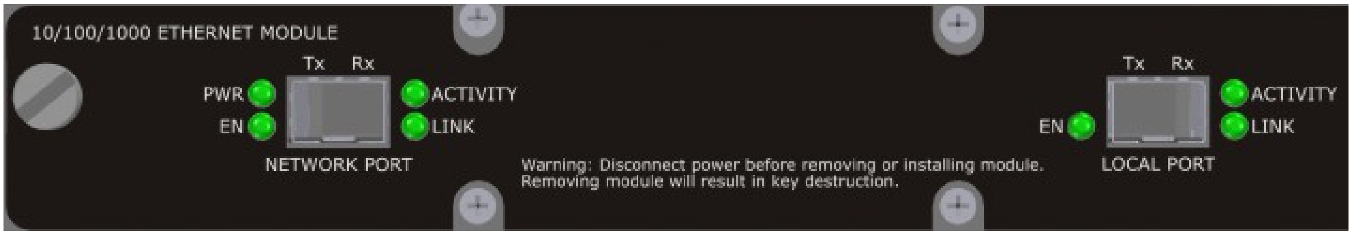
The GbE (1 Gbps) unit is available with three interface connections: electrical SFP RJ-45, single-mode (SM) optical, and multi-mode (MM) optical.

- For electrical SFP RJ-45 units, distances up to 100 meters are supported using Category 5 UTP cable. See Transceiver Specifications for more information.
- For SM optical units, distances up to 5000 meters are supported with SM fiber. See Transceiver Specifications for the longwave transceiver specifications.
- For MM optical units, distances up to 500 meters are supported with MM fiber. See Transceiver Specifications for the shortwave transceiver specifications.

Invisible laser radiation may be emitted from the aperture ports of the single-mode interface when no cable is connected. Avoid exposure and do not look into open apertures.

If the SM or MM fiber contains splices or if there are intermediate connectors or patch panels between the SEE and other equipment, the above ranges are shorter. If the SEE must function with longer distances than those listed above, add SONET repeaters to your connections.

The Tx and Rx labels on each port of the interface module refer to *transmit* and *receive*, respectively and public (network) and private (local) sides are shown. The following figure is a representation of the interface connections.


10/100/1000 ETHERNET MODULE
Tx
Rx
PWR
EN
ACTIVITY
LINK
NETWORK PORT
Warning: Disconnect power before removing or installing module.
Removing module will result in key destruction.
EN
Tx
Rx
ACTIVITY
LINK
LOCAL PORT

A common problem many network managers encounter when installing fiber optic cable is ensuring there is appropriate budget loss in the fiber path.

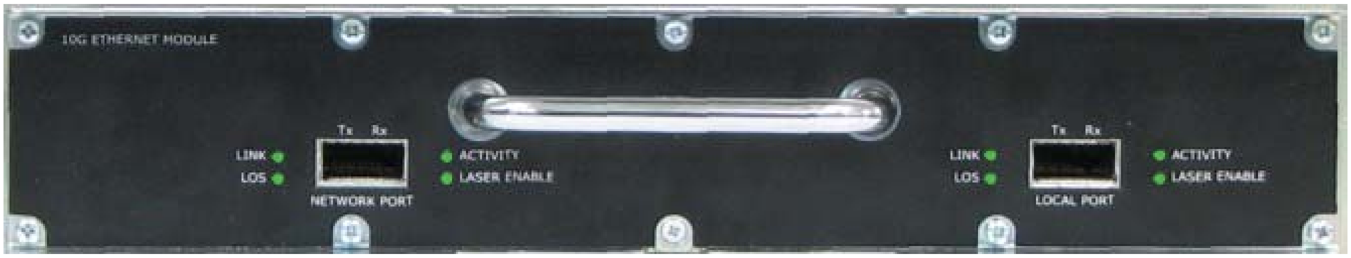
Bit errors can occur in either of these cases:

- If the power level at the receiver is less than the minimum, bit errors occur due to excessive loss.
- If the power level at the receiver is more than the maximum, bit errors occur due to saturation.

If errors occur, check your power levels using the transceiver specifications. Use an optical attenuator to reduce excessively high power levels.

10 GbE

There is a non-removable interface module evident on the rear panel of each 10 Gbps SEE. See the figure below for a view of the interface connections.



The Tx and Rx labels on each connection of the interface module refer to transmit and receive, respectively.

Invisible laser radiation may be emitted from the aperture ports when no cable is connected. Avoid exposure and do not look into open apertures.

A common problem many network managers encounter when installing fiber optic cable is ensuring there is appropriate budget loss in the fiber path.

Bit errors can occur in either of these cases:

- If the power level at the receiver is less than the minimum, bit errors occur due to excessive loss.
- If the power level at the receiver is more than the maximum, bit errors occur due to saturation.

If errors occur, check your power levels using Transceiver Specifications. Use an optical attenuator to reduce excessively high power levels.

Connecting the Cable/Optical Fiber

Attach the appropriate cable/optical fiber directly to the LC-type connector on the SFP/XFP. You may use either simplex or duplex connectors. For simplex connectors, two cables are required, one cable for transmit (Tx) and a second cable for receive (Rx). For duplex connectors, a single cable that has both Tx and Rx connectors is required.

1. Remove the protective cap from the SFP/XFP and save for future use.
2. Remove the protective caps from the connectors on the cable/optical fiber and save for future use.
3. Clean the connectors on the cable/fiber-optic cable.
4. Plug the cable/optical fiber into the LC-type connectors on the SFP/XFP.

Connecting the Ethernet Management Port

A 10/100 RJ-45 connection is used on the SEE. When successfully connected to the 10/100 RJ-45 port the green link indicator on the connector will be lit. Ethernet activity will be shown by a flashing amber LED.

Connecting the Serial Console Port

The SEE serial console port is a Data Terminal Equipment (DTE) device and can connect to other DTE devices (for example, terminals or end stations) using a null-modem RS-232C cable. The SEE can connect to a Data Communications Equipment (DCE) device (for example, a modem) using a straight through RS-232C cable. The serial cable needed for installation is dependent on the type of hardware being connected to the serial console port.

Configuration of the SEE can be completed by using the front panel and Security Management Center II. If using a console terminal for normal operation or for configuration, a serial cable can be connected between a PC running a terminal emulation program and the console port. The table below shows the PC communications settings.

Bits per second	9600
Data bits	8
Parity	None
Stop Bits	1
Flow Control	None

The recommended terminal settings when connecting to the SEE are listed in the table below.

Local Echo	Off
Line Wrap	On
Carriage Return/Carriage Return Left Translation **- Inbound** **- Outbound**	 Off Off

Applying AC Power

The SEE power supply autoranges to allow the use of input voltages from 100 to 240 volts AC and 50 to 60 Hz. For optimum reliability, protect the unit with an uninterruptible power supply (UPS). For use on a 120 V nominal input power source, a UPS with the following specifications is recommended: 300 VA rated power, 180 W output power capacity, and 120 V nominal output voltage. The SEE is designed to withstand normal power fluctuations and does not need a conditioned AC source. However, the unit does require green wire grounding (a grounded, three-pronged plug) with a low impedance connection for the ground wire to the earth ground.

⚠ *The specific power requirements are displayed on the bottom of the unit. If the AC power supply is outside the accepted range for the encryptor, it may not operate and could damage the encryptor.*

FastEthernet and GbE

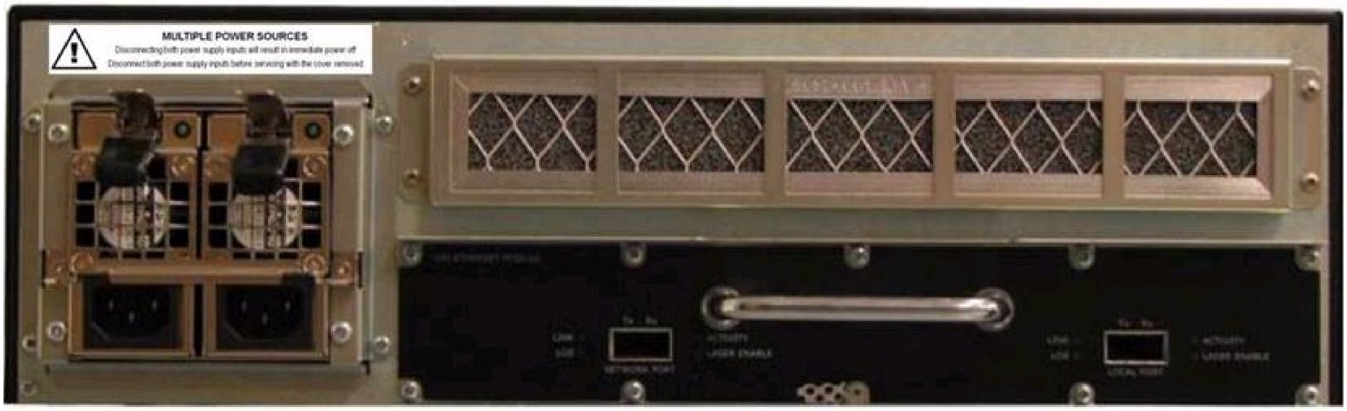
To apply AC power, complete the following steps:

1. Plug the supplied power cord into the power inlet on the rear of the encryptor and connect to the AC mains.
2. Turn the power switch on the bottom left corner of the rear panel to the ON position. The front panel LEDs will light and the fans will start turning.

The SEE takes from 90 to 120 seconds to complete booting.

10 GbE

The 10 GbE device has dual, hot-swappable AC power supply modules as shown in the following figure.


MULTIPLE POWER SOURCES
Disconnecting both power supply inputs will result in immediate power off
Disconnect both power supply inputs before servicing with the cover removed
LINK
LOS
Tx Rx
NETWORK PORT
ACTIVITY
LASER ENABLE
LOCAL PORT

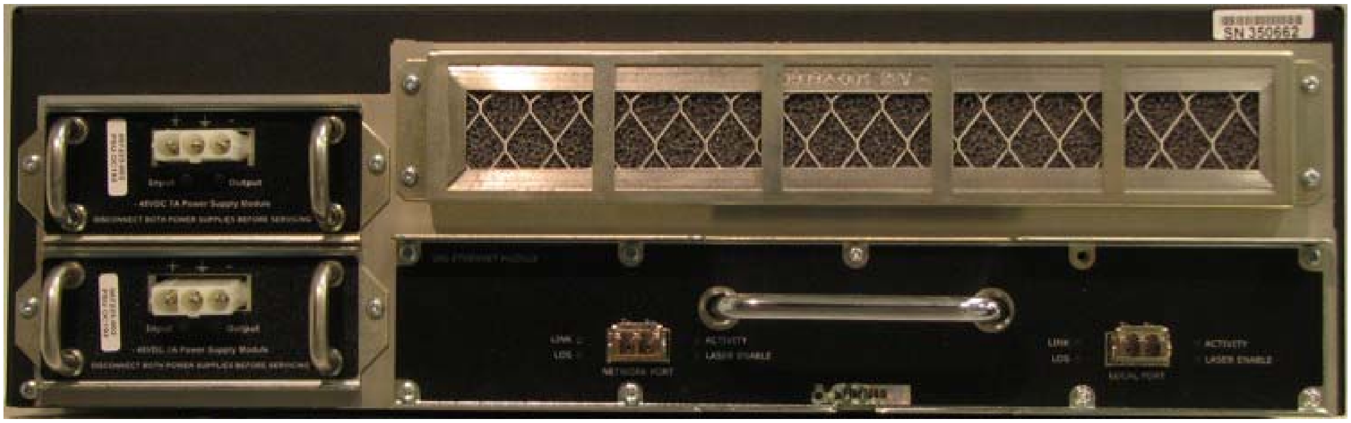
To apply AC power, complete the following steps:

1. Plug one supplied power cord into the right power inlet on the rear side of the encryptor and connect to the AC mains.
2. Plug one supplied power cord into the left power inlet on the rear side of the encryptor and connect to the AC mains.

The SEE takes from 90 to 120 seconds to complete booting.

DC Power and Grounding

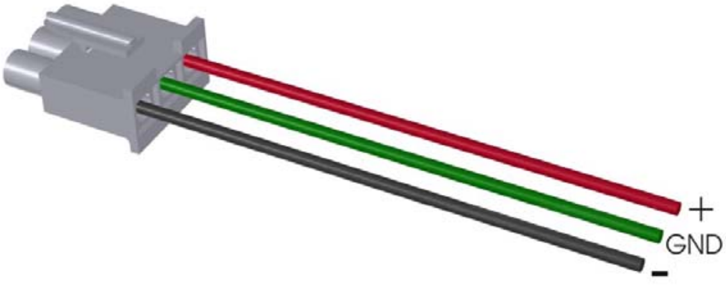
An alternate DC power supply is optionally available with the FastEthernet and GbE SEEs. The 10GbE encryptor is available with either an AC or DC dual, hot-swappable power supply. The 10 GbE encryptor with dual, hot-swappable DC power supplies is shown in the following figure.



Caution, to reduce the risk of electrical shock or energy hazards:

- Connect to a reliably grounded safety extra-low voltage (SELV) source.
- The branch circuit overcurrent protection must be rated a maximum of 15 A.
- Use 16 AWG solid copper wires only.
- Incorporate a readily accessible disconnect device that is suitably approved and rated into the field wiring.
- Install in a restricted access area in accordance with the NEC or the authority having jurisdiction.

An illustration of the DC power cable is shown below.



Power-up Self Tests

The SEE performs power-up self tests to verify the integrity and correct operational functioning of the device. Results from the power-up self tests are displayed on the LCD on the front panel. After successful testing, the following messages will be printed on the LCD:

- Message 1:
  Line 1:"Bootflash"
  Line 2:"v0.9-8"

- Message 2:
  Line 1:"SW selftest : ......"

- Message 3:
  Line 1:"SW selftest: Passed"
  Line 2:"Configuring System"

- Message 4:
  Line 1:"<*unit name*> ready"
  Line 2:"Self-tests passed"

- Message 5:
  Line 1:"FPGA FW self-test"
  Line 2:"FW self-test passed."

- Message 6:
  Line 1:"<*date*> <*time*>"
  Line 2:"up <*days*> days, <*hour:minutes*>"

If the device fails a self test, it transitions to an error state and blocks all traffic on the data ports. Information on error messages received after failure of a power-up self test is listed in Power-up Self Tests Error Messages.

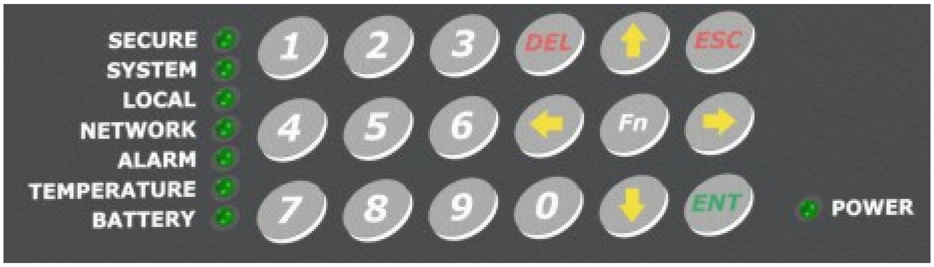
To initiate the power-up self tests on demand, reboot the encryptor.

LED Indicators

SEEs provide visual status information via LEDs on the front and rear panels of the unit.

Front Panel LEDs

A representation of the front panel LEDs is shown in the figure below. The status and activity represented by each of the front panel LEDs (red, amber, green, or flashing) is defined in the table below.



LED Name	State and Description
SECURE	▪ Green - the encryptor is certified and operating in secure mode according to the configured rules. ▪ Flashing Green - unit is certified, securing traffic, and operating in line mode according to the configured rules. ▪ Amber - the encryptor is certified and is operating in global discard mode. ▪ Flashing Amber - the encryptor is certified and is operating in global bypass mode. ▪ Red - the encryptor does not have a valid certificate installed and is operating in global discard mode. ▪ Flashing Red - the encryptor does not have a valid certificate installed and is operating in global bypass mode.
SYSTEM	▪ Off - the encryptor is no longer functioning. ▪ Green - the encryptor is functioning correctly. ▪ Flashing Green - the encryptor is functioning correctly. ▪ Red - the encryptor has detected a fault condition.

LED Name	State and Description
LOCAL	**FastEthernet and GbE** - Green - 1 Gbps full duplex. - Amber - 100 Mbps full duplex. - Flashing Amber - 10 Mbps full duplex. - Red - SFP OK, no link. - Flashing Red - SFP OK, in auto negotiation. - Flashing Red/Green - SFP OK, link down due to optical Link Loss Forwarding. - Off - No SFP detected. **10 GbE** - Green - XFP OK, link is up. - Red - XFP OK, no link. - Flashing Red/Green - XFP OK, link down due to optical Link Loss Forwarding. - Off - No XFP detected.
NETWORK	**FastEthernet and GbE** - Green - 1 Gbps full duplex. - Amber - 100 Mbps full duplex. - Flashing Amber - 10 Mbps full duplex. - Red - SFP OK, no link. - Flashing Red - SFP OK, in auto negotiation. - Flashing Red/Green - SFP OK, link down due to optical Link Loss Forwarding. - Off - No SFP detected. **10 GbE** - Green - XFP OK, link is up. - Red - XFP OK, no link. - Flashing Red/Green - XFP OK, link down due to optical Link Loss Forwarding. - Off - No XFP detected.
ALARM	- Green - there are no alarm conditions. - Flashing Amber - inactive, unacknowledged alarms exist. - Red - active, acknowledged alarms exist. - Flashing Red - active, unacknowledged alarms exist.

LED Name	State and Description
TEMPERATURE	▪ Green - the internal temperature is below the maximum allowable temperature. ▪ Flashing Red - the internal temperature exceeds the maximum allowable temperature.
BATTERY	▪ Green - the internal battery voltage is OK. ▪ Red - the internal battery voltage is low.
POWER	▪ Green - power is connected to the unit and the unit is powered on.

A link will auto negotiate the highest possible state between both local and network connections. Disconnection of either side will force a re-negotiation the other side for optimum connection state where auto negotiation is enabled.

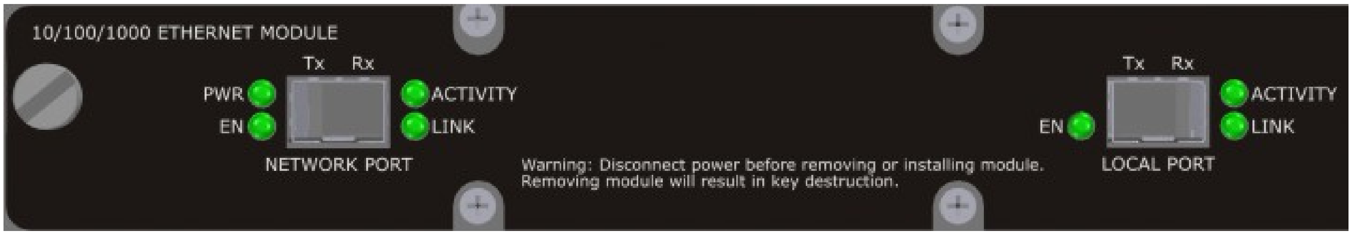
Rear Panel LEDs

On the rear panel, LEDs are located on the interface card. On the 10 GbE SEE, there are LEDs on the AC and DC power supply modules.

Interface Card LEDs

FastEthernet and GbE

The LEDs on the rear panel indicate the link status for the public (network) and private (local) ports. Green is lit when the ports are operating correctly.

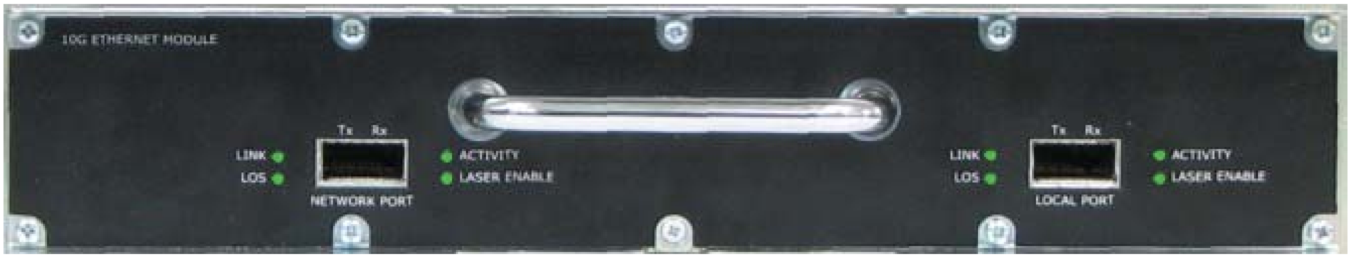

10/100/1000 ETHERNET MODULE
Tx
Rx
PWR
EN
ACTIVITY
LINK
NETWORK PORT
Warning: Disconnect power before removing or installing module.
Removing module will result in key destruction.
EN
Tx
Rx
ACTIVITY
LINK
LOCAL PORT

The following table lists each of the rear panel LEDs and a description of the status when the LED is on or off.

LED	On	Off
PWR	Power is present	Power is not present
EN	Transmitter is disabled	Transmitter is not disabled
ACTIVITY	Data is being received (LED is flashing)	Data is not being received
LINK	Signal is present	Signal is not present

10 GbE

The LEDs on the rear panel indicate the link status for the public (network) and private (local) ports. Green is lit when the ports are operating correctly.

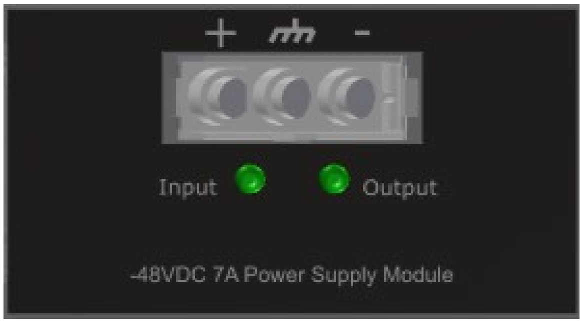


The following table lists each of the rear panel LEDs and a description of the status when the LED is on or off.

LED	On	Off
LINK	Signal is present	Signal is not present
LOS	Signal strength is OK	Loss of signal
ACTIVITY	Data is being received (LED is flashing)	Data is not being received
LASER ENABLE	Laser transmitter is enabled	Laser transmitter is disabled

DC Power Supply Module LEDs

The figure below shows the location of the LEDs on the power supply module panel. The LEDs are green when the DC power input and output is within functional specifications.



The table below lists the power supply module LEDs and a description of the status when the LED is on or off.

LED	On	Off
Input	-48 VDC nominal input power is present	-48 VDC nominal input power is not present
Output	Status of output power meets requirements	Status of output power does not meet requirements

Removing an SFP/XFP

To remove the SFP/XFP, complete the following steps:

1. Disconnect the optical fiber from the SFP/XFP LC-type connector.
2. Replace the protective caps on the optical fiber connectors.
3. Unlatch the bail clasp on the SFP/XFP and swing it downward.
4. Slide the SFP/XFP out of the slot.
5. Replace the protective cap on the SFP/XFP.

This page intentionally left blank.

Configuration

Management Options

Each SEE can be managed by different methods, which are:

- Security Management Center II (SMCII)
- serial console port
- front panel using the keypad and display

SMCII is required to fully manage the SEE and is the management method that should be used whenever possible. The front panel is used primarily to set the unit's IP address and install the certificate. The console interface provides basic configuration options.

Loading a certificate into the unit requires the combination of SMCII and a trusted person standing in front of the SEE using the front panel interface.

Console Port Operation

The console port provides a means of locally configuring and monitoring the SEE. It provides a command line interface (CLI) for examining the status and changing the configuration of certain parameters in the encryptor.

After the encryptor has finished booting it presents a login prompt. The prompt invites the user to log on to the unit with a user id and password. After three failed attempts to log on to the SEE the console will automatically lock for three minutes to prevent further attempts. This lock out is preserved across power cycles.

A user is automatically logged off if there has been no user input on the console port for the configured amount of time. The default setting is 10 minutes and can be reconfigured in SMCII. See Password Command for additional information.

User ID and Password Requirements

User ID

The user id must be between 3 and 10 characters long with no spaces.

Password

The SEE supports two levels of passwords, legacy and enhanced.

Legacy

The legacy password is case sensitive and must be between 8 and 29 characters long. The password must contain a combination of upper and lower case characters, numerals, and punctuation. Lexical checking verifies all passwords to these rules.

The same password cannot be used continually. The password reuse parameter is set to 255, which means a particular password cannot be used again for the next 255 password settings.

Enhanced

The enhanced password capability allows the password to be strengthened with various configuration options. The enhanced password features are changed using Security Management Center II and the CLI. See Password Command for additional information.

User Account Status

The user account status becomes inactive for operator level accounts if there is no activity for 30 days. In order for the user to log on to that account again the administrator will have to reactivate the account. The administrator account is never locked out due to inactivity.

User Types

Each SEE allows up to 30 unique users to be defined. Each user is assigned one of the privilege levels explained in the following table. An unconfigured or erased device contains one default Administrator account. A certificate must be loaded on the device before user accounts can be added.

User	Privileges
Administrator	Full access to all internal parameters for unlimited configuration and monitoring. The role of the administrator is to create other user accounts, load certificates into the encryptor, and configure the SEE for operation. Normally there would be only one administrator account.
Operator	View configuration parameters only. Operators cannot change their password or create, modify, or delete any internal configuration parameters.

Front Panel

The front panel consists of management connections and ports, a two line by twenty-character liquid crystal display, and a numeric keypad. Its principal use is to enter the IP address and install a certificate into the SEE. After a certificate has been installed, the front panel can no longer be used to make configuration changes.

Display Screens

The front panel has five different display screens with a combination of configurable and view-only information. The information listed on each screen is as follows:

- YYYY-MM-DD HH:MM:SS - current date and time (configurable)
  Total up time: Up X days HH:MM - time since last reboot (view-only)
  This is the default display.

- Name assigned to unit (view-only)
  IP - IP address assigned to unit (configurable)

  When configuring the IP address, the IP netmask and IP gateway must also be configured.

- Temperature - current temperature of unit in degrees Celsius (view-only)
  Alarm - maximum allowed temperature (view-only)

- Certificate mode - Certificate mode (configurable)

  The Certificate mode display shows “Waiting for X.509/certificate request” until a certificate is loaded.

- S/W Version - installed software version (view-only)
  F/W Version - hardware version (view-only)

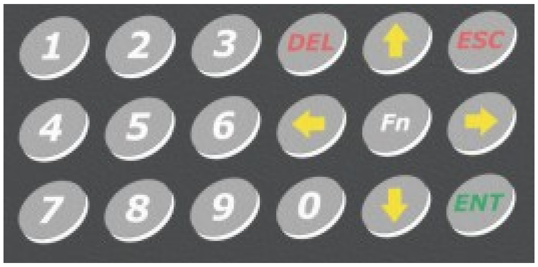
- B-Date - None (view-only)
  B-Time - None (view-only)

- B-Number - None (view-only)
  B-Delta - Dxxx (view-only)

- enc - in Mb/s - encrypted packet bandwidth (view-only - displayed on the 10Mbps and FastEthernet units only)
  dec - in Mb/s - decrypted packet bandwidth (view-only - displayed on the 10Mbps and FastEthernet units only)

Keypad Operation

Configuration changes to the configurable items listed above are accomplished using the keypad on the front panel of the encryptor.



Instructions for using the keypad are listed below:

- Press the keypad function key (Fn) to scroll through the display screens.
- Use the left and right arrows to move around on the line of data for configurable items.
- Press ENT to accept a configuration change.
- Press ESC to abandon a configuration change.
- After 5 minutes of inactivity the front panel display will return to its default mode.
- The ENT key is automatically locked when a certificate is installed. It can be unlocked and relocked using SMCII.

Factory Default Parameters

The SafeNet Ethernet Encryptor is delivered with the factory default parameters as shown in the following tables.

Parameter	Setting
Management IP Address - IPv4	0.0.0.0
Management IP Address - IPv6	::
Inband Management IP Address - IPv4	0.0.0.0
Certificate loaded	None
Date and Time	Coordinated Universal Time (UTC)

Administrator account	user=admin
	password=$Safenet1

Certificates	Not present
Key update interval	60 minutes
USB port	Locked
Global (operating) mode	Discard all
Crypto mode	AES CFB
MPLS shim bypass	Enabled
VLAN header bypass	Enabled
SNAP PID	Enabled
Auto session discovery (Unicast)	Enabled

Parameter	Setting
Auto session discovery (Multicast/VLAN)	Disabled
Auto session discovery ageing (multicast only)	0 (disabled)
Line mode	Disabled
Auto Negotiation	Enabled
Local link monitoring	Disabled
Optical link loss forwarding (LLF)	Disabled
LLF tied to connection (line mode)	Enabled
Bypass reserved multicast	Disabled
STP monitoring	Disabled
Tunnel keep alive monitoring	Disabled
Observe pending on unknown (DA) ingress	Disabled
Inter frame gap	Repeater shaved 88 bit
Alternate MPLS ethertype value	0x8848
Primary VLAN ethertype value	0x8100
Alternate VLAN ethertype value	0x8100
VLAN stack depth	2
SHIM rate	32
MTU overflow prevention on shim	Enabled
FIPS mode	Enabled
Audit and event log wrapping	Enabled
SNMP Privacy	Enabled

Ethertypes - Line Mode

Ethertype	Offset Enable	Encryption Offset	Mutate Enable	Mutated Ethertype	Unicast	Multicast	Broadcast	Injected NonMutant
0x05ff	N	0x0	NA	NA	UseCI	UseCI	UseCI	NA
0x0800	N	0x14	Y	0xf800	UseCI	UseCI	UseCI	Discard
0x0806	N	0x0	Y	0xf806	UseCI	UseCI	UseCI	Discard
0x86dd	N	0x28	Y	0xf6dd	UseCI	UseCI	UseCI	Discard
0x8808	N	0x0	N	0xf808	Bypass	Bypass	Bypass	Bypass
0x8809	N	0x0	N	0xf809	Bypass	Bypass	Bypass	Bypass
0x88cc	N	0x0	N	0xf8cc	Bypass	Bypass	Bypass	Bypass
0x9000	N	0x0	N	0xf000	Bypass	Bypass	Bypass	Bypass
Other*	N	0x0	NA	NA	UseCI	UseCI	UseCI	NA

* These are the default settings for all ethertypes not specifically listed above.

Ethertypes -Multipoint MAC Mode

Ethertype	Offset Enable	Encryption Offset	Mutate Enable	Mutated Ethertype	Unicast	Multicast	Broadcast	Injected NonMutant
0x05ff	N	0x0	NA	NA	UseCI	Bypass	Bypass	NA
0x0800	N	0x14	Y	0xf800	UseCI	Discard	Bypass	Discard
0x0806	N	0x0	N	0xf806	Bypass	Discard	Bypass	Bypass
0x86dd	N	0x28	Y	0xf6dd	UseCI	Discard	Bypass	Discard
0x8808	N	0x0	N	0xf808	Bypass	Bypass	Bypass	Bypass
0x8809	N	0x0	N	0xf809	Bypass	Bypass	Bypass	Bypass
0x88cc	N	0x0	N	0xf8cc	Bypass	Bypass	Bypass	Bypass
0x9000	N	0x0	N	0xf000	Bypass	Bypass	Bypass	Bypass
Other*	N	0x0	NA	NA	UseCI	Discard	Discard	NA

* These are the default settings for all ethertypes not specifically listed above.

Ethertypes - Multipoint VLAN Mode

Ethertype	Unicast	Multicast	Broadcast
0x05ff	UseCI	UseCI	UseCI
0x0800	UseCI	UseCI	UseCI
0x0806	UseCI	UseCI	UseCI
0x86dd	UseCI	UseCI	UseCI
0x8808	Bypass	Bypass	Bypass
0x8809	Bypass	Bypass	Bypass
0x88cc	Bypass	Bypass	Bypass
0x9000	Bypass	Bypass	Bypass
Other*	Bypass	Bypass	Bypass

* These are the default settings for all ethertypes not specifically listed above.

Connection Identifiers - Multipoint MAC Mode

CI	Origin	Action	State	Peer Name
0001	PENDING	Discard	Up	N/A
0002	System	Discard	Up	N/A
0003	System	Bypass	Up	N/A

Configuring a Factory Delivered Unit

Configuring the Ethernet Management Port

Verify the network configuration and configure the SEE's Ethernet management port settings if necessary. The SEE's current configuration can be displayed with the **ip** command and modified with the **ip –c** command. See IP Command for more information.

Logging on to the SEE

From the CLI, perform the following steps:

1. At the **LOGIN** prompt, enter **admin**.
2. At the **PASSWORD** prompt, enter **$Safenet1**.

The default administrator account information will be updated during the certification process. Password requirements are found in User ID and Password Requirements.

Setting the IP Address

The SafeNet Ethernet Encryptor is designed to be remotely managed using SMCII. Hence the SEE must be assigned a unique IP address.

The IP address to use depends on the local network. See the network administrator for a valid IP address that can be assigned to the SEE.

The SEE uses a static IP address and does not support any form of dynamic IP assignment, such as DHCP.

The IP address can be entered from the RS232 port using the **ip -s** command or from the front panel using the keypad and display.

RS232 Port

To enter the IP address from the RS232 port, type **ip -s <*index*> <*address*>/<*prefix*> <*gateway*>**. Enter the Management IP address/prefix and Management IP gateway for your device.

See the IP Command topic for more information on entering IPv4 and IPv6 management IP addresses.

```
SafeEnterprise Encryptor>ip -s 1 10.0.100.179/8 10.0.100.2
SafeEnterprise Encryptor>
```

Front Panel

To enter the IP address from the front panel:

1. Press the **Fn** key until the display shows **IP**. Press the **ENT** key.
2. Enter the IP address using the numeric keypad. The left and right arrows can be used to position the cursor over a digit for editing. After the IP address has been entered, press the **ENT** key. A display will appear prompting for the Netmask and Gateway.
3. Enter the **Netmask** and **Gateway** using the numeric keypad.
4. Press **ENT** to load the IP address into the encryptor.

Once an encryptor has a valid IP address it can be managed using Security Management Center II.

Adding the SEE to the SMCII Database

The first step in the SMCII is to add the SEE to the SMCII database. The encryptor name and description, IP address, and SNMP user name and password are entered to add the encryptor to the Device Management. See the *Security Management Center II User's Guide* for instructions.

Loading a Certificate

A certificate which has been signed by SMCII acting as a trusted Certifying Authority needs to be installed before any further configuration changes can be made.

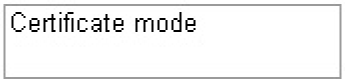
Installing a certificate requires an administrator using Security Management Center II connected to the encryptor and an operator physically located in front of the encryptor using the keypad and display. The encryptor must have been previously initialized with an IP address, netmask, and gateway. Also, the correct date and time must be set before loading a certificate.

More than one SMCII station can be used to manage a network. However, all encryptors in the network must be authenticated using the same CA. This can be accomplished by using the same SMCII server or by using an SMCII client authenticated by that SMCII server for each authentication.

If an attempt is made to load a certificate before the public/private keys have been generated, the SECURE LED on the front of the unit flashes indicating that key generation is still in progress. The SECURE LED is red if the unit has no current valid certificate and green if the unit has a current valid certificate.

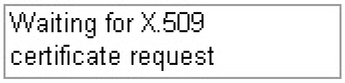
Complete the following steps to load the certificate:

1. Put the SEE into certificate mode by repeatedly pressing the **Fn** key on the SEE keypad until the LCD screen shows:

   Certificate mode

2. Press the **ENT** key to change the screen to:

   Waiting for X.509
   certificate request

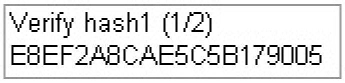
   If the screen fails to respond to the ENT key it may mean the keypad is locked. See the *Security Management Center II User's Guide* for instructions on unlocking the keypad.

3. The SMCII administrator requests the SEE to send a blank certificate to SMCII. The blank certificate contains the encryptor's public RSA key.

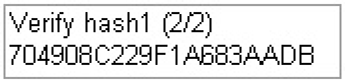
   The SEE will not accept the certificate if the encryptor's date and time is before or after the certificate's validity period. The certificate is back-dated 24 hours to account for differences between SMCII's clock and the encyptor's clock.

   When the certificate has been received, both the SEE and SMCII calculate a validation code over the blank certificate. The code is displayed in SMCII and on the SEE.

4. The SEE operator and the SMCII administrator must confirm verbally that the codes displayed in SMCII and on the SEE match. On the SEE, the code is displayed on two LCD screens. After confirming the first screen, press the right arrow on the keypad to display the second screen. An example of both screens is shown below.

   Verify hash1 (1/2)
   E8EF2A8CAE5C5B179005

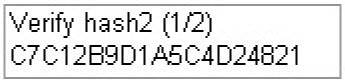
   Verify hash1 (2/2)
   704908C229F1A683AADB

   If the codes do not match it is an indication of possible tampering with the certificate during transport. The SMCII administrator should reject the blank certificate which will terminate the certificate operation.

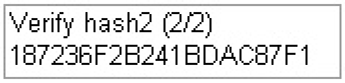
5. The SMCII administrator enters device identification information and a new user name and password which replaces the default administrator account. After the SMCII administrator clicks OK, the completed certificate is signed by SMCII and transmitted to the SEE.

Signing the certificate causes SMCII to fill in the blank certificate with a serial number and expiration date. A validation code is calculated again and displayed both on the SEE and SMCII.

6. The SEE operator and SMCII administrator must confirm verbally that the codes displayed on the SEE and in SMCII match. The validation code is shown on two LCD screens again on the SEE as shown in the following example:



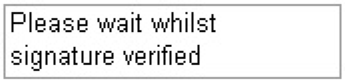
```
Verify hash2 (1/2)
C7C12B9D1A5C4D24821
```



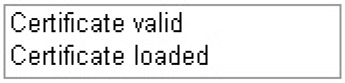
```
Verify hash2 (2/2)
187236F2B241BDAC87F1
```

7. If the codes match press the **ENT** key on the SEE to store the certificate in the encryptor. Wait while the SEE verifies that the signature on the certificate is valid.

   The following two LCD screens are shown during verification and after loading the valid certificate into the SEE’s internal configuration by replacing the existing certificate.



```
Please wait whilst
signature verified
```



```
Certificate valid
Certificate loaded
```

   The SECURE LED turns green and the ENT key is locked. Pressing the **ESC** key returns the display to the default state.

It is extremely important that the validation codes are confirmed for each step. The validation codes prevent a 'man-in-the-middle' attack when the encryptor public key is sent to SMCII and when the signed certificate is returned to the encryptor. Failure to confirm the validation codes could result in a serious compromise of your Ethernet network.

Certificates and Data Flow

The following list details tunnel and data flow functionality according to the certificate status:

- certificate has not been loaded - cannot add any tunnels
- valid certificate - can add secure and bypass tunnels
- expired certificate (no reboot or power-cycle) - cannot add new tunnels; user data on existing tunnels continues to flow (the existing tunnels do not break when the certificate has expired); existing tunnels persist through network interruptions and user data continues to flow after network interruptions are restored
- expired certificate (after reboot or power-cycle) - cannot add new tunnels; user data on bypass tunnels continues to flow; user data on secure tunnels stops (fault state)
- new certificate from different certificate authority - user data on existing tunnels continues to flow (the existing tunnels do not break when the new certificate is introduced); existing tunnels persist through network interruptions and user data continues to flow after network interruptions are restored

Certificate Expiration

When the certificate is nearing expiration, the encryptor provides notification by adding messages to the event log, setting alarms, and sending traps. The following list contains messages added to the event log:

```
WARNING - Certificate will expire in less than 28 days
WARNING - Certificate will expire in less than 21 days
WARNING - Certificate will expire in less than 14 days
WARNING - Certificate will expire in less than 7 days
WARNING - Certificate will expire in less than 6 days
WARNING - Certificate will expire in less than 5 days
WARNING - Certificate will expire in less than 4 days
WARNING - Certificate will expire in less than 3 days
WARNING - Certificate will expire in less than 2 days
WARNING - Certificate will expire in less than 24 hours
```

When the certificate is within 24 hours of expiration a trap is sent containing the text "WARNING - Certificate will expire in less than 24 hours".

The encryptor should be re-authenticated before the certificate expires. The re-authentication procedure is the same as loading the initial certificate, except there is no requirement for the SEE Branch Office operator to confirm the re-authentication in the CLI. There is no limit to the number of times the encryptor can be re-authenticated.

Configuring the Link Settings

Configure the link settings - set the current link speed and enable or disable auto negotiation. See the *Security Management Center II User's Guide* for instructions.

Configuring the Global Policy Settings

Configure the global policy settings - global operation mode, MAC address discovery, and ethertypes. See the *Security Management Center II User's Guide* for instructions.

Adding New Users

Adding new users is completed using the **users -a** command or in Security Management Center II. See the *Security Management Center II User’s Guide* for more information.

Viewing Event, Alarm, and Audit Logs

Viewing event, alarm, and audit logs is completed using the **event**, **alarm**, and **audit** commands, respectively. They can also be displayed in Security Management Center II. See the *Security Management Center II User’s Guide* for more information.

Backing Up and Restoring Configurations

Backing up and restoring configurations is completed in Security Management Center II. See the *Security Management Center II User’s Guide* for more information.

Downloading and Upgrading Firmware

Downloading and upgrading firmware is completed in Security Management Center II. See the *Security Management Center II User’s Guide* for more information.

Configuring Inband Management

If inband management will be used with the device, it can be enabled now via the **ip** command.

Use Case Scenarios

Configuring Line Mode

The example below shows how to configure secure traffic in line mode. See Modes for a network configuration and detailed information on line mode.

1. Reset the encryptor's configuration to the default state by typing the **initcfg -a** command. This command will cause the encryptor to restart.

```
SEE_A>initcfg -a

SEE_B>initcfg -a
```

2. Enable line mode on the peer encryptor and then the local encryptor by typing the **line -e** command. This command will cause the encryptor to restart.

```
SEE_A>line -e

SEE_B>line -e
```

3. Verify the Connection Identifier table is in the default state by typing the **tunnels** command. (This command is optional.)

```
SEE_A>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa
Key update interval : 60 minutes

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0001 System   Secure   Start    TBD              00:00:00:00:00:00:00

SEE_B>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb
Key update interval : 60 minutes

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0001 System   Secure   Start    TBD              00:00:00:00:00:00:00
```

4. Set the unit to encrypt data by typing the **global -e** command.

```
SEE_A>global -e

SEE_B>global -e
```

5. Confirm that the tunnels are in the Up state by typing the **tunnels** command. (This command is optional.)

```
SEE_A>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa
Key update interval : 60 minutes

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0001 System   Secure   Up       SEE_B            00:d0:1f:bb:bb:bb
```

```
SEE_B>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb
Key update interval : 60 minutes

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0001 System   Secure   Up       SEE_A            00:d0:1f:aa:aa:aa
```

Configuring Multipoint MAC Mode With Automatic Connection Discovery

The example below shows how to configure secure traffic in multipoint MAC mode with automatic connection discovery. See Modes for a network configuration and detailed information on multipoint MAC mode.

1. Set the connection mode to MAC mode by typing the **con -m** command.

```
SEE_A>con -m

SEE_B>con -m

SEE_C>con -m
```

2. Reset the encryptor's configuration to the default state by typing the **initcfg -a** command. This command will cause the encryptor to restart.

```
SEE_A>initcfg -a

SEE_B>initcfg -a

SEE_C>initcfg -a
```

3. Enable automatic connection discovery by typing the **autodisco -e** command.

```
SEE_A>autodisco -e

SEE_B>autodisco -e

SEE_C>autodisco -e
```

4. Set the unit to encrypt data by typing the **global -e** command.

```
SEE_A>global -e

SEE_B>global -e

SEE_C>global -e
```

5. Confirm that the tunnels are in the Up state by typing the **tunnels** command and that the addresses were discovered correctly by typing the **netmacs** and **locmacs** commands. (These commands are optional.)

```
SEE_A>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa
Key update interval : 60 minutes

CI   Origin    Action   State    Peer Name        Remote MAC           MAC Header
---- --------  -------- -------- ---------------- -------------------- ----------------
0001 PENDING   Discard  Up       N/A
0002 System    Discard  Up       N/A
0003 System    Bypass   Up       N/A
0004 Auto      Secure   Up       SEE_B            00:d0:1f:bb:bb:bb
0005 Auto      Secure   Up       SEE_C            00:d0:1f:cc:cc:cc
```

```
SEE_A>netmacs

Network Mac       CI
----------------- ----
00:d0:1f:bb:bb:bb 0004
00:22:22:22:22:22 0004
00:d0:1f:cc:cc:cc 0005
00:33:33:33:33:33 0005
4 Valid records

SEE_A>locmacs

Local Mac
-----------------
00:11:11:11:11:11
1 Valid record

SEE_B>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb
Key update interval : 60 minutes

CI   Origin    Action   State    Peer Name        Remote MAC           MAC Header
---- --------  -------- -------- ---------------- -------------------- ----------------
0001 PENDING   Discard  Up       N/A
0002 System    Discard  Up       N/A
0003 System    Bypass   Up       N/A
0004 Auto      Secure   Up       SEE_A            00:d0:1f:aa:aa:aa
0005 Auto      Secure   Up       SEE_C            00:d0:1f:cc:cc:cc

SEE_B>netmacs

Network Mac       CI
----------------- ----
00:d0:1f:aa:aa:aa 0004
00:11:11:11:11:11 0004
00:d0:1f:cc:cc:cc 0005
00:33:33:33:33:33 0005
4 Valid records

SEE_B>locmacs

Local Mac
-----------------
00:22:22:22:22:22
1 Valid record

SEE_C>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:cc:cc:cc
Front Panel Management MAC address : 00:d0:1f:00:cc:cc
Key update interval : 60 minutes

CI   Origin    Action   State    Peer Name        Remote MAC           MAC Header
---- --------  -------- -------- ---------------- -------------------- ----------------
0001 PENDING   Discard  Up       N/A
0002 System    Discard  Up       N/A
0003 System    Bypass   Up       N/A
0004 Auto      Secure   Up       SEE_A            00:d0:1f:aa:aa:aa
0005 Auto      Secure   Up       SEE_B            00:d0:1f:bb:bb:bb
```

```
SEE_C>netmacs

Network Mac       CI
----------------- ----
00:d0:1f:aa:aa:aa 0004
00:11:11:11:11:11 0004
00:d0:1f:bb:bb:bb 0005
00:22:22:22:22:22 0005
4 Valid records

SEE_C>locmacs

Local Mac
-----------------
00:33:33:33:33:33
1 Valid record
```

6. Disable automatic connection discovery to lock down the configuration by typing the **autodisco -d** command.

```
SEE_A>autodisco -d

SEE_B>autodisco -d

SEE_C>autodisco -d
```

Configuring Multipoint MAC Mode Manually

The example below shows how to configure secure traffic in multipoint MAC mode manually. See Modes for a network configuration and detailed information on multipoint MAC mode.

1. Set the connection mode to MAC mode by typing the **con -m** command.

```
SEE_A>con -m

SEE_B>con -m

SEE_C>con -m
```

2. Reset the encryptor's configuration to the default state by typing the **initcfg -a** command. This command will cause the encryptor to restart.

```
SEE_A>initcfg -a

SEE_B>initcfg -a

SEE_C>initcfg -a
```

3. Disable automatic connection discovery by typing the **autodisco -d** command.

```
SEE_A>autodisco -d

SEE_B>autodisco -d

SEE_C>autodisco -d
```

4. Set the unit to encrypt data by typing the **global -e** command.

```
SEE_A>global -e

SEE_B>global -e

SEE_C>global -e
```

5. Add the tunnels by typing the **tunnels -a <*MAC address*>** command.

```
SEE_A>tunnels -a 00:d0:1f:bb:bb:bb
Remote Encryptor Name : [] SEE_B
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
Header content in HEX : []
Added new tunnel ci 4

SEE_A>tunnels -a 00:d0:1f:cc:cc:cc
Remote Encryptor Name : [] SEE_C
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
Header content in HEX : []
Added new tunnel ci 5

SEE_B>tunnels -a 00:d0:1f:aa:aa:aa
Remote Encryptor Name : [] SEE_A
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
Header content in HEX : []
Added new tunnel ci 4

SEE_B>tunnels -a 00:d0:1f:cc:cc:cc
Remote Encryptor Name : [] SEE_C
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
Header content in HEX : []
Added new tunnel ci 5

SEE_C>tunnels -a 00:d0:1f:aa:aa:aa
Remote Encryptor Name : [] SEE_A
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
Header content in HEX : []
Added new tunnel ci 4

SEE_C>tunnels -a 00:d0:1f:bb:bb:bb
Remote Encryptor Name : [] SEE_B
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
Header content in HEX : []
Added new tunnel ci 5
```

6. Enter the local MAC addresses by typing the **locmacs -a <*MAC address*>** command.

```
SEE_A>locmacs -a 00:11:11:11:11:11
Added new local mac address

SEE_B>locmacs -a 00:22:22:22:22:22
Added new local mac address

SEE_C>locmacs -a 00:33:33:33:33:33
Added new local mac address
```

7. Enter the network MAC addresses by typing the **netmacs -a <*MAC address*>** command.

```
SEE_A>netmacs -a 00:22:22:22:22:22
Enter CI to associate mac address with : 4
Added new remote mac address

SEE_A>netmacs -a 00:33:33:33:33:33
Enter CI to associate mac address with : 5
Added new remote mac address

SEE_B>netmacs -a 00:11:11:11:11:11
Enter CI to associate mac address with : 4
Added new remote mac address

SEE_B>netmacs -a 00:33:33:33:33:33
Enter CI to associate mac address with : 5
Added new remote mac address
```

```
SEE_C>netmacs -a 00:11:11:11:11:11
Enter CI to associate mac address with : 4
Added new remote mac address

SEE_A>netmacs -a 00:22:22:22:22:22
Enter CI to associate mac address with : 5
Added new remote mac address
```

8. Confirm that the tunnels are in the Up state by typing the **tunnels** command . (This command is optional.)

```
SEE_A>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa
Key update interval : 60 minutes

CI   Origin    Action   State    Peer Name        Remote MAC           MAC Header
---- --------  -------- -------- ---------------- -------------------- ----------------
0001 PENDING   Discard  Up       N/A
0002 System    Discard  Up       N/A
0003 System    Bypass   Up       N/A
0004 Manual    Secure   Up       SEE_B            00:d0:1f:bb:bb:bb
0005 Manual    Secure   Up       SEE_C            00:d0:1f:cc:cc:cc

SEE_B>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb
Key update interval : 60 minutes

CI   Origin    Action   State    Peer Name        Remote MAC           MAC Header
---- --------  -------- -------- ---------------- -------------------- ----------------
0001 PENDING   Discard  Up       N/A
0002 System    Discard  Up       N/A
0003 System    Bypass   Up       N/A
0004 Manual    Secure   Up       SEE_A            00:d0:1f:aa:aa:aa
0005 Manual    Secure   Up       SEE_C            00:d0:1f:cc:cc:cc

SEE_C>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:cc:cc:cc
Front Panel Management MAC address : 00:d0:1f:00:cc:cc
Key update interval : 60 minutes

CI   Origin    Action   State    Peer Name        Remote MAC           MAC Header
---- --------  -------- -------- ---------------- -------------------- ----------------
0001 PENDING   Discard  Up       N/A
0002 System    Discard  Up       N/A
0003 System    Bypass   Up       N/A
0004 Manual    Secure   Up       SEE_A            00:d0:1f:aa:aa:aa
0005 Manual    Secure   Up       SEE_B            00:d0:1f:bb:bb:bb
```

Configuring Multipoint VLAN Mode With Automatic Connection Discovery

The example below shows how to configure secure traffic in multipoint VLAN mode with automatic connection discovery. See Modes for a network configuration and detailed information on multipoint VLAN mode.

1. Set the connection mode to VLAN mode by typing the **con -v** command.

```
SEE_A>con -v

SEE_B>con -v

SEE_C>con -v
```

2. Reset the encryptor's configuration to the default state by typing the **initcfg -a** command. This command will cause the encryptor to restart.

```
SEE_A>initcfg -a

SEE_B>initcfg -a

SEE_C>initcfg -a
```

3. Enable automatic connection discovery by typing the **autodisco -e** command.

```
SEE_A>autodisco -e

SEE_B>autodisco -e

SEE_C>autodisco -e
```

4. Set the unit to encrypt data by typing the **global -e** command.

```
SEE_A>global -e

SEE_B>global -e

SEE_C>global -e
```

5. Confirm that the tunnels are in the Up state by typing the **tunnels** command.

```
SEE_A>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa
Key update interval : 60 minutes

CI   Origin   Action   State    group info       VLAN             KEY#
---- -------- -------- -------- ---------------- ---------------- --------
0001 Auto     Secure   Up       M41a2cf_bd2d8ff6                         0
0002 Auto     Secure   Up       M41a2cf_6bb49cdf 81000003                0
0003 Auto     Secure   Up       M41a2cf_db59403e 81000002                0

SEE_B>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb
Key update interval : 60 minutes

CI   Origin   Action   State    group info       VLAN             KEY#
---- -------- -------- -------- ---------------- ---------------- --------
0001 Auto     Secure   Up       s41a2cf_bd2d8ff6                         0
0002 Auto     Secure   Up       s41a2cf_6bb49cdf 81000003                0
0003 Auto     Secure   Up       s41a2cf_db59403e 81000002                0
```

```
SEE_C>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:cc:cc:cc
Front Panel Management MAC address : 00:d0:1f:00:cc:cc
Key update interval : 60 minutes

CI   Origin   Action   State    group info       VLAN             KEY#
---- -------- -------- -------- ---------------- ---------------- --------
0001 Auto     Secure   Up       s41a2cf_bd2d8ff6                         0
0002 Auto     Secure   Up       s41a2cf_6bb49cdf 81000003                0
0003 Auto     Secure   Up       s41a2cf_db59403e 81000002                0
```

6. Disable automatic connection discovery to lock down the configuration by typing the **autodisco -d** command.

```
SEE_A>autodisco -d

SEE_B>autodisco -d

SEE_C>autodisco -d
```

Configuring Multipoint VLAN Mode Manually

The example below shows how to configure secure traffic in multipoint VLAN mode manually. See Modes for a network configuration and detailed information on multipoint VLAN mode.

1. Set the connection mode to VLAN mode by typing the **con -v** command.

```
SEE_A>con -v

SEE_B>con -v

SEE_C>con -v
```

2. Reset the encryptor's configuration to the default state by typing the **initcfg -a** command. This command will cause the encryptor to restart.

```
SEE_A>initcfg -a

SEE_B>initcfg -a

SEE_C>initcfg -a
```

3. Disable automatic connection discovery by typing the **autodisco -d** command.

```
SEE_A>autodisco -d

SEE_B>autodisco -d

SEE_C>autodisco -d
```

4. Set the unit to encrypt data by typing the **global -e** command.

```
SEE_A>global -e

SEE_B>global -e

SEE_C>global -e
```

5. Add the tunnels by typing the **tunnels -a** command.

```
SEE_A>tunnels -a sec 81000003

SEE_A>tunnels -a sec 81000002

SEE_B>tunnels -a sec 81000003

SEE_B>tunnels -a sec 81000002

SEE_C>tunnels -a sec 81000003

SEE_C>tunnels -a sec 81000002
```

6. Confirm that the tunnels are in the Up state by typing the **tunnels** command . (This command is optional.)

```
SEE_A>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa
Key update interval : 60 minutes

CI   Origin   Action   State    group info       VLAN             KEY#
---- -------- -------- -------- ---------------- ---------------- --------
0001 Auto     Secure   Up       M41a2cf_bd2d8ff6                         0
0002 Auto     Secure   Up       M41a2cf_6bb49cdf 81000003                0
0003 Auto     Secure   Up       M41a2cf_db59403e 81000002                0

SEE_B>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb
Key update interval : 60 minutes

CI   Origin   Action   State    group info       VLAN             KEY#
---- -------- -------- -------- ---------------- ---------------- --------
0001 Auto     Secure   Up       s41a2cf_bd2d8ff6                         0
0002 Auto     Secure   Up       s41a2cf_6bb49cdf 81000003                0
0003 Auto     Secure   Up       s41a2cf_db59403e 81000002                0

SEE_C>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:cc:cc:cc
Front Panel Management MAC address : 00:d0:1f:00:cc:cc
Key update interval : 60 minutes

CI   Origin   Action   State    group info       VLAN             KEY#
---- -------- -------- -------- ---------------- ---------------- --------
0001 Auto     Secure   Up       s41a2cf_bd2d8ff6                         0
0002 Auto     Secure   Up       s41a2cf_6bb49cdf 81000003                0
0003 Auto     Secure   Up       s41a2cf_db59403e 81000002                0
```

Configuring STP Monitoring

The example below details the steps to configure the device for STP monitoring.

1. Enable auto-discovery.

```
SEE>autodisco -e

Automatic Unicast discovery enabled

Automatic Multicast/VLAN discovery enabled
```

2. Set the Ethertype Table policy for 0x05ff multicast addressed frames to bypass *and/or* set the policy to ‘Reserved Multicast bypass enabled’.

```
SEE>ethertypes -e

Enter Ethertype [(O)ther, Value (Hex)]: 05ff
Type exists
Offset Enable: <(Y)es | (N)o>: [No]
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Follow CI]
Multicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Bypass]
Broadcast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Bypass]
Updated existing ethertype
```

and/or

```
SEE>policy -b –e

Reserved Multicast bypass enabled
```

3. Enable STP monitoring.

```
SEE>policy -s -e

STP monitoring enabled
```

STP monitoring only applies when the switch devices connected to the SEE device local and network ports are configured for per VLAN spanning tree (PVST).

This page intentionally left blank.

Command Reference

Format Conventions

Command references use the following format conventions.

- **Bold** type indicates keywords the user must enter.
- Variables are in *italicized* type and are enclosed in angle brackets < >. For example, <*ipAddress*> indicates that the user enters the specific IP address.
- An argument shown in brackets [ ] indicates that the argument is optional.
- Arguments shown in braces { } indicate that one, and only one, of the arguments is required.
- Arguments separated by the vertical bar | indicate that one of the arguments must be used.

Command Usage Guidelines

Command usage guidelines are listed below:

- The full command name must be entered.
- Commands must be entered in lowercase, for example the command 'alarm.' Entering a command with any combination of lowercase and uppercase letters will produce an 'Undefined command' error message.
- Keystrokes are stored in a typeahead buffer until displayed in the CLI.
- Keystrokes can be deleted using either the BACKSPACE key or the DELETE key.
- Context-sensitive help is available using the '-h' argument after the command. For example, entering 'users -h' displays all arguments, including a description for each argument, that are available for use with the **help** command.
- The console displays the default value or current setting for each field in brackets and allows the user to type in a new value if desired. Pressing ENTER accepts the default or current setting.
- For commands that display messages (alarm, audit, and event), after the first twelve messages have been displayed the user can press **ENTER** to display the next record, press the **SPACEBAR** to display twelve more records, press **C** to display all the remaining records continuously, or press **Q** to quit the alarm display and return to the command prompt.

Alarm Command

Syntax	Use to	Users
alarm	display all active alarms.	Administrator Operator
alarm -a <x> <y>...	acknowledge specified alarms.	Administrator
alarm -a *	acknowledge all alarms.	Administrator
alarm -n	print the number of alarms in the alarm table.	Administrator Operator
alarm -h	display the help message.	Administrator Operator

This command displays the alarm table and acknowledges a single fault or multiple specified faults. The following information is displayed when the **alarm** command is entered:

- Alarm count - number of total alarms
- Unacknowledged count - number of unacknowledged alarms
- Sequence number - alarms are listed numerically by the alarm id
- Id - number corresponding to the alarm recorded; see Traps for a list of alarm messages
- Date and time the alarm was recorded in YYYY-MM-DD HH:MM:SS format
- Status of the alarm - active or inactive; not acknowledged (NAK) or acknowledged (ACK)
- Alarm message

Alarm conditions that occur will be listed in the table with a state of ACTIVE NAK (not acknowledged) at the same time an event log message is logged and a trap will be sent out if one or more trap handlers is configured. Once an alarm is acknowledged, the alarm state becomes ACTIVE_ACK (acknowledged), and the alarm will remain in the table until the actual condition goes away.

If an alarm condition occurs and is resolved before a user has acknowledged it, then it will remain in the table in a state of INACTIVE_NAK. As soon as the alarm is acknowledged it will disappear from the alarm table as it is no longer in the active condition.

Examples

Display the Alarm Table

The example below shows the output when the **alarm** command is entered. In this example, there are 4 active alarms that have not been acknowledged.

```
SEE>alarm
Alarm count = 4   Unacknowledged count = 4
(001): id=004 2006-01-09 12:00:02 ACTIVE_NAK   Local port link down indication
(002): id=005 2006-01-09 12:00:02 ACTIVE_NAK   Network port link down indication
(003): id=010 2006-01-09 12:00:02 ACTIVE_NAK   Local interface loss of signal
(004): id=024 2006-01-09 12:00:02 ACTIVE_NAK   Network interface loss of signal
SEE>
```

Acknowledge an Alarm

The following example shows alarm 001 being acknowledged and the revised display when the **alarm** command is entered. The unacknowledged count and the alarm status are both updated.

```
SEE>alarm -a 1
Acknowledged alarm 1
SEE>alarm
Alarm count = 4   Unacknowledged count = 3
(001): id=004 2006-01-09 12:00:02 ACTIVE_ACK   Local port link down indication
(002): id=005 2006-01-09 12:00:02 ACTIVE_NAK   Network port link down indication
(003): id=010 2006-01-09 12:00:02 ACTIVE_NAK   Local interface loss of signal
(004): id=024 2006-01-09 12:00:02 ACTIVE_NAK   Network interface loss of signal
SEE>
```

Display the Number of Alarms

The **alarm -n** command displays the total number of active alarms and the number of active, unacknowledged alarms.

```
SEE>alarm -n
Alarm count = 4
Unacknowledged count = 3
SEE>
```

Audit Command

Syntax	Use to	Users
audit	display the audit log.	Administrator Operator
audit -l <*n*>	list the last *n* records in the log.	Administrator Operator
audit -s <*n*>	list records in the log starting from number *n*.	Administrator Operator
audit -n	print the number of records in the audit log.	Administrator Operator
audit -c	clear the audit log.	Administrator
audit -w {on|off}	turn wrapping on or off.	Administrator
audit -h	display the help message.	Administrator Operator

This command is used to display and clear the audit log. The following information is displayed when the **audit** command is entered:

- number of audit records currently contained in the audit log
- sequence number - entries are numbered in chronological order
- date and time the audit message was recorded in YYYY-MM-DD HH:MM:SS format
- audit message

The audit log can have wrapping mode on or off. When wrapping mode is on, a new message is added to the log replacing the previous oldest message once the log is full at 4000 messages. When wrapping mode is off, new messages are discarded once the log file is full. The default setting is on.

Examples

Display the Audit Log

The example below shows the output when the **audit** command is entered. There are 5 audit log entries.

```
SEE>audit
Number of audit records is 5
Log wrapping enabled
(001): 2010-06-21 10:22:16 User account added as follows Id: admin, Name:
administrator, Status: yes, Level: administrator, Console: yes, Snmp: yes
(002): 2010-06-21 10:20:02 admin: Keypad enabled
(003): 2010-06-21 10:15:17 admin: New certificate requested
(004): 2010-06-21 10:14:02 admin: New certificate requested
(005): 2010-06-21 10:12:42 admin: New certificate received from CA  number= 7
CA=f1:f2:f3:f4
SEE>
```

List the Last *N* Records in the Log

The following example displays the last *n* entries in the log.

```
SEE>audit -l 2
Number of audit records is 5
Log wrapping enabled
(004): 2010-06-21 10:14:02 admin: New certificate requested
(005): 2010-06-21 10:12:42 admin: New certificate received from CA  number= 7
CA=f1:f2:f3:f4
SEE>
```

List the Records in the Log Starting at Number *N*

The following example displays the records in the log beginning with number *n*.

```
SEE>audit -s 3
Number of audit records is 5
Log wrapping enabled
(003): 2010-06-21 10:15:17 admin: New certificate requested
(004): 2010-06-21 10:14:02 admin: New certificate requested
(005): 2010-06-21 10:12:42 admin: New certificate received from CA  number= 7
CA=f1:f2:f3:f4
SEE>
```

Display the Number of Entries

The following example simply displays the number of entries in the audit log.

```
SEE>audit -n
Number of audit records is 5
SEE>
```

Clear the Audit Log

This example shows the audit log being cleared of all entries. Confirmation of this action is requested.

```
SEE>audit -c
Are you sure you want to clear the log ? (y/n) y
SEE>
```

Disable Wrapping

This example shows audit log wrapping being disabled.

```
SEE>audit -w off
Disabling wrapping
SEE>
```

Autodisco Command

Syntax	Use to	Users
autodisco	display the current automatic connection discovery status.	Administrator Operator
autodisco -e [u | m]	enable the automatic connection discovery feature unicast or multicast/VLAN.	Administrator
autodisco -d [u | m]	disable the automatic connection discovery feature unicast or multicast/VLAN.	Administrator
autodisco -a <*minutes*>	remove multicast group session if there is no traffic after *n* minutes.	Administrator
autodisco -h	display the help message.	Administrator Operator

The **autodisco** command enables and disables the automatic connection discovery feature when the device is in multipoint mode. Auto-discovery allows for the automatic creation of connections from observed traffic. When enabled, Ethernet frames passing between local and remote encryptors with previously unknown MAC addresses or VLAN IDs will initiate the connection auto-discovery process.

The auto-discovery mechanism applies only for newly discovered MAC addresses or VLAN IDs when the global setting is set to encrypt all (secure). When a unicast MAC address is discovered, the encryptor will assign it to the pending connection (CI 1) while it determines whether there is a remote encryptor protecting the address.

Auto-discovery allows simple deployment of encryptors into a meshed network since the encryptors will automatically learn the topology and establish secure connections between themselves.

- Unicast automatic connection discovery is not configurable when the device is in VLAN mode.

- Auto-discovery ageing is only applicable for multicast group session in multipoint MAC mode.

- For security reasons it is recommended that once encryptors have been deployed and have learned the network topology that auto-discovery be disabled to block all unknown MAC addresses. However, auto-discovery must be enabled for STP.

Examples

Display the Automatic Discovery Status

The automatic discovery status is displayed using the **autodisco** command. The following display is for an encryptor in multipoint MAC mode.

```
SEE>autodisco

Unicast discovery: enabled
Multicast/VLAN discovery: enabled (ageing 5 mins)

SEE>
```

Disable Automatic Discovery

Use the **autodisco -d** command to disable automatic discovery.

```
SEE>autodisco -d

Automatic Unicast discovery disabled

Automatic Multicast/VLAN discovery disabled

SEE>
```

Enable Automatic Discovery

Use the **autodisco -e u** command to enable automatic unicast discovery.

```
SEE>autodisco -e u
Automatic Unicast discovery enabled
SEE>
```

Use the **autodisco -e m** command to enable automatic multicast/VLAN discovery.

```
SEE>autodisco -e m
Automatic Multicast/VLAN session discovery enabled
SEE>
```

In order to secure multicast traffic in multipoint MAC Mode, update ethertype 0x0800 and set multicast to follow CI. See Ethertypes Command for additional details.

Multicast Session Ageing

Use the **autodisco -a <***minutes***>** command to remove a session after *n* minutes of no traffic. A session is removed after 5 minutes of no traffic in the following example.

```
SEE>autodisco -a 5
ageing set to 5 mins
SEE>
```

Multicast ageing can only age out a multicast group connection if multicast ageing is enabled on all encryptors in the multipoint mesh. Whichever encryptor has the highest ageing value, that ageing value will be used as the timeout value for the multicast group connection.

Certificate Command

Syntax	Use to	Users
certificate	display the certificate list.	Administrator Operator
certificate -s <*index*>	display the details for the selected certificate.	Administrator
certificate -h	display the help message.	Administrator Operator

This command shows whether or not a valid certificate(s) has been loaded into the unit. If the certificate is valid, it also shows the details of the Certifying Authority and the dates between which the certificate is valid. The following information is displayed when the **certificate -s <***index***>** command is entered:

- Version - identifies the certificate format for this certificate
- Serial number - number used to distinguish this certificate from other certificates issued by the CA
- Digest algorithm - algorithm employed during authentication
- Signature algorithm - algorithm used by the CA to sign the certificate
- CA name - name of the certifying authority that signed the certificate
- My name - name assigned to the device by the CA
- Not before - beginning of certificate validity period
- Not after - end of certificate validity period

Examples

Display the Certificate List

The following example shows the **certificate** command display.

```
SEE>certificate

Index   Type     Name               Subj Key         CA Key         Valid
1       v1                          RSA(1024)        RSA(1024)      3645 Days
2       v2                          RSA(2048)        RSA(4096)      3643 Days

SEE>
```

Display the Certificate Details

Type the **certificate -s <*index*>** command to display the details for the selected certificate.

```
SEE>certificate -s 1
Version: 1
SerialNumber: 3
Digest algorithm: SHA
Signature algorithm: SHA
CA Name: United States:Safenet:Support
My Name: United States:Safenet:Sales:
Not Before: Thu Jun 4 16:42:53 2009
Not After: Tue Jun 4 16:42:53 2019
SEE>
```

Con Command

Syntax	Use to	Users
con	display the connection mode status.	Administrator Operator
con -m	enable MAC connection mode.	Administrator
con -v	enable VLAN connection mode.	Administrator
con -h	display the help message.	Administrator Operator

This command is used to display the connection mode status and to change the connection mode to MAC or VLAN.

When in multipoint mode (line mode is disabled), the Connection mode (as selected by the **con** command) can be selected to use either the MAC Address or VLAN ID to determine policy. This is indicated by the tunnel column heading 'Remote MAC' or 'VLAN', respectively. See Tunnels Command for additional information. If the ethertype policy specifies 'UseCI', then the inbound frame will be bound to an entry in the Connection Identifier table based on the Remote MAC or VLAN of the frame. The Remote MAC or VLAN tunnel entry associated with the inbound frame is defined as:

- the destination MAC Address or VLAN ID for frames received on the *local* port, and
- the source MAC Address or VLAN ID for frames received on the *network* port.

Examples

Display the Connection Mode Status

The following example shows the **con** command displaying the current connection mode status.

```
SEE>con

Connection mode: MAC

SEE>
```

Change the Connection Mode to VLAN

Type the **con -v** command to change the connection mode to VLAN.

```
SEE>con -v

Warning this command will reset all tunnel/CI, MAC
data to their factory defaults and reboot the unit!
do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y

Connection mode change to: VLAN Connection mode

Resetting config and rebooting . . .
```

Crypto Command

Syntax	Use to	Users
crypto	display the global cryptographic mode settings.	Administrator Operator
crypto -s	set the global cryptographic mode configuration.	Administrator
crypto -h	display the help message.	Administrator Operator

This command shows the global cryptographic mode settings. The settings are as follows:

- algorithm - AES.
- mode - counter mode or cipher feedback (CFB) for the 100 and 1000 Mbps units; the default setting is CFB to aid backward compatibility. The 10 Gbps units are set to counter mode and are not configurable.
- key length - 256 bit.

The global operation mode must be set to discard or bypass in order to set the cryptographic mode. See Global Command for more information on setting this parameter.

The crypto mode cannot be changed from counter mode to CFB when multicast policies are in effect. To change the crypto mode if multicast policies are in effect, complete the following:

- disable multicast discovery
- change the global operation mode from FollowCI to bypass or discard
- remove all multicast sessions

In order for a 1 Gbps device to interoperate with a 10 Gbps device, the mode must be set to counter mode. A 1Gbps device shall interoperate with a 10Gbps device in multipoint mode as long as the 1Gbps device is in counter mode and both devices have line mode disabled and connection mode set to either MAC Address (MAC mode) or VLAN ID (VLAN mode). If the 1Gbps device's cryptographic mode is set to CFB and connected to a 10Gbps device, the tunnels may be 'up' (if the session establishment and exchange of keys was successful). However, the decryption of data shall fail as the peer encrypted using a different mode.

When the cryptographic mode is changed, all tunnels are stopped and then restarted automatically.

Examples

Display the Cryptographic Mode Settings

The following shows the **crypto** command display.

```
SEE>crypto

Global Crypto Mode:
        Algorithm = AES
        Mode = CFB
        Key Length = 256

SEE>
```

Configure the Cryptographic Mode

Type the **crypto -s** command to change the cryptographic mode.

```
SEE>crypto -s
Global Crypto Mode Configuration options:
-->(1)  Algorithm = AES
        Mode = CFB
        Key Length = 256
   (2)  Algorithm = AES
        Mode = Counter
        Key Length = 256

Enter new Global Crypto Mode >: [1] 2

Warning this command will restart all tunnels!
Do you wish to proceed? (y/n) y

Are you sure? (y/n) y

Global Crypto Mode set to:
        Algorithm = AES
        Mode = Counter
        Key Length = 256

SEE>
```

Date Command

Syntax	Use to	Users
date	view the SEE's date and time.	Administrator Operator
date YYYY-MM-DD HH:MM:SS	set a new date and time on the encryptor.	Administrator
date -h	display the help message.	Administrator Operator

The **date** command sets the SEE's time-of-day clock. Alarm, audit, and event messages are timestamped using the value configured with the **date** command.

The values for these settings must fall in the following ranges: YYYY is 2000-2038, MM is 1-12, DD is 1-31, HH is 0-23, MM is 0-59, and SS is 0-59.

The **date** command displays the following information:

- date the SEE is set to in YYYY-MM-DD format
- time the SEE is set to in HH:MM:SS format
- the amount of time since the last power on

If only the date is entered, the time will default to the time currently set on the device.

The encryptor does not support time zones. All peer encryptors (with secure connections between them) must be set to a common reference time so the secure session establishment process can successfully authenticate each others credentials, including certificate validity period.

It is very important to set the time in a factory default unit. Failing to do so will cause the encryptor to believe it has been tampered. This will result in all certificate, user, and connection information being erased when the unit restarts.

Examples

Display the Current Date and Time

This is an example of the display when the **date** command is entered.

```
SEE>date
2006-01-09 16:43:46 up 0 days 02:34
SEE>
```

Set a New Date and Time

The following example sets the date and time to January 9, 2006; 2:55:40 p.m.

```
SEE>date 2006-01-09 14:55:40
Setting to Mon Jan 09 14:55:40 2006
SEE>
```

Eping Command

Syntax	**Use to**	**Users**
eping	display the help message.	Administrator Operator
eping -m <*MAC address*>	ping the specified MAC address.	Administrator Operator
eping -b	broadcast destination.	Administrator
eping -l <*size*>	send the specified buffer size.	Administrator
eping -c <*count*>	repeat specified number of times.	Administrator
eping -v <*VLAN*>	send a VLAN tagged frame.	Administrator
eping -d <*VLAN*>	send a VLAN double tagged frame.	Administrator
eping -h	display the help message.	Administrator Operator

The **eping** command provides the ability to ping a specified encryptor using the MAC address. Other options include broadcasting the destination, sending the specified buffer size, etc.

Examples

Ping the Specified MAC Address

The following example displays pinging an encryptor using the **eping -m <***MAC address***>** command.

```
SEE>eping -m 00:20:e2:12:34:58

64 bytes from 00:20:e2:12:34:58 time=27 ms

SEE>
```

Ping the Specified MAC Address and Send the Buffer Size

The following example displays pinging an encryptor and sending a buffer size of 200 using the **eping -m <***MAC address***> -l <***size***>** command.

```
SEE>eping -m 00:20:e2:12:34:58 -l 200

200 bytes from 00:20:e2:12:34:58 time=17 ms

SEE>
```

Ping the Specified MAC Address and Send the Buffer Size for a Specified Number of Times

The following example displays pinging an encryptor and sending a buffer size of 200 two times using the **eping -m <***MAC address***> -l <***size***> -c <***count***>** command.

```
SEE>eping -m 00:20:e2:12:34:58 -l 200 -c 2

200 bytes from 00:20:e2:12:34:58 time=16 ms


200 bytes from 00:20:e2:12:34:58 time=20 ms

SEE>
```

Ping the Specified MAC Address and Send the Buffer Size for a Specified Number of Times With a VLAN Tag

The following example displays pinging an encryptor and sending a buffer size of 200 two times with a VLAN tag using the **eping -m <***MAC address***> -l <***size***> -c <***count***> -v <***VLAN***>** command.

```
SEE>eping -m 00:20:e2:12:34:58 -l 200 -c 2 -v 81000002

200 bytes from 00:20:e2:12:34:58 time=40 ms


200 bytes from 00:20:e2:12:34:58 time=48 ms

SEE>
```

Broadcast Destination

The following example displays the **eping -b** command.

```
SEE>eping -b

64 bytes from 00:0d:b9:17:23:7e time=1 ms
64 bytes from 00:0d:b9:16:5c:1e time=29 ms
64 bytes from 00:0d:b9:16:5b:ca time=30 ms
64 bytes from 00:20:e2:30:16:3a time=52 ms
64 bytes from 00:20:e2:30:14:bb time=53 ms
64 bytes from 00:20:e2:12:34:58 time=53 ms
64 bytes from 00:20:e2:30:05:9f time=53 ms
64 bytes from 00:02:b6:41:a2:cf time=32 ms

SEE>
```

Erase Command

Syntax	Use to	Users
erase	erase the current configuration and revert to the factory defaults.	Administrator
erase -h	display the help message.	Administrator Operator

The unit's administrator account name, password, the date and time, and the USB port setting are returned to the factory default parameters and the unit is rebooted. The IP address is maintained so management connectivity is not lost.

If the SEE’s configuration is erased, see Configuration in the Possible Problems and Solutions topic for information on reconfiguring the SEE.

All users and connections will be deleted and the unit's certificate will be destroyed. The unit will need to be certified and configured again.

Example

Erase the SEE

This example shows the **erase** command being entered. Confirmation of this action is required.

```
SEE>erase
Warning this command will erase the configuration to factory defaults
do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y
Erasing unit and rebooting . . .
```

Ethertypes Command

Syntax	Use to	Users
ethertypes	display all records in the Ethertype table.	Administrator Operator
ethertypes -a	add records to the Ethertype table.	Administrator
ethertypes -d <*ethertype*>	delete a specified ethertype from the Ethertype table.	Administrator
ethertypes -d *	delete all ethertypes except 'Other' from the Ethertype table.	Administrator
ethertypes -e	edit records in the Ethertype table.	Administrator
ethertypes -r	reset the diagnostic counts. This command is available only on the 100 and 1000 Mbps units.	Administrator
ethertypes -c	turn the diagnostic counts on and off. This command is available only on the 100 and 1000 Mbps units.	Administrator
ethertypes -l	list the diagnostic counts. This command is available only on the 100 and 1000 Mbps units.	Administrator
ethertypes -h	display a list of commonly used ethertype names and their associated hexadecimal value.	Administrator Operator

The **ethertypes** command displays the Ethertype table and allows entries to be added, edited, and deleted. The Ethertype table holds a total of 16 entries, which includes 14 user definable types as well as 'length encoded' (05ff) and 'other' types. The default values are listed below:

- length encoded (05ff)
- IPv4 (0800)
- ARP (0806)
- IPv6 (86dd)
- Mac control (8808)
- 8809
- 88cc
- Loopback (9000)
- other

Ethertype mutation is the ability to select a specific ethertype in a frame and replace it with a custom ethertype to disguise the packet's protocol type. On the ingress encryptor (encrypting encryptor) the ethertype is mutated to a user specified value. On the egress encryptor (decrypting encryptor) the mutation process is reversed. Ethertype mutation prevents interoperability issues with devices that perform L3+ snooping. Ethertype mutation also provides disguising of the users network protocols.

When the entry's Unicast, Multicast, or Broadcast field is set to 'Follow CI' the system refers to the Connection Identifier table to determine the processing action. In the CLI, all ethertypes are referred to by the hex value except for 'other' which is referenced by 'o' or 'other'.

In order to secure multicast traffic in multipoint MAC Mode, update ethertype 0x0800 and set multicast to follow CI.

Ethertype field descriptions are listed below:

- Ethertype - hexadecimal value
- Offset Enable - when set, observe Offset Bytes
- Encryption Offset - number of bytes in frame left in clear from ethertype field
- Mutate Enable - set the ability to replace a specific ethertype with a custom ethertype
- Mutated Ethertype - hexadecimal value for the custom ethertype
- Unicast action - follow the Connection Identifier table, discard, or bypass
- Multicast action - discard or bypass
- Broadcast action - discard or bypass
- Injected NonMutant - discard or bypass

Examples

Display the Ethertype Table

An example of the **ethertypes** command, when the device is in multipoint MAC mode, is listed below. All entries in the Ethertype table are displayed. See Factory Default Parameters for the default settings for all connection modes.

```
SEE>ethertypes

                     Offset Encryption Mutate Mutated                                 Injected
Ethertype (Name)     Enable Offset     Enable Ethertype Unicast   Multicast Broadcast NonMutant
------------------   ------ ---------- ------ --------- --------- --------- --------- ---------
0x05ff (Length)      N      0x0        NA     NA        UseCI     Bypass    Bypass    NA
0x0800 (IPv4)        N      0x14       Y      0xf800    UseCI     Discard   Bypass    Discard
0x0806 (ARP)         N      0x0        N      0xf806    Bypass    Discard   Bypass    Bypass
0x86dd (IPv6)        N      0x28       Y      0xf6dd    UseCI     Discard   Bypass    Discard
0x8808 (MAC-C)       N      0x0        N      0xf808    Bypass    Bypass    Bypass    Bypass
0x8809 (SPMA)        N      0x0        N      0xf809    Bypass    Bypass    Bypass    Bypass
0x88cc (LLDP)        N      0x0        N      0xf8cc    Bypass    Bypass    Bypass    Bypass
0x9000 (Loopback)    N      0x0        N      0xf000    Bypass    Bypass    Bypass    Bypass
Other                N      0x0        NA     NA        UseCI     Discard   Discard   NA

9 Records in Ethertype table
Diagnostic counts disabled.

SEE>
```

Add an Entry

An entry is added to the Ethertype table using the **ethertypes -a** command. If the entry already exists, an error message displays and the command aborts.

```
SEE>ethertypes -a

Enter Ethertype [(O)ther, Value (Hex)]: 801
Offset Enable: <(Y)es | (N)o>: [No]
Mutation Enable: <(Y)es | (N)o>: [No]
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Follow CI]
Multicast Action: <(D)iscard | (B)ypass>: [Discard]
Broadcast Action: <(D)iscard | (B)ypass>: [Discard]
Added new Ethertype
SEE>
```

Edit an Entry

An entry is edited in the Ethertype table using the **ethertypes -e** command. The user is prompted for a hex ethertype value to be edited. To select the 'other' entry, enter 'o' or 'other'. If the entry exists, prompts are displayed with the current values for the fields.

If a user tries to edit a nonexistent hex value, an error message displays and the command aborts.

```
SEE>ethertypes -e

Enter Ethertype [(O)ther, Value (Hex)]: 801
Type exists
Offset Enable: <(Y)es | (N)o>: [No]
Mutation Enable: <(Y)es | (N)o>: [No]
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Follow CI] B
Multicast Action: <(D)iscard | (B)ypass>: [Discard]
Broadcast Action: <(D)iscard | (B)ypass>: [Discard]
Updated existing ethertype
SEE>
```

Delete an Entry

An entry is deleted using the **ethertypes -d <*ethertypevalue*>** command. If the hex ethertype value exists, a prompt displays requesting confirmation to delete the entry. The ethertype value 'Other' cannot be deleted. The wild card '*' deletes all table entries except for 'Other.'

If a user tries to delete a nonexistent hex ethertype value, an error message displays and the command aborts.

```
SEE>ethertypes -d 801
Type exists
Are you sure you want to delete ethertype 0x0801 ? (y/n) y
Deleted Ethertype 0x0801
done
SEE>
```

Enable the Diagnostic Count

The **ethertypes -c** command toggles the action between enabling and disabling the diagnostic count. The diagnostic count is disabled by default. To enable the count, enter the command **ethertypes -c**.

The diagnostic count setting is not persistent across a restart. As such, enabling the count will be reset back to disabled after restarting the device.

```
SEE>ethertypes -c

Ethertype diagnostic count is enabled
SEE>
```

List the Diagnostic Count

The **ethertypes -l** command lists the ethertype(s) and the count.

```
SEE>ethertypes -l

Port    Ethertype  Count
------  ---------  -----
Remote  0x0800     22
Remote  0x0806     1418
Remote  0x88cc     14
Remote  0xf800     6220
Remote  0xfc0f     3207
Local   0x0800     15159
Local   0x0806     313
SEE>
```

Reset the Diagnostic Count

The **ethertypes -r** command is used to reset the diagnostic count to zero.

```
SEE>ethertypes -r

Ethertype diagnostic counts reset!
SEE>
```

Event Command

Syntax	Use to	Users
event	display the event log.	Administrator Operator
event -l <*n*>	list the last *n* records in the log.	Administrator Operator
event -s <*n*>	list records in the log starting from number *n*.	Administrator Operator
event -n	print the number of records in the event log.	Administrator Operator
event -c	clear the event log.	Administrator
event -w {on | off}	turn wrapping on or off.	Administrator
event -h	display the help message.	Administrator Operator

This command is used to display and clear the event log. The following information is displayed when the **event** command is entered:

- number of records currently contained in event log
- sequence number - entries are numbered in chronological order
- date and time the event was recorded in YYYY-MM-DD HH:MM:SS format
- event message

The **event** command functions the same as the **audit** command. See Audit Command for information and examples.

FIPS Command

Syntax	Use to	Users
fips	display the current FIPS operation mode.	Administrator Operator
fips on	enable FIPS mode.	Administrator
fips off	disable FIPS mode.	Administrator
fips -h	display the help message.	Administrator Operator

FIPS mode is turned on by default. FIPS mode must be turned off before changing any setting that is not approved under the FIPS140-2 certification.

FIPS mode can be turned on only if all non-FIPS approved modes are disabled.

Examples

Display the FIPS Status

The following example shows the status of the FIPS mode.

```
SEE>fips
FIPS mode enabled
SEE>
```

Disable FIPS Mode

FIPS mode is turned off in the following example.

```
SEE>fips off
Turning FIPS mode off means that this encryptor
is NOT running in a FIPS140-2 certified mode !!

Do you wish to proceed ? (y/n) y
Warning: Turning FIPS mode off will erase the configuration and reboot this
encryptor
Do you wish to proceed ? (y/n) y


Are you sure ? (y/n) y
Disable FIPS mode selected. Validation...succeeded.
FIPS mode Disabled
This encryptor is NO longer running in a FIPS140-2 certified mode!
SEE>
```

Enable FIPS Mode

FIPS mode is dependent on the **snmpcfg** command setting. As shown in the following example, a message is displayed if SNMP privacy is not turned on.

```
SEE>fips on
Warning: Turning FIPS mode on will erase the configuration and reboot this
encryptor
Do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y
Enable FIPS mode selected. Validation...failed.

FIPS Mode cannot currently be enabled. Please make the following change to the
configuration:

        SNMP Privacy must be ON - run snmpcfg command.

SEE>
```

In the following example, FIPS mode is enabled.

```
SEE>fips on
Warning: Turning FIPS mode on will erase the configuration and reboot this
encryptor
Do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y
Enable FIPS mode selected. Validation...succeeded.
FIPS Mode Enabled


SEE>
```

Framegap Command

Syntax	Use to	Users
framegap	display the current interframe gap status.	Administrator Operator
framegap -r	set the interframe gap to repeater (88 bit times).	Administrator
framegap -s	set the interframe gap to standard (96 bit times).	Administrator
framegap -h	display the help message.	Administrator Operator

The InterFrame Gap (IFG) is the recovery time between Ethernet frames that allows a device time to prepare for the next frame. This command is used to configure the minimum IFG. The options are the standard IEEE 802.3 - 96 bit IFG and the repeater shaved 88 bit IFG. The default value is the repeater (88 bit times).

The smaller IFG may lead to more collisions in some networks. If that is the case, change the IFG from repeater (88) to standard (96).

Examples

Display the Interframe Gap Status

The **framegap** command is used to display the current interframe gap status.

```
SEE>framegap

Interframe gap status: repeater (88 bit times)

SEE>
```

Set the Interframe Gap to Standard

The interframe gap is set to standard using the **framegap -s** command.

```
SEE>framegap -s

Interframe gap set to standard (96 bit times)

SEE>
```

Set the Interframe Gap to Repeater

The interframe gap is set to repeater using the **framegap -r** command.

```
SEE>framegap -r

Interframe gap set to repeater (88 bit times)

SEE>
```

Global Command

Syntax	Use to	Users
global	display the global mode state.	Administrator Operator
global -b	set the global mode state to bypass.	Administrator
global -d	set the global mode state to discard.	Administrator
global -e	set the global mode state to encrypt.	Administrator
global -h	display the help message.	Administrator Operator

The **global** command is used to set the top level Ethernet processing policy for received Ethernet frames in both line and multipoint mode.

*When the global operation mode is changed from encrypt to either bypass or discard, the multicast group and VLAN group connections are stopped (depending on the connection mode of the device). Setting the global operation mode back to encrypt does not restart the group connections. In this case, the stopped connections can be restarted with the **tunnels -r** command.*

Examples

Display the Global Mode State

The **global** command displays the current global mode status.

```
SEE>global

Global mode: discard

SEE>
```

Set the Global Mode to Bypass

The **global -b** command is used to set the global mode state to bypass.

```
SEE>global -b

Global mode set to bypass

SEE>
```

Set the Global Mode to Discard

The **global -d** command is used to set the global mode state to discard.

```
SEE>global -d

Global mode set to discard

SEE>
```

Set the Global Mode to Encrypt

The **global -e** command is used to set the global mode state to encrypt.

```
SEE>global -e

Global mode set to encrypt

SEE>
```

Help Command

Syntax	Use to	Users
help	display information on all available console commands.	Administrator Operator
help -h	display the help message.	Administrator Operator

The **help** command lists all console commands with a description of each.

Example

Display the Console Commands List

The following example shows the output when the **help** command is entered.

```
SEE>help
alarm             - View, clear & acknowledge alarms
audit             - View/Clear the audit log
autodisco         - Enable/Disable Automatic session discovery
certificate       - View the current certificate details
con               - View/Modify Connection Mode
crypto            - View/Modify the global Crypto Mode
date              - View/Modify date and time
eping             - Encryptor ping for Ethernet Encryptors
erase             - Erase unit
ethertypes        - View/Modify ethertypes
event             - View/Clear the event log
fips              - View/Modify FIPS operation mode
framegap          - View/Modify interframe gap parameter
global            - View/Modify global mode
help              - List all available commands
history           - Print command history
inband_vlan       - View/Modify VLAN table for inband management
initcfg           - Set configuration to default
ip                - View/Modify IP management settings
line              - Enable/Disable Line mode
linkspeed         - View/Modify link settings
locmacs           - View/Modify local mac addresses
logout            - Logout from console
mpls              - View/Modify MPLS specific parameters
netmacs           - View/Modify network mac addresses
password          - View/Modify user password policy
policy            - View/Modify miscellaneous policy settings
prompt            - Change the console prompt
reboot            - Reboot the unit
sfp               - View SFP information
shim              - View/Modify Counter Mode SHIM parameters
snap              - View/Modify SNAP protocol specific handling
snmpcfg           - View/Modify SNMP Privacy mode
stats             - View Port Statistics
tunnels           - View/Modify tunnels
usb               - Lock or unlock USB port
users             - View/Modify system users
version           - Display version information
vlan              - View/Modify VLAN specific parameters

Try 'command -h' for more detailed help

SEE>
```

*Only the **sfp** command or the **xfp** command will be listed on the **help** command display. The **sfp** command will be listed for 1 Gbps units. The **xfp** command will be listed for 10 Gbps encryptors.*

History Command

Syntax	Use to	Users
history	display a list of the last 25 console commands entered.	Administrator Operator
history -h	display the help message.	Administrator Operator

This list contains up to a maximum of 25 console commands entered in the current user session. Command history is cleared when logged off.

The up and down arrow keys can be used to scroll through previously entered commands in the list.

Example

Display the History

The following example shows the output when the **history** command is entered.

```
SEE>history

01: date 2006-01-09 14:55:40
02: alarm
03: audit
04: certificate
05: tunnels
SEE>
```

Inband_vlan Command

Syntax	Use to	Users
inband_vlan	list all the inband VLAN tags.	Administrator Operator
inband_vlan -a <*tag*> <*tag*>	add an inband VLAN tag. The variable 'tag' is a combination of the ethertype and VLAN ID. For example, 8100 and 0002, where 8100 is a well known ethertype for VLAN and 0002 is the VLAN ID. (multipoint VLAN mode only) For example: **inband_vlan -a** adds an untagged tag. **inband_vlan -a 8100 0FFF** adds a single tag. **inband_vlan -a 9100 FFF 8100 123** adds a double tag. **inband_vlan -a 91000FFF81000123** adds a double tag.	Administrator
inband_vlan -e <*index*> <*tag*> <*tag*>	edit an inband VLAN tag using the index number.	Administrator
inband_vlan -d <*index*> <*index*> ...	delete a specified inband VLAN tag(s) using the index number.	Administrator
inband_vlan -h	display the help message.	Administrator Operator

The core network between encryptor devices may have implemented 802.1Q VLAN tagging. As a result, the inband management frames may not traverse the core network and reach the peer encryptor due to the lack of a VLAN tag.

The **inband_vlan** command is used to create a table that associates remote encryptors with VLAN headers for peer detection and communications. Once the encryptor determines which peer encryptor to associate with a specified VLAN header, the inband management traffic will be tagged with the specified VLAN header between encryptors. This tag will be added to all inband management frames that are sent from the encryptor.

See the Inband Management topic for general information on inband management, encryptor settings, and router settings.

Examples

Display the Inband VLAN Table

The **inband_vlan** command is used to display the inband VLAN table.

```
SEE>inband_vlan

index : tag(s)
--------------------------------------
    1 : (untagged)
    2 : 8100 0005
    3 : 8100 0006
--------------------------------------

SEE>
```

Add an Inband VLAN Tag

The **inband_vlan -a <*tag*>** command adds a single tag with the specified ethertype and VLAN ID.

```
SEE>inband_vlan -a 8100 0005
SEE>
```

Edit an Entry

An inband VLAN tag is edited using the **inband_vlan -e <***index***> <***tag***>** command.

```
SEE>inband_vlan -e 2 8100 0008
SEE>
```

Delete an Entry

An inband VLAN tag is deleted using the **inband_vlan -d <***index***>** command.

```
SEE>inband_vlan -d 3
deleted vlan entry 3
SEE>
```

Initcfg Command

Syntax	Use to	Users
initcfg -a	reset the connections, local MAC addresses, network MAC addresses, and global mode action to the default values.	Administrator
initcfg -c	reset the connections, local MAC addresses, and network MAC addresses to the default values.	Administrator
initcfg -g	reset the global mode action and Ethertype table to the default values.	Administrator
initcfg -1	test basic connectivity and encryption in line mode and multipoint mode.	Administrator
initcfg -2	expand on test level 1. This test includes ARP and IPv6 traffic in line mode and encryption of length encoded and other unlisted ethertypes in multipoint mode.	Administrator
initcfg -3	expand on test level 2 in line mode only. It enables encryption on length encoded packets to identify potential issues with control plan packet handling.	Administrator
initcfg -4	expand on test level 3 in line mode only with the exception that Bypass Reserved Multicast is set to disable.	Administrator
initcfg -h	display the help message.	Administrator Operator

The **initcfg** command is used to reset the connections, local MAC addresses, network MAC addresses, and global mode action to their initial configuration. It is also used for network testing in line mode and multipoint mode. The encryptor is rebooted after each of these configuration changes.

Entering just the ***initcfg*** *command displays the help message.*

Test Levels

Test level commands reset the encryptor configuration for network testing and problem resolution. They are intended to be used in sequential order beginning with test level 1. Test levels for line mode and multipoint mode are described below.

Verify that the unit is in the correct mode for testing before executing the test level commands. The ***line*** *command verifies whether line mode is enabled or disabled. Use the* ***line -e*** *or* ***line -d*** *command to enable or disable line mode as required.*

Level 1- Line Mode and Multipoint Mode

Level 1 tests for basic connectivity and encryption in both line mode and multipoint mode. At this test level, the crypto stream is stripped down to a single ethertype (IPv4), with mutation enabled, and injected nonmutant handling set to discard. Successful testing at this level verifies the following:

- Management ethertype (0xFCOF) traverses the network.
- Session establishment is working.
- IPv4 Traffic traverses networks, for example, a mutated type traverses the network.

Level 2 - Line Mode

Level 2 expands on the crypto stream by including ARP and IPv6 traffic. This level offers interim complexity into the crypto stream, without a specifically targeted goal. It can pick up issues such as packet re-ordering, but simply presents the next level of configuration complexity.

Level 2 - Multipoint Mode

Level 2 expands the basic connectivity test by encrypting length encoded and other unlisted ethertypes. If the test fails at this point, use the ethertype logging command (**ethertypes –c**, **ethertypes -r**) to detect other ethertypes seen on the network. Once detected, specific ethertype entries can be added to the ethertype table for individual handling.

Level 3 - Line Mode

Level 3 is used in line mode only. It enables encryption on length encoded packets to identify potential issues with control plan packet handling. It is recommended to run at this level for at least 20 minutes to ensure any protocol timeouts will occur.

Level 4 - Line Mode

Level 4 is used in line mode only. It is the same as level 3 with the exception that Bypass Reserved Multicast is set to disabled. If corruption/packet loss occurs at level 4 and not level 3, then suspect that reserved multicast packets are being injected into the crypto stream by network equipment.

Examples

Reset the Connections, MAC Addresses, and Global Mode

Use the **initcfg -a** command to reset the connections, local MAC addresses, network MAC addresses, Ethertype table, and global mode action to the default values. The encryptor is automatically rebooted.

```
SEE>initcfg -a

Warning this command will reset all tunnel/CI, MAC and global
data to their factory defaults and reboot the unit!
do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y

Resetting config and rebooting . . .
```

Reset the Connections and MAC Addresses

Use the **initcfg -c** command to reset the connections, local MAC addresses, and network MAC addresses to the default values. The encryptor is automatically rebooted.

```
SEE>initcfg -c

Warning this command will reset all tunnel/CI and MAC entries to
their factory defaults and reboot the unit!
do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y

Resetting config and rebooting . . .
```

Reset the Global Mode

Use the **initcfg -g** command to reset the Ethertype table and global mode action to the default values. The encryptor is automatically rebooted.

```
SEE>initcfg -g

Warning this command will reset all global configuration and ethertype
table data to the factory defaults and reboot the unit!
do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y

Resetting config and rebooting . . .
```

Change the Default Settings for Network Testing

The **initcfg -*N*** command is used to reset the encryptor configuration to execute different levels of testing. The command results are the same for all four test levels. Confirmation to run this command is required.

```
SEE>initcfg -1
Setting of Level 1 defaults is testing/commissioning purposes only.
do you wish to proceed ? (y/n) y


Are you sure ? (y/n) y


Resetting config. . .Done.
SEE>
```

IP Command

Syntax	Use to	Users
ip	display the management IP address/prefix and gateway, inband management IP address/prefix and gateway, and Ethernet management port settings.	Administrator Operator
ip -s <*index*> <*address*>/<*prefix*> <*gateway*>	configure the IP address/prefix and gateway for the specified port.	Administrator
ip -e <*index*>	enable the specified port.	Administrator
ip -d <*index*>	disable the specified port.	Administrator
ip -i {-e | -d }	enable or disable the device as an inband gateway.	Administrator
ip -v <*tag*>	set the inband VLAN tag (line mode only).	Administrator
ip -c	modify the Ethernet management port settings.	Administrator
ip -h	display the help message.	Administrator Operator

The SEE must be assigned a unique IP address before it can be configured for operation. The **ip -s** command is used to set or update the IPv4 or IPv6 management address/prefix and gateway and the IPv4 inband management address/prefix and gateway.

IPv6 is not supported for inband management.

The following settings are configurable via the **ip -s** command:

- Address/Prefix - IP address of the Ethernet port used for out-of-band SMCII management/network prefix notation for the subnet mask.
- Gateway - assigned when the SEE and the management station are on different networks; identifies the local router port on the same network as the SEE gateway's management port. The SEE sends all packets to the specified router to be forwarded to the management station.

If the SEE gateway's management port is directly connected to the management station, the host IP address and the management port IP address must be on the same network.

The following index numbers are used to distinguish the different ports in the IP address table:

- 1 - Management IP address - IPv4
- 2 - Management IP address - IPv6
- 3 - Inband management address - IPv4

IPv4 addressing uses a 4 byte value displayed in the dotted decimal notation, for example 203.21.127.32. IPv6 addressing uses the standard eight groups of four hexadecimal digits with each group separated by a colon (:), for example 2001:0db8:85a3:08d3:1319:8a2e:0370:7348. The standard IPv6 abbreviations apply.

A port cannot be enabled if the address is all zero's (0).

See the Inband Management topic for general information on inband management, encryptor settings, and router settings.

Examples

Enter the Management IP Address

Use the **ip -s** command to enter the new management IP address and settings.

```
SEE>ip -s 1 10.0.100.179/8 10.0.100.2
SEE>
```

Enable the Port

Type the **ip -e <*index*>** command to enable a port. The following example shows the management port with IPv4 addressing being enabled.

```
SEE>ip -e 1
SEE>
```

Display the IP Settings

The **ip** command displays the current settings.

```
SEE>ip

Index  Port         Status    AF   Address/Prefix
                                   Gateway
-----  ------------ --------  ---- --------------------------------------------
  1    Management   Enabled   IPv4 10.0.100.179/8
                                   10.0.100.2
  2    Management6  Disabled  IPv6 ::/0
                                    ::
  3    Inband Mgmt  Disabled  IPv4 0.0.0.0/0
                                   0.0.0.0

Inband Management Gateway Enabled: N
Inband Default VLAN tag:           N/A (line mode only)

Front Panel Ethernet Port:
    Configured: Auto Negotiation: Enabled
                Maximum Advertised Rate: 100 Mbit/s, Full Duplex.
    Current Status: Link State: Up
                    Auto Negotiation Status: Complete
                    Actual Rate: 100 Mbit/s, Full Duplex.
    Link Partner: Maximum Advertised Rate: 100 Mbit/s, Full Duplex.

SEE>
```

Modify the Ethernet Management Port Settings

Type **ip -c** to configure the front panel Ethernet port link rate. In the following example, auto-negotiation is disabled and the link rate is set to 10 Mbps half duplex.

```
SEE>ip -c
Enable Auto-Negotiation (y/n/q) n
Disable Auto-negotiation selected
Enable 100 Mbps (y/n/q)? n
10 Mbps selected
Enable Full Duplex (y/n/q)? n
Half Duplex selected
Configuring Management Port, please wait...
Auto-negotiation disabled and rate fixed to 10 Mbps Half Duplex
SEE>
```

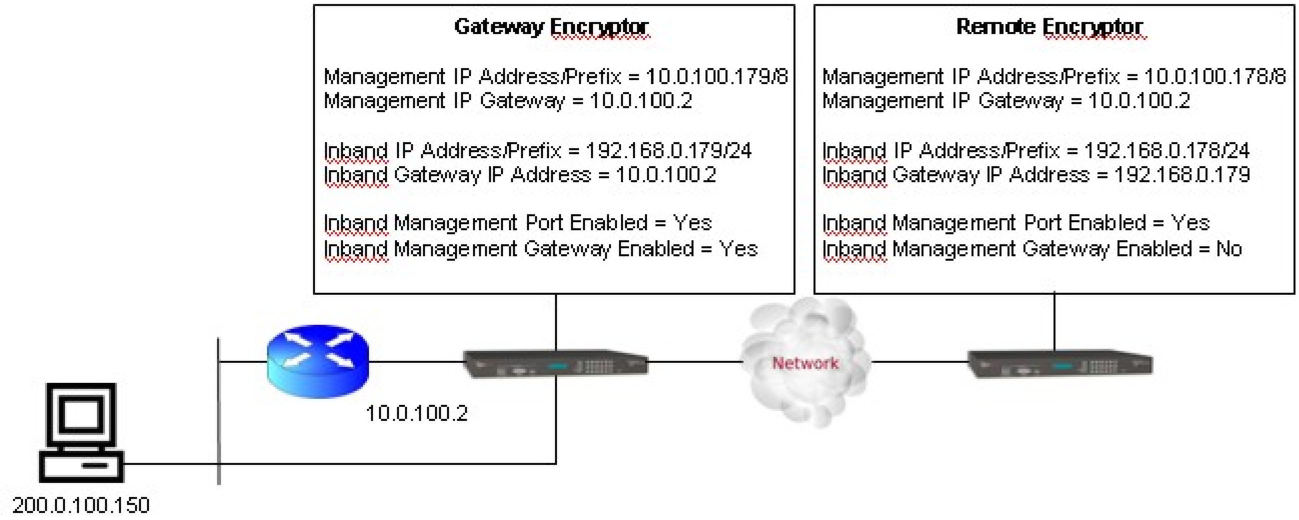
Set the Inband VLAN Tag

Type **ip -v <***tag*> to set a specified VLAN header. The inband management traffic will be tagged with the specified VLAN header between encryptors. The entered tag value will be added to all inband management frames that are sent from the encryptor. This is used for line mode only.

```
SEE>ip -v 81000024
SEE>
```

Inband Management Examples

The following diagram illustrates the network used in the examples.


Gateway Encryptor
Management IP Address/Prefix = 10.0.100.179/8
Management IP Gateway = 10.0.100.2
Inband IP Address/Prefix = 192.168.0.179/24
Inband Gateway IP Address = 10.0.100.2
Inband Management Port Enabled = Yes
Inband Management Gateway Enabled = Yes
Remote Encryptor
Management IP Address/Prefix = 10.0.100.178/8
Management IP Gateway = 10.0.100.2
Inband IP Address/Prefix = 192.168.0.178/24
Inband Gateway IP Address = 192.168.0.179
Inband Management Port Enabled = Yes
Inband Management Gateway Enabled = No
Network
10.0.100.2
200.0.100.150

Configure Inband Management on the Gateway SEE

This is an example of configuring inband management on the gateway encryptor.

1. Type the inband management IP address/prefix and gateway.
   SEE>**ip -s 3 192.168.0.179/24 10.0.100.2**
   SEE>

2. Enable the inband management port.
   SEE>**ip -e 3**
   SEE>

3. Enable the inband management gateway.
   SEE>**ip -i -e**
   SEE>

Inband management is now configured as shown in the following display.

```
SEE>ip

Index  Port         Status    AF   Address/Prefix
                                   Gateway
-----  ------------ --------  ---- --------------------------------------------
  1    Management   Enabled   IPv4 10.0.100.179/8
                                   10.0.100.2
  2    Management6  Disabled  IPv6 ::/0
                                   ::
  3    Inband Mgmt  Enabled   IPv4 192.168.0.179/24
                                   10.0.100.2

Inband Management Gateway Enabled: Y
Inband Default VLAN tag:           N/A (line mode only)

Front Panel Ethernet Port:
    Configured: Auto Negotiation: Enabled
                Maximum Advertised Rate: 100 Mbit/s, Full Duplex.
    Current Status: Link State: Up
                    Auto Negotiation Status: Complete
                    Actual Rate: 100 Mbit/s, Full Duplex.
    Link Partner: Maximum Advertised Rate: 100 Mbit/s, Full Duplex.

SEE>
```

Configure Inband Management on the Remote SEE

This is an example of configuring the remote encryptor managed via inband management.

1. Type the inband management IP address/prefix and gateway.
   SEE>**ip -s 3 192.168.0.178/24 192.168.0.179**
   SEE>

2. Enable the inband management port.
   SEE>**ip -e 3**
   SEE>

Inband management is now configured as shown in the following display.

```
SEE>ip

Index  Port         Status    AF   Address/Prefix
                                   Gateway
-----  ------------ --------  ---- --------------------------------------------
  1    Management   Enabled   IPv4 10.0.100.179/8
                                   10.0.100.2
  2    Management6  Disabled  IPv6 ::/0
                                   ::
  3    Inband Mgmt  Enabled   IPv4 192.168.0.178/24
                                   192.168.0.179

Inband Management Gateway Enabled: N
Inband Default VLAN tag:           N/A (line mode only)

Front Panel Ethernet Port:
    Configured: Auto Negotiation: Enabled
                Maximum Advertised Rate: 100 Mbit/s, Full Duplex.
    Current Status: Link State: Up
                    Auto Negotiation Status: Complete
                    Actual Rate: 100 Mbit/s, Full Duplex.
    Link Partner: Maximum Advertised Rate: 100 Mbit/s, Full Duplex.

SEE>
```

Line Command

Syntax	Use to	Users
line	display the current line mode status.	Administrator Operator
line -e	enable line mode.	Administrator
line -d	disable line mode.	Administrator
line -h	display the help message.	Administrator Operator

The line command is used to enable and disable line mode. Line mode fully encrypts all data point-to-point, between two designated SEEs. The line mode feature allows the user to configure two SEEs to run as dedicated peers for each other. Only one pair of line mode SEE devices can reside on the same circuit. If more than two SEE devices reside on the same LAN circuit, auto discovery or manual tunnel creation must be used.

Line mode is disabled by default. Line mode must be enabled on *both* SEEs for point-to-point data encryption.

Global mode must be set to encrypt data for line mode to operate correctly. The CLI commands **autodisco**, **netmacs**, and **locmacs** are not available when the device is in line mode.

All connections, local MAC addresses, and network MAC addresses will be reset to the factory defaults when line mode is enabled or disabled.

Examples

Display the Line Mode Status

The **line** command displays the line mode status.

```
SEE>line

Line mode: disabled

SEE>
```

Enable Line Mode

*Verify that data is being encrypted using the **global** command. If data is not being encrypted, use the **global -e** command to configure data for encryption before enabling line mode.*

The **line -e** command enables line mode.

```
SEE>line -e

Warning this command will reset all tunnel/CI, MAC
data to their factory defaults and reboot the unit!
do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y

Line mode enabled

Resetting config and rebooting . . .
```

Line mode cannot be enabled when the device is in VLAN mode. The following example shows the output when trying to enable line mode when VLAN mode is enabled.

```
SEE>line -e
Unknown option: e
SEE>
```

Disable Line Mode

The **line -d** command disables line mode.

```
SEE>line -d

Warning this command will reset all tunnel/CI, MAC
data to their factory defaults and reboot the unit!
do you wish to proceed ? (y/n) y

Are you sure ? (y/n) y

Line mode disabled

Resetting config and rebooting . . .
```

Linkspeed Command

Syntax	Use to	Users
linkspeed	display the current link speed setting.	Administrator Operator
linkspeed -a {-e | -d }	enable or disable auto negotiation.	Administrator
linkspeed -s	set the link speed for the device. (Electrical interfaces only)	Administrator
linkspeed -m {-e | -d}	enable/disable local link monitoring (forces unit into discard on local link loss).	Administrator
linkspeed -f	sets the optical link loss forwarding (oLLF) action.	Administrator
linkspeed -c {-e | -d }	ties the optical LLF to the connection status. (Line mode only)	Administrator
linkspeed -e	sets the electrical link loss forwarding (eLLF) action.	Administrator
linkspeed -l {-e | -d}	enable or disable tying the optical LLF to the connection status. (Line mode only)	Administrator
linkspeed -h	display the help message.	Administrator Operator

The **linkspeed** command displays and sets the maximum link speed for the encryptor. It is also used to configure automatic link loss recovery and set the link loss forwarding.

Examples

Display the Current Link Speed

The maximum link capability, current link speed setting, link status, and auto negotiation status are displayed using the **linkspeed** command.

```
SEE>linkspeed

Link parameter                             Status
-----------------------                    -------------------
Maximum link capability                      1Gb/s Full Duplex
Configured link speed (Electrical            1Gb/s Full Duplex
Current link status                          1Gb/s Full Duplex
Current link status (Network)                1Gb/s Full Duplex
Current link status (Local)                  1Gb/s Full Duplex
Local link monitoring                                 disabled

Auto Negotiation                                       enabled

Optical Link Loss Forwarding                          disabled
Optical LLF tied to connection status (line mode)      enabled

Electrical Link Loss Forwarding                        disabled
Electrical LLF tied to connection status (mesh mode)   disabled
Electrical LLF nominated connection in mesh mode        ci# n/a


SEE>
```

Enable Auto Negotiation

Use the **linkspeed -a -e** command to enable auto negotiation for the link speed.

```
SEE>linkspeed -a -e
Auto Negotiation enabled
SEE>
```

Disable Auto Negotiation

Use the **linkspeed -a -d** command to disable auto negotiation for the link speed.

```
SEE>linkspeed -a -d
Auto Negotiation disabled
SEE>
```

Set a New Link Speed Value

Changing the link speed value to a new setting is performed with the **linkspeed -s** command. Link speed options are listed with the corresponding numerical value listed in parentheses. To change the setting, type the number corresponding to the speed required. To leave the link speed setting unchanged, press **ENTER**.

The current link speed setting has an arrow on the left and is also listed in brackets beside 'New link speed.'

```
SEE>linkspeed -s
Link speed options:
10Mb/s Full Duplex (1)
100Mb/s Full Duplex (2)
->1Gb/s Full Duplex (3)
New link speed >: [3] 2
Link speed set to:   100Mb/s Full Duplex

SEE>
```

Local Link Monitoring

The **linkspeed -m -e** command enables local link monitoring. This command is used to set the unit to global discard mode in the event of link loss being detected on the local port (that is, the local port cable is unplugged). Once in global discard mode, the device will not pass traffic until an administrator has logged in and changed the global mode back to secure.

```
SEE>linkspeed -m -e
SEE>
```

Set the Optical Link Loss Forwarding Action

The example below shows the optical link loss forwarding action being set to forward link loss on both the local and network links to the opposite link.

```
SEE>linkspeed -f

Optical Link loss forwarding options:
->           disabled (1)
   propagate Net->Loc (2)
   propagate Loc->Net (3)
  propagate Loc<->Net (4)
New optical link loss forwarding setting >: [1] 4
Optical Link Loss Forwarding set to: propagate Loc<->Net

SEE>
```

Extend the Optical Link Loss Forwarding Action to the Connection Status

The **linkspeed -c -e** command extends the concept of the link loss forwarding action in line mode to the connection status.

```
SEE>linkspeed -c -e

Optical LLF tied to connection (line mode only) enabled

SEE>
```

Set the Electrical Link Loss Forwarding Action

The **linkspeed -e** command sets the electrical link loss forwarding action.

```
SEE>linkspeed -e
Electrical Link loss forwarding options:
->           disabled (1)
   propagate Net->Loc (2)
New Electrical link loss forwarding setting >: [1] 2
Electrical Link Loss Forwarding set to: propagate Net->Loc

SEE>
```

Enable Tying the Optical Link Loss Forwarding to the Connection Status

The **linkspeed -l -e** command ties the optical LLF to the connection status.

```
SEE>linkspeed -l -e

CI   Origin   Action   State    group info       VLAN             KEY#
---- -------- -------- -------- ---------------- ---------------- --------
0001 Auto     Secure   Up       M30070b_5610d932 81000002               13
0002 Auto     Secure   Up       M30070b_51295af1 81000003               13

New Electrical link loss forwarding nominated connection >: 2
Electrical LLF tied to connection status Ci 2 (mesh mode) - enabled

SEE>
```

Locmacs Command

Syntax	Use to	Users
locmacs	display all records in the local MAC address table.	Administrator Operator
locmacs -a <*MAC address*>	add a record to the local MAC address table.	Administrator
locmacs -d <*MAC address*>	delete a record from the local MAC address table.	Administrator
locmacs -d *	delete all local MAC addresses from the local MAC address table.	Administrator
locmacs -n	display the number of local MAC addresses.	Administrator Operator
locmacs -h	display the help message.	Administrator Operator

The **locmacs** command is used to manipulate MAC addresses located on the local port of the encryptor.

This command is only available when the encryptor is in multipoint MAC mode.

Examples

Display the Local MAC Addresses

The **locmacs** command displays all entries in the local MAC address table.

```
SEE>locmacs

Local Mac
-----------------
00:d0:1f:06:a3:12
00:d0:1f:06:a3:13
2 Valid records

SEE>
```

Add a Local MAC Address

The **locmacs -a <*MAC address*>** command adds an entry to the local MAC address table. If the MAC address is already entered in the local or network MAC address table, an error message displays and the command aborts.

```
SEE>locmacs -a 00:d0:1f:06:a3:14
Added new local mac address
SEE>
```

Delete a Local MAC Address

The **locmacs -d <*MAC address*>** command is used to delete a local MAC address. If an invalid or nonexistent local MAC address is entered, an error message displays and the command aborts. The wild card '*' deletes all local MAC addresses.

```
SEE>locmacs -d 00:d0:1f:06:a3:13
Are you sure you want to delete mac address ? (y/n) y
Deleted mac address
SEE>
```

Display the Number of Local MAC Addresses

The **locmacs -n** command displays the number of entries in the local MAC address table.

```
SEE>locmacs -n
3 Valid records
SEE>
```

Logout Command

Syntax	Use to	Users
logout	log the current user off the console and return to the login prompt.	Administrator Operator
logout -h	display the help message.	Administrator Operator

The **logout** command terminates the text-based interface session.

Example

Log Out of the CLI Session

The **logout** command ends the CLI session.

```
SEE>logout
LOGIN:
```

MPLS Command

Syntax	Use to	Users
mpls	display the current MPLS shim header bypass status.	Administrator Operator
mpls -p {-e | -d}	enable and disable the MPLS shim header bypass status.	Administrator
mpls -a	set an alternate MPLS ethertype value.	Administrator
mpls -h	display the help message.	Administrator Operator

The **mpls** command sets the policy for processing Ethernet frames that are tagged with labels on MultiProtocol Label Switching (MPLS) networks. MPLS uses labels to forward packets across the network (conventional network layer forwarding uses network protocol layer headers; that is, IP addresses) and is usually used for ‘class of service’ or traffic engineering purposes.

Layer 2 Ethernet networks carry MPLS labels in shim headers. The shim header is inserted between the link layer and the network layer. Ethernet uses values 0x8847 and 0x8848 to indicate the presence of a shim header. Ethertype value 0x8847 indicates that a frame is carrying an MPLS unicast packet and ethertype 0x8848 is used to indicate that a frame is carrying an MPLS multicast packet.

If the MPLS shim header bypass feature is enabled, the unicast (0x8847) MPLS shim is ignored and encryption starts after the MPLS label. The multicast shim can also be detected in the Alternate MPLS ethertype field which is by default set to 0x8848. A maximum MPLS stack depth of 2 labels is supported.

If the MPLS shim header bypass feature is disabled then the encryptor will not automatically detect the presence of MPLS shims. If a shim is present (unicast or multicast) then the encryptor will treat this as the ethertype to determine the encryption policy from the Ethertype table. If no explicit policy is listed then this ethertype will be processed according to the ‘Other’ ethertypes rule.

Examples

Display the MPLS Header Status

The **mpls** command is used to display the current MPLS shim header bypass status and alternate ethertype value.

```
SEE>mpls

MPLS parameter                                  Status
--------------                                  --------
Protocol shim(s) bypass                         enabled
Alternate MPLS ethertype                        0x8848

SEE>
```

Enable the MPLS Header

The MPLS shim header bypass status is enabled using the **mpls -p -e** command.

```
SEE>mpls -p -e

MPLS protocol bypass enabled

SEE>
```

Disable the MPLS Header

The MPLS shim header bypass status is disabled using the **mpls -p -d** command.

```
SEE>mpls -p -d

MPLS protocol bypass disabled

SEE>
```

Set an Alternate MPLS Ethertype Value

The **mpls -a** command is used to set an alternate MPLS ethertype definition.

```
SEE>mpls -a

Enter alternate MPLS ethertype [0x0600-0xFFFF]: 0x8847
SEE>
```

Netmacs Command

Syntax	Use to	Users
netmacs	display all records in the network MAC address table.	Administrator Operator
netmacs -a <*MAC address*>	add a network MAC address to the tunnel specified by the CI.	Administrator
netmacs -a <*MAC address*> -m	add a network MAC address to the tunnel specified by the remote encryptor MAC address.	Administrator
netmacs -d <*MAC address*>	delete a record from the network MAC address table.	Administrator
netmacs -d *	delete all network MAC addresses from the network MAC address table.	Administrator
netmacs -e <*MAC address*>	edit a record in the network MAC address table.	Administrator
netmacs -l <*CI*>	list network MAC addresses for the tunnel specified by the CI.	Administrator Operator
netmacs -l <*MAC address*> -m	list network MAC addresses for the tunnel specified by the remote encryptor MAC address.	Administrator Operator
netmacs -n	display the number of network MAC addresses.	Administrator Operator
netmacs -h	display the help message.	Administrator Operator

The **netmacs** command is used to manipulate records in the network MAC address table. The network MAC address table stores MAC addresses located on the network port of the encryptor and behind a remote encryptor. Each entry has a valid Connection Identifier (CI) number associating that MAC address to an entry in the CI table.

This command is only available when the encryptor is in multipoint MAC mode.

Connection identifiers are added by entering MAC addresses located on the network port of the encryptor and behind a remote encryptor. The default reference field for an entry is the CI number. The option '-m' allows the user to refer to an entry using its MAC address rather than its CI. This modifier is valid for use with the add argument.

Examples

Display the Network MAC Address Table

The **netmacs** command is used to display all entries in the network MAC address table.

```
SEE>netmacs

Network Mac       CI
----------------- ----
00:e7:1d:14:23:06 0004
00:03:34:56:aa:16 0004
00:03:34:56:aa:17 0004
00:d0:1f:06:12:33 0005
00:d0:aa:23:12:cc 0005
00:d0:1f:06:12:34 0006
00:d0:1f:06:12:35 0007
7 Valid records

SEE>
```

Add a Network MAC Address

The **netmacs -a <*MAC address*>** command is used to add a network MAC address. If the MAC address *is not* already entered in the network MAC address table, the user is prompted for the CI to associate with the address. If an invalid or nonexistent CI is entered, an error message displays and the command aborts.

If the MAC address *is* already entered in the network MAC address table, an error message displays and the command aborts.

If the MAC address *is* already entered in the local MAC address table, the user is prompted to move the MAC address to another tunnel. If the response is yes, the existing address is moved to the specified tunnel. If the response is no, the address is not moved.

```
SEE>netmacs -a 00:d0:aa:23:12:ca
Enter CI to associate mac address with : 4
Added new remote mac address
SEE>
```

Add a Network MAC Address Using the Remote Encryptor MAC Address

The **netmacs -a <*MAC address*> -m** command is used to add a network MAC address using the remote encryptor MAC address. If the MAC address *is not* already entered in the network MAC address table, the user is prompted for the remote encryptor MAC address, as a reference to the CI, to associate with the network MAC address. If an invalid or nonexistent remote encryptor MAC address is entered, an error message displays and the command aborts.

If the MAC address *is* already entered in the network MAC address table, an error message displays and the command aborts.

If the MAC address *is* already entered in the local MAC address table, the user is prompted to move the MAC address to another tunnel. If the response is yes, the existing address is moved to the specified tunnel. If the response is no, the address is not moved.

```
SEE>netmacs -a 00:d0:aa:23:12:cb -m
Remote encryptor mac address : 00:d0:1f:06:12:33
Added new remote mac address
SEE>
```

Delete a Network MAC Address

The **netmacs -d <*MAC address*>** command is used to delete a network MAC address. If an invalid or nonexistent network MAC address is entered, an error message displays and the command aborts. The wild card '*' deletes all network MAC addresses.

```
SEE>netmacs -d 00:d0:aa:23:12:ca
Are you sure you want to delete mac address ? (y/n) y
Deleted mac address
SEE>
```

Edit a Network MAC Address

The **netmacs -e <*MAC address*>** command is used to edit a network MAC address. The user is prompted for the *new* CI to associate with the network MAC address.

If an invalid or nonexistent network MAC address is entered, an error message displays and the command aborts.

```
SEE>netmacs -e 00:d0:aa:23:12:cc
Enter CI to associate mac address with : 6
Moved mac address
SEE>
```

List Network MAC Addresses

The **netmacs -l <*CI*>** command is used to list network MAC addresses. If a valid CI is entered, the network MAC address(es) associated with the CI is listed. If '*' is entered for the CI, all records will be displayed.

If an invalid or nonexistent CI is entered, an empty Network MAC table displays.

```
SEE>netmacs -l 4

Network Mac       CI
----------------- ----
00:03:34:56:aa:16 0004
00:03:34:56:aa:17 0004
2 Valid records

SEE>
```

Display the Number of Network MAC Addresses

The **netmacs -n** command displays the number of entries in the network MAC address table.

```
SEE>netmacs -n
7 Valid records
SEE>
```

Password Command

Syntax	Use to	Users
password	display the current password settings.	Administrator Operator
password -r <0-255>	set the reuse history size.	Administrator
password -e {on | off}	turn the enhanced password mode on or off.	Administrator
password -m <8-29>	set the minimum password length.	Administrator
password -u <1-2>	set the minimum number of uppercase characters.	Administrator
password -l <1-2>	set the minimum number of lowercase characters.	Administrator
password -n <1-2>	set the minimum number of numerical characters.	Administrator
password -s <1-2>	set the minimum number of special characters.	Administrator
password -h	display the help message.	Administrator Operator

The **password** command allows the password to be strengthened with various configuration options. The enhanced password mode, when enabled with the **password -e** command, enforces the following:

- the password and user ID must be different.
- the current password lexical requirements when logging on the device.
- setting a user account (not the administrator account) to inactive if two unsuccessful logon attempts are made within a 60 minute period. A user with administrator privileges is required to unlock the account.
- an event message is logged for unsuccessful logon attempts.
- the password expiration setting.

Password history discourages frequent password reuse. A record of previous user passwords is maintained for each account and when the password is changed the device ensures that old passwords are not reused. The size of the history can be configured thus allowing fine control over how often user account passwords may be recycled. If password reuse is disabled (set to 0) then no checking of user password reuse is enforced.

Examples

Display the Current Password Settings

The **password** command displays the current password policy.

```
SEE>password

Password enhanced mode: Disabled
Password lexical check: Enabled
Password reuse history: 255

Password requirements: 1.

Length of 8-29 characters
2. At least 1 uppercase alpha character
3. At least 1 lowercase alpha character
4. At least 1 numerical character
5. At least 1 special character

SEE>
```

Enable Enhanced Password Mode

Type **password -e on** to turn enhanced password mode on.

```
SEE>password -e on
Enabling enhanced passwords
SEE>
```

Set Password Reuse

Type **password -r <*n*>** to set the password reuse parameter. In the following example, the reuse parameter is set to 25.

```
SEE>password -r 25
Password reuse history: 25
SEE>
```

Policy Command

Syntax	**Use to**	**Users**
policy	display the current policy settings.	Administrator Operator
policy -b {-e | -d}	enable or disable bypass of reserved multicast addresses.	Administrator
policy -s {-e | -d}	enable or disable STP monitoring for deletion of local MAC address table entries.	Administrator
policy -k {-e | -d}	enable or disable the tunnel keep alive monitoring.	Administrator
policy -i {-e | -d}	enable or disable bypassing ingress packets received on the network port with unknown destination addresses.	Administrator
policy -m {-b | -d}	bypass or discard the default multicast/VLAN action.	Administrator
policy -p -a <*MAC address*>	add a specified MAC address to be bypassed. (VLAN mode only)	Administrator
policy -p -e <*index*>	edit bypassing of a specified MAC address (using the index). (VLAN mode only)	Administrator
policy -p -d <*index*>	delete bypassing of a specified MAC address (using the index). (VLAN mode only)	Administrator
policy -h	display the help message.	Administrator Operator

The **policy** command is used to enable or disable the following policy settings:

- Bypass - controls bypass of reserved multicast addresses
- STP - controls STP monitoring for deletion of local MAC address table entries

STP monitoring only applies when the switch devices connected to the SEE device local and network ports are configured for per VLAN spanning tree (PVST).

- Keep alive - controls tunnel keep alive monitoring
- Ingress - controls whether the encryptor will discard or bypass ingress packets received on the network port with unknown destination addresses. Previously, ingress packets were always discarded if their destination MAC address was not in the local MAC address table. This setting is used for testing purposes.
- Default Multicast/VLAN action - controls bypassing or discarding frames not classified by the multicast or VLAN group connections
- Bypass MAC address in VLAN mode - controls adding, editing, or deleting MAC addresses to be bypassed when in VLAN mode

See Miscellaneous Policy Settings for additional information.

Examples

Display the Policy Settings in MAC Mode

The **policy** command is used to display the current policy settings. The following example shows the display when the encryptor is in MAC mode.

```
SEE>policy

Policy parameter(s)                            Status
-------------------                            --------
Bypass Reserved Multicast                      Disabled
STP Monitoring                                 Disabled
Tunnel Keep Alive Monitoring                   Disabled
Observe Pending on unknown (DA) Ingress        Disabled
Default Multicast/VLAN Action                  Discard

SEE>
```

Display the Policy Settings in VLAN Mode

The **policy** command is used to display the current policy settings. The following example shows the display when the encryptor is in VLAN mode.

```
SEE>policy

Policy parameter(s)                            Status
-------------------                            --------
Bypass Reserved Multicast                      Disabled
STP Monitoring                                 Disabled
Tunnel Keep Alive Monitoring                   Disabled
Observe Pending on unknown (DA) Ingress        Disabled
Default Multicast/VLAN Action                  Discard

VLAN Connection Mode Reserved MAC Addresses:

Index Reserved MAC         Bypass
----- -------------------- ---------
0001  01:00:5e:01:01:01    enabled
0002  01:00:5e:01:01:02    enabled
0003  01:00:5e:01:01:03    disabled

SEE>
```

Enable Bypass of Reserved Multicast Addresses

Bypass of reserved multicast addresses is enabled using the **policy -b -e** command.

```
SEE>policy -b -e

Reserved Multicast bypass enabled

SEE>
```

Disable Bypass of Reserved Multicast Addresses

Bypass of reserved multicast addresses is disabled using the **policy -b -d** command.

```
SEE>policy -b -d

Reserved Multicast bypass disabled

SEE>
```

Enable STP Monitoring

STP monitoring is enabled using the **policy -s -e** command.

```
SEE>policy -s -e

STP monitoring enabled

SEE>
```

Disable STP Monitoring

STP monitoring is disabled using the **policy -s -d** command.

```
SEE>policy -s -d

STP monitoring disabled

SEE>
```

Enable Tunnel Keep Alive Monitoring

Tunnel keep alive monitoring is enabled using the **policy -k -e** command.

```
SEE>policy -k -e

Tunnel keep alive monitoring enabled

SEE>
```

Disable Tunnel Keep Alive Monitoring

Tunnel keep alive monitoring is disabled using the **policy -k -d** command.

```
SEE>policy -k -d

Tunnel keep alive monitoring disabled

SEE>
```

Enable Bypassing Ingress Packets

Bypassing ingress packets is enabled using the **policy -i -e** command.

```
SEE>policy -i -e

Observe pending action on unknown ingress enabled

SEE>
```

Disable Bypassing Ingress Packets

Bypassing ingress packets is disabled using the **policy -i -d** command.

```
SEE>policy -i -d

Observe pending action on unknown ingress disabled

SEE>
```

Set the Multicast/VLAN Action to Bypass

Set the multicast/VLAN action to bypass using the **policy -m -b** command.

```
SEE>policy -m -b

Default Multicast/VLAN Action Set to Bypass

SEE>
```

Add a MAC Address to be Bypassed

Type the **policy -p -a <***MAC address***>** command to add a MAC address to be bypassed.

```
SEE>policy -p -a 01:00:5e:01:01:01

Reserved MAC Address Bypass Action: <(E)nable | (D)isable>: [Enable]
Reserved MAC Address added

SEE>
```

Prompt Command

Syntax	Use to	Users
prompt	set the prompt to another name.	Administrator
prompt -h	display the help message.	Administrator Operator

The prompt is limited to a maximum of 30 alphabetic, numeric, and special characters. Spaces are not permitted in the prompt name. All text after a space is discarded.

Example

Change the Prompt

The following example shows the prompt being changed from SafeEnterprise Encryptor to Denver-SEE-3.

```
SafeEnterprise Encryptor>prompt Denver-SEE-3
Denver-SEE-3>
```

Reboot Command

Syntax	Use to	Users
reboot	reboot the unit.	Administrator
reboot -h	display the help message.	Administrator Operator

The **reboot** command resets the encryptor hardware. Traffic flow through the SEE is disrupted during the reboot for approximately 60 seconds. Confirmation to reboot the hardware is requested.

Example

Reboot the SEE

The following is an example of rebooting the SEE.

```
SEE>reboot
Are you sure you want to reboot the unit ? (y/n) y
Rebooting . . .
```

SFP Command

Syntax	Use to	Users
sfp	display the detected SFP information.	Administrator Operator
sfp -l	display the local port SFP information.	Administrator Operator
sfp -n	display the network port SFP information.	Administrator Operator
sfp -d	display the SFP diagnostics.	Administrator Operator
sfp -v	display detailed SFP information.	Administrator Operator
sfp -h	display the help message.	Administrator Operator

This command displays the detected and detailed small form-factor pluggable (SFP) optical transceiver information. This command is only available on the 1 Gbps encryptors. See Transceiver Specifications for information on the optical transceiver specifications.

Examples

List the Detected SFP Transceiver Information

The **sfp** command lists the detected SFP transceiver information.

```
SEE>sfp

================================================================================
 SFP LOCAL PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name           = FINISAR CORP.
Vendor Part Number    = FTLF8519P2BNL
Vendor Serial Number  = PFCON4B
Vendor Revision       = A
Date Code             = 090320


================================================================================
 SFP NETWORK PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name           = FINISAR CORP.
Vendor Part Number    = FTLF8519P2BNL
Vendor Serial Number  = PFC1B2P
Vendor Revision       = A
Date Code             = 090321

SEE>
```

List the SFP Transceiver Diagnostics

The **sfp-d** command lists the SFP transceiver diagnostics.

```
SEE>sfp -d

================================================================================
 SFP LOCAL PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name           = FINISAR CORP.
Vendor Part Number    = FTLF8519P2BNL
Vendor Serial Number  = PFCON4B
Vendor Revision       = A
Date Code             = 090320


================================================================================
                           |  Warning Limits |   Alarm Limits  |     Flags     |
--------------------------------------------------------------------------------
Parameter       | Measured |  High  |   Low  |  High  |   Low  |  Warn | Alarm |
--------------------------------------------------------------------------------
Temperature (C) |   +35.29 |    +90 |    -20 |    +95 |    -25 |    OK |    OK |
VCC (V)         |    +3.20 |  +3.70 |  +2.90 |  +3.90 |  +2.70 |    OK |    OK |
TX Bias (uA)    |     8180 |  14000 |   2000 |  17000 |   1000 |    OK |    OK |
TX Power (dBm)  |    -4.59 |  -2.00 | -11.03 |  -2.00 | -11.74 |    OK |    OK |
RX Power (dBm)  |    -4.29 |  -1.00 | -18.02 |  +1.00 | -20.00 |    OK |    OK |
================================================================================


================================================================================
 SFP NETWORK PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name           = FINISAR CORP.
Vendor Part Number    = FTLF8519P2BNL
Vendor Serial Number  = PFC1B2P
Vendor Revision       = A
Date Code             = 090321


================================================================================
                           |  Warning Limits |   Alarm Limits  |     Flags     |
--------------------------------------------------------------------------------
Parameter       | Measured |  High  |   Low  |  High  |   Low  |  Warn | Alarm |
--------------------------------------------------------------------------------
Temperature (C) |   +37.14 |    +90 |    -20 |    +95 |    -25 |    OK |    OK |
VCC (V)         |    +3.20 |  +3.70 |  +2.90 |  +3.90 |  +2.70 |    OK |    OK |
TX Bias (uA)    |     8188 |  14000 |   2000 |  17000 |   1000 |    OK |    OK |
TX Power (dBm)  |    -4.53 |  -2.00 | -11.03 |  -2.00 | -11.74 |    OK |    OK |
RX Power (dBm)  |    -4.85 |  -1.00 | -18.02 |  +1.00 | -20.00 |    OK |    OK |

SEE>
```

List the Detailed SFP Transceiver Information

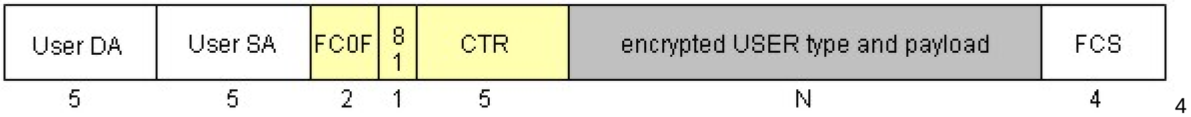
The **sfp-v** command lists the detailed SFP transceiver information.

```
SEE>sfp -v

================================================================================
 SFP LOCAL PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name            = FINISAR CORP.
Vendor Part Number     = FTLF8519P2BNL
Vendor Serial Number   = PFCON4B
Vendor Revision        = A
Date Code              = 090320
SONET Compliance       = N/A
Ethernet Compliance    = 1000BASE-SX
FC Link Length         = Intermediate Distance (I)
FC Tx Technology       = Shortwave Laser w/o OFC (SN)
FC Tx Media            = Multi-mode 62.5m (M6) & Multi-mode 50 m (M5, M5E)
FC Speed               = 200 MBytes/s & 100 MBytes/s
Encoding               = 8B/10B
Nominal Bit Rate       = 2100 Mbits/s
Link length (9/125)    = 0 m
Link length (50/125)   = 300 m
Link length (62.5/125) = 150 m
Link length (Copper)   = 0 m
Vendor OUI             = 009065
Laser Wavelength       = 850 nm
Bit Rate Max (%)       = 0
Bit Rate Min (%)       = 0
Diagnostic Monitoring  = Implemented
SFF-8472 Compliance    = Revision 9.3


================================================================================
 SFP NETWORK PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name            = FINISAR CORP.
Vendor Part Number     = FTLF8519P2BNL
Vendor Serial Number   = PFC1B2P
Vendor Revision        = A
Date Code              = 090321
SONET Compliance       = N/A
Ethernet Compliance    = 1000BASE-SX
FC Link Length         = Intermediate Distance (I)
FC Tx Technology       = Shortwave Laser w/o OFC (SN)
FC Tx Media            = Multi-mode 62.5m (M6) & Multi-mode 50 m (M5, M5E)
FC Speed               = 200 MBytes/s & 100 MBytes/s
Encoding               = 8B/10B
Nominal Bit Rate       = 2100 Mbits/s
Link length (9/125)    = 0 m
Link length (50/125)   = 300 m
Link length (62.5/125) = 150 m
Link length (Copper)   = 0 m
Vendor OUI             = 009065
Laser Wavelength       = 850 nm
Bit Rate Max (%)       = 0
Bit Rate Min (%)       = 0
Diagnostic Monitoring  = Implemented
SFF-8472 Compliance    = Revision 9.3

SEE>
```

Shim Command

Syntax	**Use to**	**Users**
shim	display the current shim header insertion rate.	Administrator Operator
shim -r *<0-32767>*	modify the shim header insertion rate.	Administrator
shim -m {-e | -d}	prevent MTU overflow on shim insertion.	Administrator
shim -h	display the help message.	Administrator Operator

To synchronize the CTR value between encryptors for counter mode operation, a shim header is inserted into a frame. The shim is 8-bytes long and has the following format:



The shims are detected and removed by the decrypting encryptor before the frame is passed to the network.

The original ethertype is encrypted if a shim is inserted into the frame.

In line mode or multipoint MAC mode, if the received CTR value is out of order (as in a replay or reordering attack), all unshimmed frames are discarded until the next shimmed frame with a valid CTR is received. If a frame is lost in the network, the subsequent frames will be decrypted incorrectly until the next shim frame is received and the CTR resynchronized. The shims are detected and removed by the decrypting encryptor before the frame is passed to the network.

For unicast encrypted frames in multipoint MAC mode, the **shim** command controls inserting a shim header into frames to support counter (CTR) mode encryption. The shim header is inserted into select frames based on the defined shim insertion rate. The default shim header insertion rate is set to one shim header per 32 frames. The setting of the shim header insertion rate allows the user to select the balance between data throughput and error recovery. The user can effectively take a slight hit on throughput for improved error recovery, or achieve maximum throughput and minimum latency with reduced error recovery capability. Increasing the shim insertion rate (16) will reduce potential frame loss, but will increase overhead; decreasing the rate of insertion (100) will reduce overhead, but will increase potential frame loss.

A setting of zero disables shim insertion. The use of a Shim Insertion rate of zero should be limited to very specific, controlled scenarios; this is effectively trading off any error recovery capability since there will be no indication of crypto sync loss on the data ports. This scenario setting should be reserved for laboratory environments rather than live deployments.

Decreasing the insertion rate, by setting the value significantly higher than every 32 frames, will not dramatically increase throughput, but it will reduce error recovery.

Shim insertion behavior can be further tuned by disabling, or enabling, shim insertion on frames which would subsequently violate the maximum MTU setting based on the following:

- If the encryptor link speed is 10 Gbps, the MTU overflow limit is 1510 bytes.
- If the encryptor link speed is 1 Gbps, the MTU overflow is 256 bytes.
- If the encryptor link speed is 10 Mbps or 100 Mbps, there is no MTU overflow protection for the link.

Examples

Display the Current Shim Header Insertion Rate

The **shim** command displays the current shim header insertion rate.

```
SEE>shim
SHIM parameter                          Status
----------------------                  --------
SHIM rate                               32
MTU overflow prevention on shim         enabled
SEE>
```

Modify the Current Shim Header Insertion Rate

The **shim -r <*0 - 32767*>** command modifies the shim header insertion rate to the required value.

```
SEE>shim -r 16
Shim insertion rate updated:

SHIM parameter                           Status
----------------------                   --------
SHIM rate                                16
MTU overflow prevention on shim          enabled
SEE>
```

Disable Shim Header Insertion

The **shim -m -d** command disables MTU overflow protection on shim insertion.

```
SEE>shim -m -d
MTU overflow prevention updated:

SHIM parameter                           Status
----------------------                   --------
SHIM rate                                16
MTU overflow prevention on shim          disabled
SEE>
```

SNAP Command

Syntax	Use to	Users
snap	display the current SNAP PID Ethertype status.	Administrator Operator
snap -p {-e | -d}	enable and disable the SNAP PID Ethertype status.	Administrator
snap -h	display the help message.	Administrator Operator

The **snap** command is used to enable and disable the SNAP PID Ethertype status.

When enabled, the SNAP header PID field in length encapsulated 802.3 SAP SNAP frames is used as an ethertype and is matched to the ethertype policy table.

When disabled, the 802.3 SAP SNAP frames are categorized as length encapsulated frames such as the 0x05ff ethertype entry.

Examples

Display the SNAP Status

The **snap** command displays the SNAP PID Ethertype status.

```
SEE>snap

SNAP parameter                                  Status
--------------                                  -------
Observe SNAP PID for ethertype processing       enabled

SEE>
```

Enable SNAP

The **snap -p -e** command enables the SNAP PID Ethertype status.

```
SEE>snap -p -e
SNAP PID for ethertype processing enabled

SEE>
```

Disable SNAP

The **snap -p -d** command disables the SNAP PID Ethertype status.

```
SEE>snap -p -d
SNAP PID for ethertype processing disabled

SEE>
```

SNMPCFG Command

Syntax	Use to	Users
snmpcfg	display the current SNMP privacy status.	Administrator Operator
snmpcfg -p {on | off}	enable or disable SNMP privacy.	Administrator
snmpcfg -h	display the help message.	Administrator Operator

The **snmpcfg** command displays the current SNMP privacy status and enables or disables SNMP privacy.

SNMP privacy can be disabled only when FIPS mode is disabled. See FIPS Command for instructions on disabling FIPS mode.

Examples

Display the SNMP Privacy Status

The following example shows the current SNMP privacy status.

```
SEE>snmpcfg
SNMP Privacy mode enabled
SEE>
```

Disable SNMP Privacy

The following example shows SNMP privacy being disabled. FIPS mode must be disabled before SNMP privacy can be disabled.

```
SEE>snmpcfg -p off
Disable SNMP Privacy selected. Validation...succeeded.
SNMP Privacy Disabled
SEE>
```

Stats Command

Syntax	Use to	Users
stats	display the local and network port statistics.	Administrator Operator
stats -l	display the local port statistics.	Administrator Operator
stats -n	display the network port statistics.	Administrator Operator
stats -r	reset the statistics.	Administrator
stats -h	display the help message.	Administrator Operator

This command is used to display the local and network port statistics and reset the statistics.

Examples

Display the Local and Network Port Statistics

The following example shows the **stats** command displaying the local and network port statistics.

```
SEE>stats

Ethernet Local Port Statistics:

Rx Corrupted Frames      = 0
Rx Interframe Gap Errors = 0
Rx Octet Count           = 497530632
Rx Frame Count           = 4090995
Rx FCS Errored Frames    = 0
Rx PCS Errored Frames    = 0
Rx Undersized Frames     = 0
Rx Oversized Frames      = 0
Rx Discarded Frames      = 10485
Rx PCS Sync Status       = In Sync
Tx Octet Count           = 619650479
Tx Frame Count           = 5616436
Tx FCS Errored Frames    = 0


Ethernet Network Port Statistics:

Rx Corrupted Frames      = 0
Rx Interframe Gap Errors = 0
Rx Octet Count           = 665189869
Rx Frame Count           = 5641120
Rx FCS Errored Frames    = 0
Rx PCS Errored Frames    = 0
Rx Undersized Frames     = 0
Rx Oversized Frames      = 0
Rx Discarded Frames      = 1024
Rx PCS Sync Status       = In Sync
Rx Manage Octet Count    = 2910616
Rx Manage Frame Count    = 23662
Rx Manage Drop Frames    = 0
Tx Octet Count           = 534823630
Tx Manage Octet Count    = 5968931
Tx Frame Count           = 4127716
Tx Manage Frame Count    = 47204
Tx FCS Errored Frames    = 0
Rx Shim Octets           = 42412552
Tx Shim Octets           = 31993616

SEE>
```

Reset the Statistics

Type the **stats -r** command to reset the encryptor's statistics.

```
SEE>stats -r

Ethernet statistics reset to zero.

SEE>
```

Tunnels Command

Syntax	Use to	Users
tunnels	display all tunnels.	Administrator Operator
tunnels -a <*MAC address*>	add a tunnel using the remote encryptor's MAC address. (Line mode and multipoint MAC mode only)	Administrator
tunnels -a {sec | dis | byp} <*tag*> <*tag*>	add a tunnel and set traffic to secure, discard, or bypass. The variable 'tag' is a combination of the ethertype and VLAN ID. For example, 8100 and 0002, where 8100 is a well known ethertype for VLAN and 0002 is the VLAN ID. (multipoint VLAN mode only) For example: **tunnels -a sec** adds a secure tunnel, null tag session. **tunnels -a sec 8100 0FFF** adds a secure tunnel, 1 tag session. **tunnels -a sec 9100 FFF 8100 123** adds a secure tunnel, 2 tag session. **tunnels -a sec 91000FFF81000123** adds a secure tunnel, 2 tag session.	Administrator
tunnels -d <*CI*>	delete a tunnel specified by the connection identifier.	Administrator
tunnels -d <*MAC address*> -m	delete a tunnel specified by the remote encryptor's MAC address. (Line mode and multipoint MAC mode only)	Administrator
tunnels -d *	delete all tunnels.	Administrator
tunnels -e <*CI*>	edit a tunnel specified by the connection identifier.	Administrator
tunnels -e <*MAC address*> -m	edit a tunnel specified by the remote encryptor's MAC address. (Line mode and multipoint MAC mode only)	Administrator
tunnels -l <*CI*>	display a tunnel specified by the connection identifier.	Administrator Operator
tunnels -l <*MAC address*> -m	display a tunnel specified by the remote encryptor's MAC address. (Line mode and multipoint MAC mode only)	Administrator Operator
tunnels -l *	display all tunnels.	Administrator Operator
tunnels -s <*CI*>	stop a tunnel specified by the connection identifier.	Administrator
tunnels -s <*MAC address*> -m	stop a tunnel specified by the remote encryptor's MAC address. (Line mode and multipoint MAC mode only)	Administrator
tunnels -s *	stop all tunnels.	Administrator
tunnels -r <*CI*>	restart a tunnel specified by the connection identifier.	Administrator
tunnels -r <*MAC address*> -m	restart a tunnel specified by the remote encryptor's MAC address. (Line mode and multipoint MAC mode only)	Administrator
tunnels -r *	restart all tunnels.	Administrator
tunnels -k <*n*>	modify the key update interval.	Administrator
tunnels -h	display the help message.	Administrator Operator

The **tunnels** command is used to add and manipulate records in the Connection Identifier (CI) table.

For unicast frame encryption, entries in the CI (tunnels) table represent the addresses protected by each CI entry. These CI entries contain either the MAC address of the remote encryptor protecting the network MAC table devices (when the connection policy is set to MAC Address), or the network VLAN ID (when the connection policy is set to VLAN ID).

For multicast frame encryption, entries in the CI table represent a single multicast address and the CI table will contain the multicast address rather than the remote encryptor's MAC address (when the connection policy is set to MAC Address). This requires multicast group key encryption in contrast to normal peer key encryption. If 'Enable Multicast Auto Discovery' is enabled then multicast group addresses will be automatically added to the network MAC address table as they are discovered, and the table lists the associated connection identifier for that group.

During auto-discovery the first observed multicast VLAN tag will be retained for use in encryptor group key management traffic. If multicast traffic will be sent to more than one VLAN then this learned value should be replaced with a common unique VLAN number on all encryptors that will process multicast traffic. See VLAN Command for additional information.

The CI table has 3 default entries:

- CI 1 - pending
- CI 2 - discard
- CI 3 - bypass

The only default entry that can have the tunnel action modified by the user is the pending entry, CI 1. The valid action settings for pending are discard and bypass. All other records in the table will be either automatically discovered or manually entered. When the CI table is displayed, the network MAC address list associated with the CI is displayed also.

The fields contained in the CI table are listed below:

- CI (Connection Identifier) - id number for a tunnel between two encryptors.
- Origin - system, system pending, auto, or manual.
- (Tunnel) Action - secure, bypass, or discard Ethernet frame on this connection.
- State - start, ready, up, start, or fault.
- Peer Name (Remote Encryptor Name) - for unicast frames, this is the peer encryptor's name that is automatically learned during session establishment. It is informational only as changes will not affect the operation of the tunnel, but may lead to confusion if it does not match the name of the peer device. (Line mode and multipoint MAC mode only)
- Peer Name (Group Key Name) - for multicast frames, this is the group key name for the CI and is automatically generated during session establishment (multipoint MAC mode only). The group key name for multicast entries has information about the connection, for example **M 030422 3**, where:
  M indicates that the managed encryptor is acting as the current key master for this multicast group (if not present then another encryptor in the group is the key master)
  030422 replicates the last 3 bytes of the original key master's MAC address
  3 indicates the number of times that the key master has shared its key with other members of the group.
- Remote MAC - MAC address of the peer encryptor bound to this connection. (Line mode and multipoint MAC mode only)
- Header content in HEX (0xnnnn...): 0x81000010 (Line mode and multipoint MAC mode only)

- group info (Group Key Name) - group key management information for the VLAN group connection (multipoint VLAN mode only). The group key name for VLAN group entries has information about the connection, for example **M41a2cf_bd2d8ff6**, where:
  M indicates that the managed encryptor is acting as the current key master for this VLAN group (if s instead of M, then another encryptor in the group is the key master)
  41a2cf replicates the last 3 bytes of the original key master's MAC address
  bd2d8ff6 represents a random unique identifier for the group
- VLAN - the same as 'tag 'described above. (multipoint VLAN mode only)
- Key# - number of times the connection had a key update. This occurs more or less frequently depending on the key update interval setting. (multipoint VLAN mode only)

Origin

The origin values are described as follows:

- System - predefined tunnel for discard and bypass actions
- System pending - predefined tunnel for automatically discovered pending action
- Auto - automatically generated tunnel
- Manual - user configured tunnel

State

The tunnel state will be one of the following depending on the current state of the key exchange process:

- Start - initial state for the tunnel negotiation, peer state is unknown
- Ready - peer state is in start/ready and device is ready to negotiate
- Up - tunnel has successfully negotiated and is up and running
- Stop - tunnel has been stopped by the user
- Fault - tunnel negotiation encountered an error and is in fault state

These tunnel states may be seen momentarily during the key exchange process:

- Flow1 - the first message in the three-way key exchange has been sent by the initiating encryptor
- Flow2 - if the 'flow1' message was successful, a reply (second message in the three-way key exchange) from the responding encryptor was sent to the initiating encryptor
- Flow3 - if the 'flow2' message was successful, a reply (third message in the three-way key exchange) from the initiating encryptor was sent to the responding encryptor

Examples

Display All Tunnels - Line Mode

The **tunnels** command displays all tunnels. The following display is for an encryptor in line mode.

```
SEE>tunnels

Interface (tunnel/CI) MAC address  : 00:0d:b9:17:23:7e
Front Panel Management MAC address : 00:0d:b9:17:23:7c

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0001 System   Secure   Up       RDC-SEE-04       00:0d:b9:16:5b:ca

SEE>
```

Display All Tunnels - Multipoint MAC Mode

The **tunnels** command displays all tunnels. The following display is for an encryptor in multipoint MAC mode.

```
SEE>tunnels

Interface (tunnel/CI) MAC address  : 00:20:e2:12:34:58
Front Panel Management MAC address : 00:20:e2:30:13:51>
Key update interval : 10minutes

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0001 PENDING  Discard  Up       N/A
        00:11:11:26:dd:2c 00:0c:f1:c3:c1:fd
0002 System   Discard  Up       N/A
0003 System   Bypass   Up       N/A
0004 Auto     Secure   Up       M 123458   9     01:00:5e:01:01:01     81000002
0005 Auto     Secure   Up       RDC-SEE-03       00:0d:b9:17:23:7e
        00:11:11:26:dd:ca 00:0c:f1:a0:a9:9b
0006 Auto     Secure   Up       RDC-SEE-10-D     00:20:e2:30:14:bb     81000002
        00:11:11:26:dd:0d 00:11:11:53:7f:d0
0007 Auto     Secure   Up       RDC-SEE-08       00:20:e2:12:34:59     81000002
        00:11:11:26:dc:ce 00:11:11:26:dd:1d
0008 Auto     Secure   Up       M 123458 10      01:00:5e:01:01:02     81000002
0009 Auto     Secure   Up       M 123458 13      01:00:5e:01:01:03     81000002

SEE>
```

Display All Tunnels - Multipoint VLAN Mode

The **tunnels** command displays all tunnels. The following display is for an encryptor in multipoint VLAN mode.

```
SEE>tunnels

Interface (tunnel/CI) MAC address : 00:20:e2:30:05:9f
Front Panel Management MAC address : 00:20:e2:30:10:42
Key update interval : 60 minutes

CI   Origin   Action   State    group info       VLAN             KEY#
---- -------- -------- -------- ---------------- ---------------- --------
0001 Auto     Secure   Up       s41a2cf_bd2d8ff6                        92
0002 Auto     Secure   Up       s41a2cf_6bb49cdf 81000003               92
0003 Auto     Secure   Up       s41a2cf_db59403e 81000002               92
0004 Manual   Secure   Up       M30059f_e4c66179 81000fff                0

SEE>
```

Add a Tunnel - Line or Multipoint MAC Mode

The **tunnels -a <*MAC address*>** creates a tunnel. If the MAC address is already entered in the CI table, an error message displays and the command aborts. The Remote Encryptor Name is the Host name typed in SMCII when the certificate is loaded.

```
SEE>tunnels -a 00:d0:1f:06:12:35
Remote Encryptor Name : []
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] s
Header content in HEX : []
Added new tunnel ci 7
SEE>
```

Add a Tunnel - Multipoint VLAN Mode

The **tunnels -a sec <*tag*>** command creates a secure tunnel in multipoint VLAN mode with the specified ethertype and VLAN ID.

```
SEE>tunnels -a sec 8100000a
SEE>
```

Delete a Tunnel

The **tunnels -d <*CI*>** command deletes a tunnel using the connection identifier. If the CI number exists, a prompt displays requesting confirmation to delete the entry. When the entry is deleted, all the network MAC addresses associated with the CI are deleted from the network MAC table.

If a user tries to delete a nonexistent entry, CI 1, CI 2, or CI 3, an error message displays and the command aborts.

```
SEE>tunnels -d 7

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0007 Manual   Secure   Start    TBD              00:d0:1f:06:12:35

Are you sure you want to delete tunnel? (y/n) y
Deleted tunnel 7
SEE>
```

Multicast group connections (tunnels) can remain active even when there is no multicast traffic due to the group key mechanism implementation. As a result, deleting an inactive multicast group connection will result in the session reestablishing. One approach to deleting an inactive group connection is to first set auto-discovery to disabled and then delete the connection. A second approach to delete an inactive multicast group connection (tunnel) with auto-discovery enabled would be to enable multicast ageing and then the tunnel will be deleted automatically. See Autodisco Command for additional information.

Edit a Tunnel

The **tunnels -e <*CI*>** command edits a tunnel using the connection identifier.

If a user tries to edit a nonexistent entry, an error message displays and the command aborts.

```
SEE>tunnels -e 5

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0005 Manual   Secure   Up       GigE2            00:d0:1f:06:12:33

Remote Encryptor MAC:: [00:d0:1f:06:12:33]
Remote Encryptor Name : []
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Secure] b
Header content in HEX : []
Updated existing tunnel
SEE>
```

Stop a Tunnel

The **tunnels -s <***MAC address***> -m** command prevents network traffic from flowing using the remote encryptor's MAC address.

If a user tries to stop a nonexistent entry, an error message displays and the command aborts.

```
SEE>tunnels -s 00:d0:1f:06:12:33 –m
Changed state of tunnel 5
SEE>
```

Restart a Tunnel

The **tunnels -r *** command forces all tunnels to be renegotiated. The restart argument issues a stop and then a start command for the tunnels.

If a user tries to restart a nonexistent entry, CI 1, CI 2, or CI 3, an error message displays and the command aborts.

```
SEE>tunnels -r *
Changed state of 6 tunnels
SEE>
```

List a Tunnel

The **tunnels -l** <*MAC address***> -m** command displays a tunnel's information using the remote encryptor's MAC address.

If a user tries to list a nonexistent entry, an error message displays and the command aborts.

```
SEE>tunnels -l 00:e7:1d:14:23:06 -m

CI   Origin   Action   State    Peer Name        Remote MAC           MAC Header
---- -------- -------- -------- ---------------- -------------------- ----------------
0004 Auto     Secure   Up       Data             00:e7:1d:14:23:06
  00:03:34:56:aa:16 00:03:34:56:aa:17 00:d0:aa:23:12:ca

SEE>
```

Modify the Key Update Interval

The **tunnels -k <***n***>** command is used to change the key update interval. The key update will take place after the current key update interval expires or the tunnel is restarted. The minimum interval is 1 minute and the maximum interval is 60 minutes. The default interval is 60 minutes.

```
SEE>tunnels -k 30
Key Update interval set to 30 minutes.
NB: Change will take effect after current key update
     period has expired or on tunnel restart!
SEE>
```

USB Command

Syntax	Use to	Users
usb	display the current USB port status.	Administrator Operator
usb lock	disable the USB port.	Administrator
usb unlock	enable the USB port.	Administrator
usb -h	display the help message.	Administrator Operator

The **usb** command displays the current USB port status and disables or enables the USB port.

Examples

Display the USB Port Status

The following example shows the current USB port status.

```
SEE>usb
USB port is locked
SEE>
```

Unlock the USB Port

The following example shows the USB port being enabled.

```
SEE>usb unlock
USB port is unlocked
SEE>
```

Users Command

Syntax	Use to	Users
users	list the current users table.	Administrator Operator
users -a	add a user.	Administrator
users -e <*index*>	edit a user entry.	Administrator
users -d <*index*>	delete a user entry.	Administrator
users -n	display the number of users.	Administrator Operator
users -h	display the help message.	Administrator Operator

Information on the privilege levels and maximum number of users is explained in User Types.

During the certification process the default user id and password are deleted when a new user id and password is entered. However, the default user id and password can be reused if desired. SNMP access is enabled by default so the encryptor can be managed by SMCII. The same user id and password are used for access via SMCII or the CLI.

The following information can be displayed and configured with the **users** command:

- User id - identifier for the user account
- User name - name associated with the user id
- Status - user account is active or inactive - default is active
- Level - administrator or operator privilege level - default is operator
- Console access - management via the CLI is enabled or disabled - default is enabled
- SNMP access - management via SMCII is enabled or disabled - default is enabled
- Password - password for the user account
- Confirm password - re-enter the password for the user account
- Password expiry - date that the current password expires - the date can be set to a specified date, sixty days from the current date, or disabled

Examples

Display the Users Table

The following example shows the list of user(s) and associated account information.

```
SEE>users

Number of users in table is 2

Index User ID Active Level         Console SNMP P/W Check P/W Expiry
----- ------- ------ -----         ------- ---- --------- ----------
1     admin   Yes    Administrator Yes     Yes  Passed    Disabled
2     safenet Yes    Administrator Yes     Yes  Passed    2010-10-25
SEE>
```

Add a New User Account

This example shows a new user account being added with a password expiration of 60 days.

```
SEE>users -a
User id: <3-10 characters>: [] sclark
User name: <max 30 characters>: [] Sam Clark
Status: <(A)ctive | (I)nactive>: [Active]
Level: <(A)dmin | (O)perator: [Operator]
Console access: <(E)nabled | (D)isabled>: [Enabled]
SNMP access: <(E)nabled | (D)isabled>: [Enabled]
Password: <8-29 characters>: [] ********
Confirm password: <8-29 characters>: ********
Password expiry: <yyyy-mm-dd | (S)ixty days | (D)isabled>: [0000-00-00] s

Is the information correct? (y/n/q) y
New record added- index 3
SEE>
```

Update a User Account

The user account status is being changed to inactive in this example.

```
SEE>users -e 3
User id: <3-10 characters>: [sclark]
User name: <max 30 characters>: [Sam Clark]
Status: <(A)ctive | (I)nactive>: [Active] i
Level: <(A)dmin | (O)perator: [Operator]
Console access: <(E)nabled | (D)isabled>: [Enabled]
SNMP access: <(E)nabled | (D)isabled>: [Enabled]
Password: <8-29 characters>: []
Password expiry: <yyyy-mm-dd | (S)ixty days | (D)isabled>: [2010-08-25]

Is the information correct? (y/n/q) y
Record updated
SEE>
```

Delete a User Account

The user account with an index of ‘3’ is being deleted in this example.

```
SEE>users -d 3

UserId     Active Level         Console Snmp
------     ------ -----         ------- ----
sclark     No     Operator      Yes     Yes
Are you sure you want to delete this entry ? (y/n) y
Record deleted
SEE>
```

Display the Number of Users

The **users -n** command displays the total number of user accounts created.

```
SEE>users -n
Number of users = 2
SEE>
```

Version Command

Syntax	Use to	Users
version	display the firmware version and build information.	Administrator Operator
version -h	display the help message.	Administrator Operator

This **version** command displays the following information about the software and firmware currently installed on the SEE.

- Version - version number for the installed software
- Library version - library number including build number

Example

Display the Software Version

The following is a representation of the **version** command display.

See the Customer Release Notes for the correct version information.

```
SEE>version

Software:
    Version     : 4.0.0

Library
    Build ID: 5.D115
SEE>
```

VLAN Command

Syntax	Use to	Users
vlan	display the current VLAN header bypass status.	Administrator Operator
vlan -p {-e | -d}	enable and disable the VLAN header bypass.	Administrator
vlan -1	set the VLAN primary ethertype.	Administrator
vlan -2	set the VLAN alternate ethertype.	Administrator
vlan -m {-e | -d}	enable and disable multicast management VLAN substitution. (Line mode and multipoint mode only)	Administrator
vlan -v	set VLAN tags for multicast VLAN substitution. (Line mode and multipoint mode only)	Administrator
vlan -s {1 | 2}	set the number of stacked VLAN IDs used to establish a VLAN connection.	Administrator
vlan -h	display the help message.	Administrator Operator

The **vlan** command is used to enable and disable the VLAN header bypass status. A primary and alternate VLAN ethertype value can also be set using this command. The primary and alternate VLAN ethertype 0x8100 is programmed into the encryptor.

When enabled, VLAN tags are automatically bypassed and encryption starts after the VLAN tags. This is only for the configured primary and alternate VLAN ethertypes. A maximum stack depth of 2 VLAN tags is supported.

The default ethertype policy for VLAN tagged frames depends on the protocol switched over the VLAN (it depends on the preceding ethertype after the tag).

When enabled, the tunnel with the peer encryptor learns the VLAN tag required to communicate with the peer encryptor.

When disabled, the VLAN tags are encrypted and the default ethertype policy for VLAN tagged frames is the 'other' ethertype.

The **vlan –s** command allows you to select the number of VLAN tags that will be used to define a unique connection in the CI table (see Tunnels Command). If the value is selected as 1 tag, then irrespective of the number of VLAN tags present for an inbound frame only the outer tag will be used. If 2 tags are specified for the **vlan –s** option, then a unique connection will use both tags in the CI table, or just 1 tag if only 1 exists for the inbound frame.

The VLAN primary ethertype is the value that will be parsed on the tags to identify tagged frames. It has a default value of 8100. This may be changed as required to match the value in use in the network. For example some network vendors use a VLAN ethertype value of 9100. In the Q-in-Q case where the VLAN ethertypes may differ, there is an ability to specify an alternate ethertype. This may be enabled on a per connection basis to specify that the alternate ethertype be used on the inner tag for frames that have 2 tags.

Examples

Display the VLAN Header Status

The **vlan** command is used to display the current VLAN header bypass status and alternate ethertype value. The following example is for an encryptor in line or multipoint mode.

```
SEE>vlan

VLAN parameter                                  Status
--------------                                  --------
Protocol tag(s) bypass                          enabled
VLAN primary ethertype                          0x8100
VLAN alternate ethertype                        0x8100
Multicast management VLAN substitution          disabled
Multicast management VLAN substitution tag      81000002

Number of stacked VLAN Ids (VLAN connection mode): 2

SEE>
```

Enable the VLAN Header

The VLAN header is enabled using the **vlan -p -e** command.

```
SEE>vlan -p -e

VLAN protocol bypass enabled

SEE>
```

Disable the VLAN Header

The VLAN header is disabled using the **vlan -p -d** command.

```
SEE>vlan -p -d

VLAN protocol bypass disabled

SEE>
```

Set the VLAN Primary Ethertype

The VLAN primary ethertype is set using the **vlan -1** command.

```
SEE>vlan -1
Enter VLAN primary ethertype [0x0600-0xFFFF]: 9100
SEE>
```

Clear the Multicast Management VLAN Substitution Tag

The multicast management VLAN substitution tag is cleared using the **vlan -v** command.

```
SEE>vlan -v
Cleared Multicast management VLAN substitution tag
SEE>
```

XFP Command

Syntax	Use to	Users
xfp	display the local and network port detected XFP information.	Administrator Operator
xfp -l	display the local port XFP information.	Administrator Operator
xfp -n	display the network port XFP information.	Administrator Operator
xfp -d	display the XFP diagnostics.	Administrator Operator
xfp -v	display detailed XFP information.	Administrator Operator
xfp -h	display the help message.	Administrator Operator

This command displays the detected and detailed 10 gigabit small form-factor pluggable (XFP) optical transceiver information. This command is only available on the 10 Gbps encryptors. See Transceiver Specifications for information on the optical transceiver specifications.

Examples

List the Detected XFP Transceiver Information

The **xfp** command lists the detected XFP transceiver information.

```
SEE>xfp

================================================================================
 XFP LOCAL PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name            = FINISAR CORP.
Vendor Part Number     = FTLX3811M360
Vendor Serial Number   = AGN0B4L
Vendor Revision        = 00
Date Code              = 091203


================================================================================
 XFP NETWORK PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name            = FINISAR CORP.
Vendor Part Number     = FTLX1811M3
Vendor Serial Number   = AH70DF0
Vendor Revision        = 00
Date Code              = 100304

SEE>
```

List the XFP Transceiver Diagnostics

The **xfp-d** command lists the XFP transceiver diagnostics.

```
SEE>xfp -d

================================================================================
 XFP LOCAL PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name           = FINISAR CORP.
Vendor Part Number    = FTLX3811M360
Vendor Serial Number  = AGN0B4L
Vendor Revision       = 00
Date Code             = 091203


================================================================================
                           |  Warning Limits |   Alarm Limits  |     Flags     |
--------------------------------------------------------------------------------
Parameter       | Measured |  High  |   Low  |  High  |   Low  |  Warn | Alarm |
--------------------------------------------------------------------------------
Temperature (C) |   +32.15 |    +75 |    -10 |    +78 |    -13 |    OK |    OK |
AUX1 Laser (C)  |   +47.52 |    +40 |    +24 |    +45 |    +20 |  HIGH |  HIGH |
AUX2 +5V (V)    |    +4.99 |  +5.30 |  +4.70 |  +5.50 |  +4.50 |    OK |    OK |
TX Bias (uA)    |    79436 | 121000 |  35000 | 131000 |  30000 |    OK |    OK |
TX Power (dBm)  |    +1.92 |  +4.50 |  -2.50 |  +5.00 |  -3.00 |    OK |    OK |
RX Power (dBm)  |   -19.96 |  -5.50 | -25.53 |  -5.00 | -26.02 |   LOW |   LOW |
================================================================================


================================================================================
 XFP NETWORK PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name           = FINISAR CORP.
Vendor Part Number    = FTLX1811M3
Vendor Serial Number  = AH70DF0
Vendor Revision       = 00
Date Code             = 100304


================================================================================
                           |  Warning Limits |   Alarm Limits  |     Flags     |
--------------------------------------------------------------------------------
Parameter       | Measured |  High  |   Low  |  High  |   Low  |  Warn | Alarm |
--------------------------------------------------------------------------------
Temperature (C) |   +32.86 |    +75 |    -10 |    +78 |    -13 |    OK |    OK |
AUX1 Laser (C)  |   +35.73 |    +40 |    +24 |    +45 |    +20 |    OK |    OK |
AUX2 +5V (V)    |    +4.99 |  +5.30 |  +4.70 |  +5.50 |  +4.50 |    OK |    OK |
TX Bias (uA)    |    55760 | 121000 |  35000 | 131000 |  30000 |    OK |    OK |
TX Power (dBm)  |    +1.98 |  +6.00 |  -1.50 |  +6.50 |  -2.00 |    OK |    OK |
RX Power (dBm)  |   -10.37 |  -5.50 | -25.53 |  -5.00 | -26.02 |    OK |    OK |

SEE>
```

List the Detailed XFP Transceiver Information

The **xfp-v** command lists the detailed XFP transceiver information.

```
SEE>xfp -v

================================================================================
 XFP LOCAL PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name            = FINISAR CORP.
Vendor Part Number     = FTLX3811M360
Vendor Serial Number   = AGN0B4L
Vendor Revision        = 00
Date Code              = 091203
Extended Identifier    = Power Level 3 Module (3.5 W Maximum)
Extended Identifier    = Module with CDR function
Extended Identifier    = TX Ref Clock Input Not Required
10 GbE Compliance      = N/A
10 Gb FC Compliance    = N/A
Lower Speed Links      = N/A
SONET Interconnect     =  N/A
SONET Short Haul       = N/A
SONET Long Haul        = G.959.1 P1L1-2D2
SONET Very Long Haul   = N/A
Encoding Support       = 64B/66B & 8B10B & SONET Scrambled & NRZ
Bit Rate (min-max)     = 9900 - 11100 MBits/s
Length (SMF)           = 80 km
Length (EBW 50/125 um) = 0 m
Length (50/125 um)     = 0 m
Length (62.5/125 um)   = 0 m
Length (Copper)        = 0 m
Device Technology      = No wavelength control
Device Technology      = Cooled transmitter
Device Technology      = APD detector
Device Technology      = Transmitter NOT Tunable
Transmitter Technology = 1550nm EML
CDR Support            = 9.95 & 10.3 & 10.5 & 10.7 & 11.1 & XFI L/B
Vendor OUI             = 009065
Wavelength             = 1529.11 nm
Wavelength Tolerance   = +/- 0.020 nm
Max Case Temperature   = 70 (C)
Max Power Dissipation  = 3500 mW
Max Power Power Down   = 1500 mW
Max current +5V        = 350 mA
Max current +3V3       = 400 mA
Max current +1V8       = 800 mA
Max current -5V2       = 0 mA
Diagnostic Monitoring  = No BER Support
Received Power         = Average Power
Enhanced Options       = Soft TX_DISABLE & Soft P_down
Auxiliary A/D Input 1  = Laser temperature
Auxiliary A/D Input 2  = +5V supply voltage
```

```
================================================================================
 XFP NETWORK PORT SERIAL DIGITAL DIAGNOSTICS
================================================================================
Vendor Name            = FINISAR CORP.
Vendor Part Number     = FTLX1811M3
Vendor Serial Number   = AH70DF0
Vendor Revision        = 00
Date Code              = 100304
Extended Identifier    = Power Level 3 Module (3.5 W Maximum)
Extended Identifier    = Module with CDR function
Extended Identifier    = TX Ref Clock Input Not Required
10 GbE Compliance      = N/A
10 Gb FC Compliance    = N/A
Lower Speed Links      = N/A
SONET Interconnect     = N/A
SONET Short Haul       = N/A
SONET Long Haul        = G.959.1 P1L1-2D2
SONET Very Long Haul   = N/A
Encoding Support       = 64B/66B & 8B10B & SONET Scrambled & NRZ
Bit Rate (min-max)     = 9900 - 11100 MBits/s
Length (SMF)           = 80 km
Length (EBW 50/125 um) = 0 m
Length (50/125 um)     = 0 m
Length (62.5/125 um)   = 0 m
Length (Copper)        = 0 m
Device Technology      = No wavelength control
Device Technology      = Cooled transmitter
Device Technology      = APD detector
Device Technology      = Transmitter NOT Tunable
Transmitter Technology = 1550nm EML
CDR Support            = 9.95 & 10.3 & 10.5 & 10.7 & 11.1 & XFI L/B
Vendor OUI             = 009065
Wavelength             = 1550.00 nm
Wavelength Tolerance   = +/- 17.100 nm
Max Case Temperature   = 70 (C)
Max Power Dissipation  = 3500 mW
Max Power Power Down   = 1500 mW
Max current +5V        = 350 mA
Max current +3V3       = 400 mA
Max current +1V8       = 800 mA
Max current -5V2       = 0 mA
Diagnostic Monitoring  = No BER Support
Received Power         = Average Power
Enhanced Options       = Soft TX_DISABLE & Soft P_down
Auxiliary A/D Input 1  = Laser temperature
Auxiliary A/D Input 2  = +5V supply voltage

SEE>
```

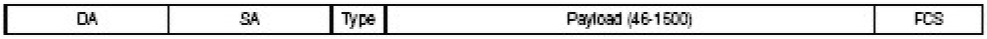
This page intentionally left blank.

Ethernet Frames

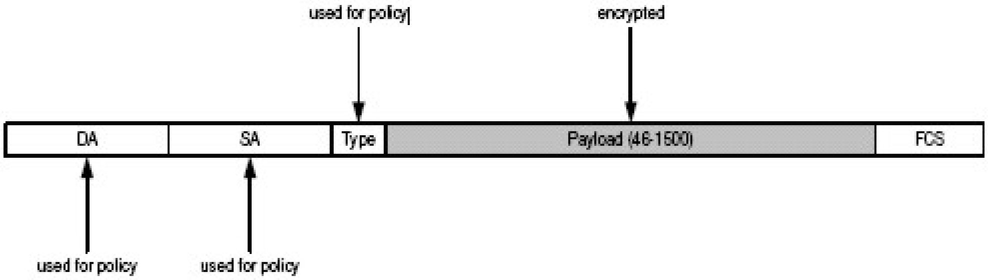
Ethernet II

The original and main Ethernet frame format is Ethernet (Version II), also known as DIX (Digital, Intel, and Xerox). Many higher level protocols such as TCP/IP and IPX use Ethernet II Type encapsulation.

This frame format is the most commonly used for data plane traffic. It is of the format:

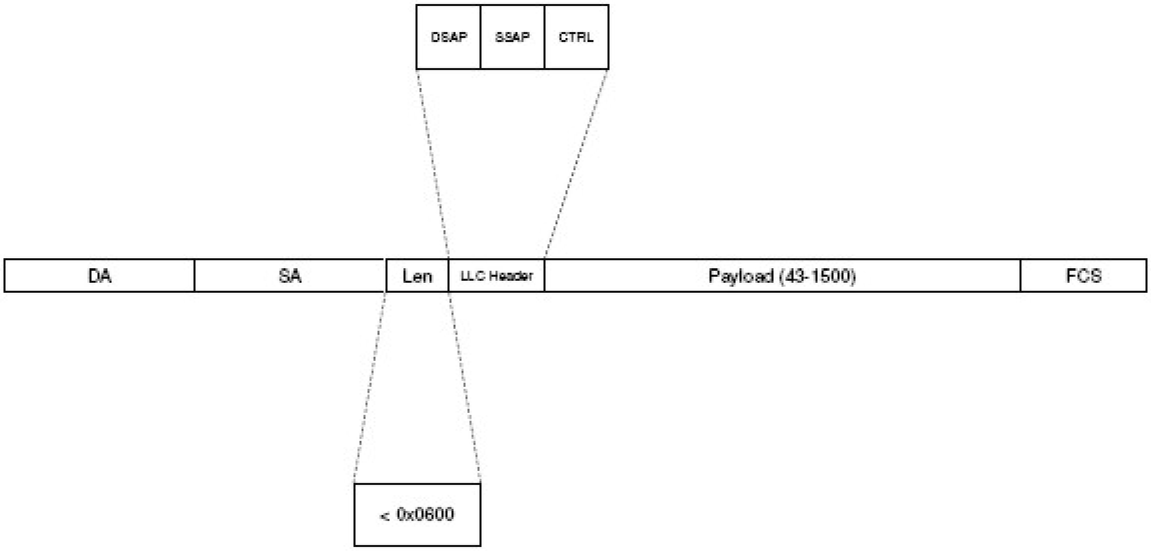


It is encrypted as follows:

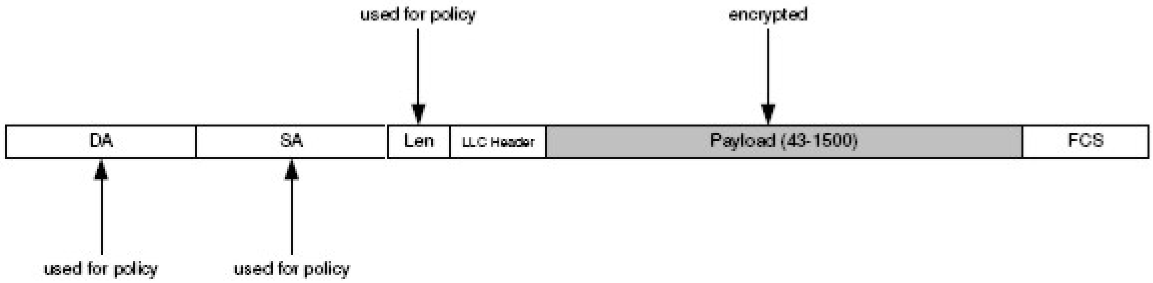


IEEE 802.3 SAP (with 802.2 LLC header)

In an IEEE 802.3 SAP (Service Access Point) frame, the ethertype field is replaced by a Length field and is then followed by an LLC (Logical Link Control) header which carries information about the type of protocol contained in the packet. The length field ranging 0x0000-0x05dc indicates the number of valid bytes in the payload. This frame format is the most commonly used for control plane traffic. The 802.3 SAP frame has this format:



It is encrypted as follows:

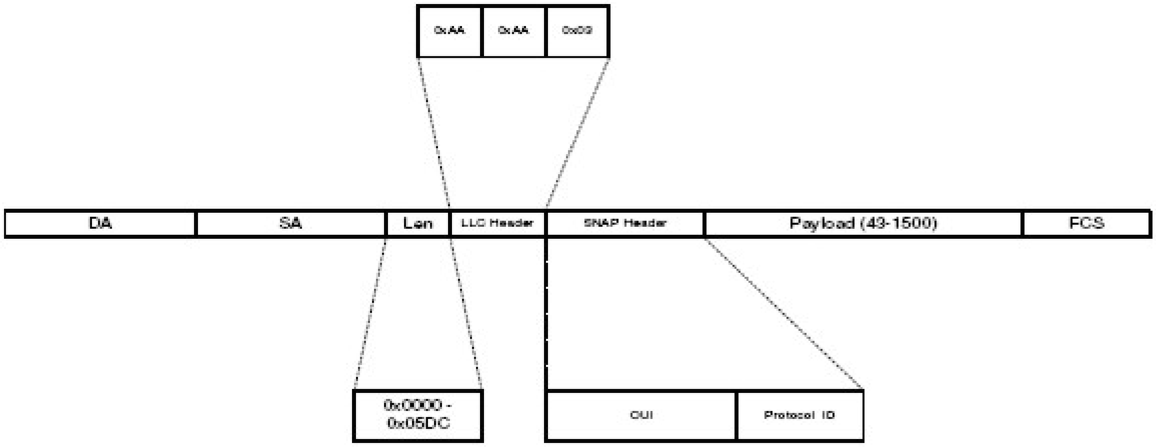


IEEE 802.3 SAP SNAP (with 802.2 LLC header and SNAP Header)

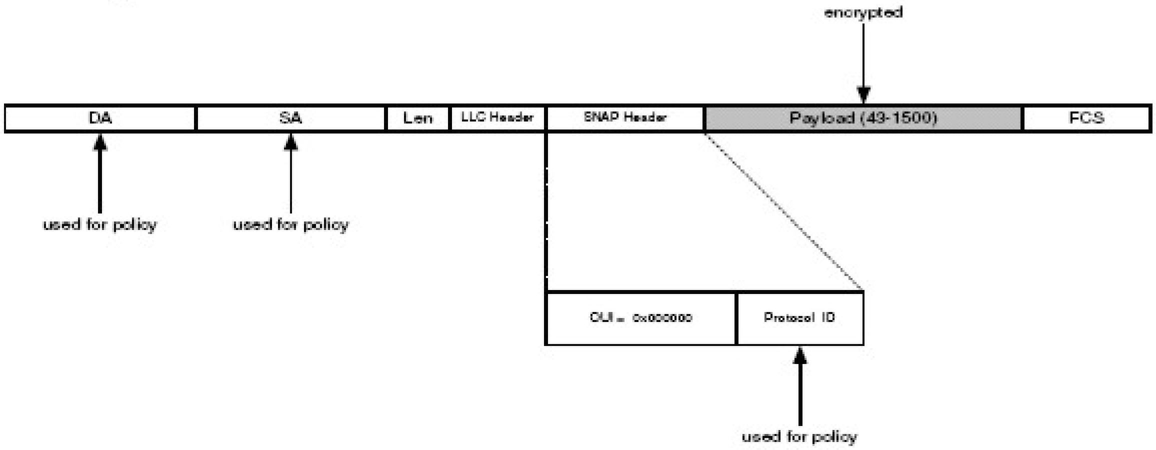
The IEEE 802.3 LLC SNAP format was defined to support a larger number of protocols than could be supported by the IEEE 802.3 SAP format. In the IEEE 802.3 SAP SNAP format, protocol is provided in an additional SNAP header Protocol ID field.

The SNAP OUI is an organizationally unique identifier. This allows different vendors to implement their own Ethernet protocol set. A special reserved OUI value of all zeros 0x000000 indicates that the SNAP Protocol ID (PID) is equivalent to the Ethernet Ethertype Type field values. Refer to RFC1024 for more details.

This frame format is the most commonly used for control plane traffic. The 802.3 SAP SNAP frame has this format:



It is encrypted as follows:



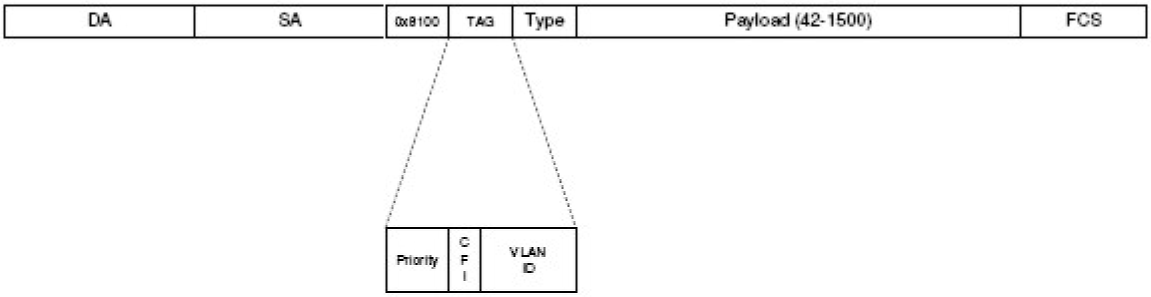
VLAN

A VLAN frame extension or tag can be inserted between the source address and the type/length field in any of the Ethernet frame types.

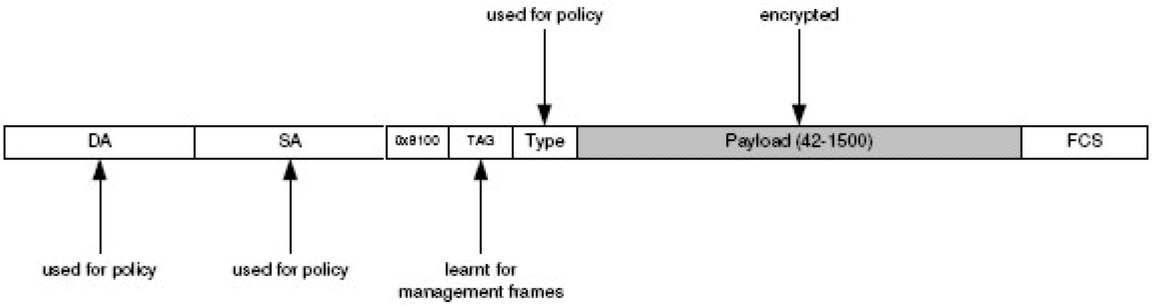
The VLAN tag consists of the following fields:

- User Priority
- Canonical Form Indicator
- VLAN Identifier

It is of the format:

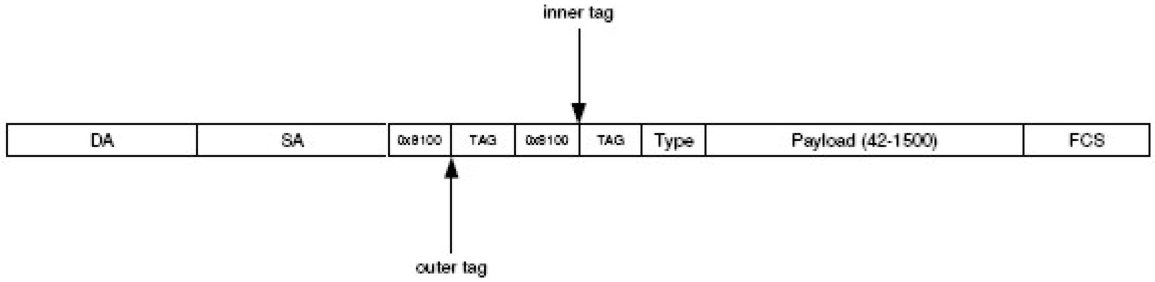


By default, the SEE is transparent to the configured primary and alternate VLAN ethertypes. It is encrypted as follows:



Stacked VLAN

Multiple VLAN tags can be inserted in an Ethernet frame. This is referred to as VLAN tag stacking. In an Ethernet-based DSL aggregation network, service providers can use two VLAN tags to allow for a larger number of customers to be aggregated. This is known as Q-in-Q, VLAN-in-VLAN, or double-tagging.



Frames consist of an inner tag and an outer tag.The inner VLAN tag is known as the customer or customer equipment VLAN, C-VLAN, CE-VLAN, or C-TAG. The inner tag is usually designated with an ethertype of 0x8100.

The outer VLAN tag is known as the service or service provider VLAN, S-VLAN, SP-VLAN, PE-VLAN, or S-TAG. The outer (service) VLAN tag is designated by a variety of ethertypes:

- 0x8100 - default used by Cisco
- 0x88A8 - default used by Extreme Networks
- 0x9100 - default used by Juniper
- 0x9200 - supported by several vendors

Most network devices have the ability to specify the value of the ethertype to designate the outer and sometimes inner tag.

Stacked 0x8100 VLANs

To allow traffic across the network correctly the encryptor automatically bypasses any detected VLAN tags. The Ethernet encryptor supports a maximum of 2 stacked VLAN tags.

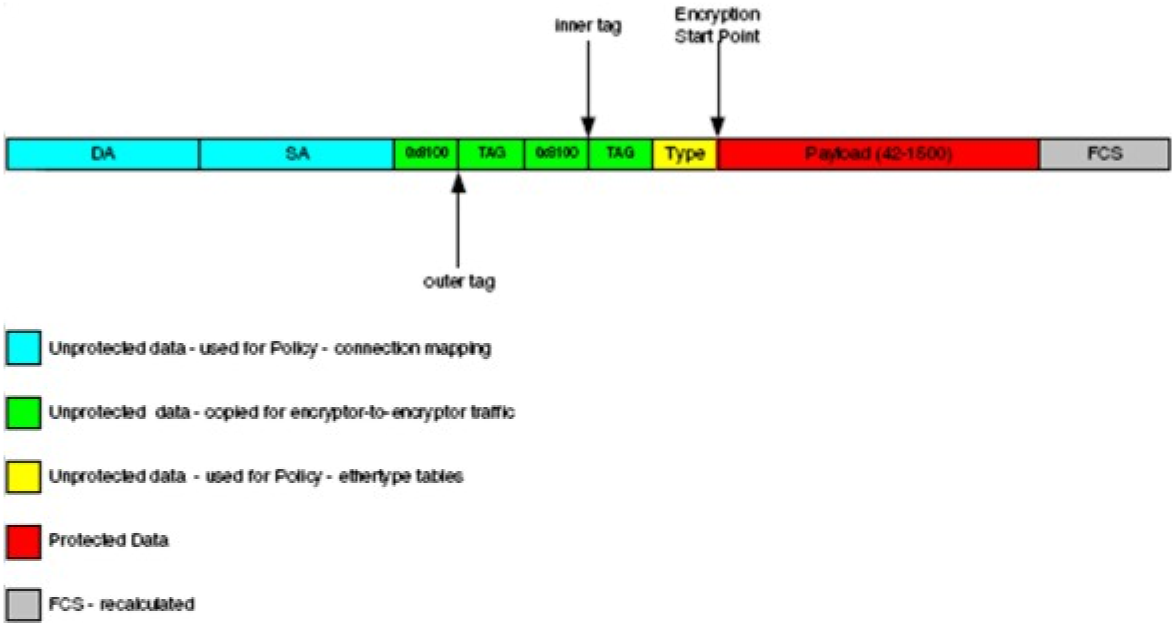
The default behavior of the encryptor is to start encryption after any detected VLAN tag(s). This feature is controlled by the VLAN header bypass feature which is enabled by default. Disabling this feature will start encryption directly after the first detected ethertype.

The encryptor automatically detects VLAN tag(s) via the configured primary and alternate VLAN ethertypes. See VLAN Command for additional information. The ethertype after the second VLAN tag is used for ethertype table policy.

For a particular connection the encryptor learns the VLAN tag(s). The learned tag(s) are pre-pended to encryptor management traffic. This is to ensure that management traffic reaches the remote encryptor. This feature is controlled by the auto-discovery feature which is enabled by default. If this feature is disabled, the VLAN tag(s) will not be learned.

Double to single tag exchange within the network is supported under default conditions. When double tag to single tag exchange occurs within the network it should not affect the encrypted data or the encryptor-to-encryptor management traffic. This is as long as the network applies the same policy to the encryptor-to-encryptor management traffic as it does to the normal network traffic.

In the following example, the Layer 2 payload is encrypted. The final type/length field is used for policy along with the destination and source MAC addresses. The VLAN tags are learned for use by encryptor-to-encryptor management traffic.


inner tag
Encryption Start Point
DA
SA
0x8100
TAG
0x8100
TAG
Type
Payload (42-1500)
FCS
outer tag
Unprotected data - used for Policy - connection mapping
Unprotected data - copied for encryptor-to-encryptor traffic
Unprotected data - used for Policy - ethertype tables
Protected Data
FCS - recalculated

If the default configuration has changed, type the following commands:

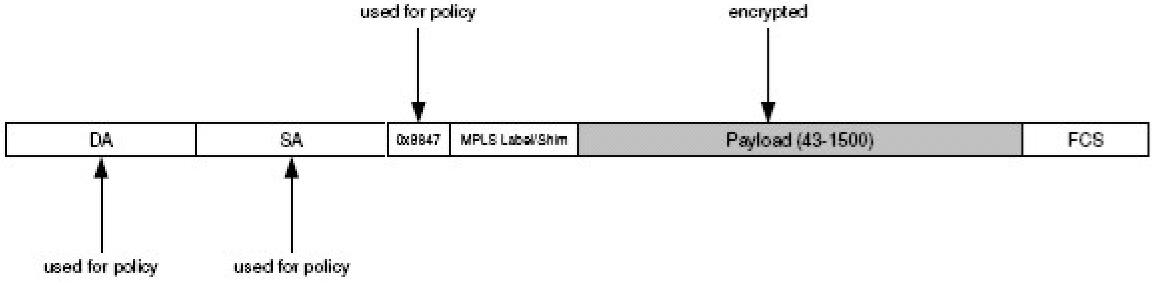
1. **vlan –p –e** to enable automatic VLAN header bypass
2. **autodisco -e** to enable auto-discovery

MPLS

MPLS uses labels to forward packets across the network (conventional network layer forwarding uses network protocol layer headers; that is, IP addresses) and is usually used for ‘class of service’ or traffic engineering purposes. Layer 2 Ethernet networks carry MPLS labels in shim headers, where shims/labels are added to an IP packet to route it through a switched network. The SEE is transparent to MPLS shims, and a maximum MPLS stack depth of 2 labels is supported.

The shim header is inserted between the link layer and the network layer. Ethernet uses values 0x8847 and 0x8848 to indicate the presence of a shim header. Ethertype value 0x8847 indicates that a frame is carrying an MPLS unicast packet and ethertype 0x8848 is used to indicate that a frame is carrying an MPLS multicast packet.

It is encrypted as follows:



This page intentionally left blank.

Maintenance

Replacing an AC Power Supply Module

Replacement power supply modules can be ordered from Technical Support.

When the LED on the power supply module is GREEN, the power supply is operating normally. When the LED is OFF, either the input AC voltage to the power supply module or the power supply module itself is in a fault or out-of-specification condition. If the input AC voltage is within specification, the power supply module must be replaced. To replace the power supply module, complete the following steps:

⚠ *The cover of the power supply module is used as a heat sink for cooling. Under full load conditions, the cover can reach temperatures from 120° to 140° F. Wear gloves to prevent injury.*

See Electrostatic Discharge for a statement on ESD management practices and potential hazards.

1. Remove the power cord from the power supply module being replaced.
2. Remove the retaining bar by unscrewing the screw on each end of the bar.
3. On the power supply module to be replaced, press the handle down and carefully remove the module. Set the module aside to cool off before disposal.
4. Insert the new power supply module into the power system.
5. Reinstall the retaining bar.
6. Plug the power cord into the power inlet on the new power supply module. When the power supply module is correctly installed the LED will turn green.

This page intentionally left blank.

Troubleshooting

Possible Problems and Solutions

The SafeNet Ethernet Encryptor does not contain any user serviceable parts and must be returned to the factory if repairs are necessary.

Category	Sympton	Explanation and Possible Solutions
LEDs	All LEDs are off.	▪ Make sure the power cable is attached and plugged in to both the device and the power outlet. ▪ Make sure that the power switch on the rear panel is turned on. ▪ The power outlet may not be functioning. Test this with other equipment. ▪ The SEE external fuse has failed. Replace the fuse with a 1.6A fast blow fuse. A spare fuse is shipped in the fuse holder. After replacing the fuse, if the new fuse fails when the unit is turned on or shortly thereafter contact SafeNet Technical Support. (This applies to devices with DC power supply modules only. There is not a user replaceable fuse on devices with AC power supply modules.)
	All LEDs are flashing.	All LEDs flashing after power-up indicates the SEE software has encountered a fatal condition. Contact SafeNet Customer Support.
	LEDs are flashing in sequential order.	The power-up self tests failed. The front panel LCD shows a 'system halted' error message. Contact SafeNet Customer Support. Unit will have to be returned.
	SYSTEM LED is red.	There is an error initializing the encryptor and it must be rebooted. If power cycling does not solve the problem contact SafeNet Customer Support.
	SYSTEM LED is off.	The encryptor is not functioning and must be rebooted. If power cycling does not solve the problem contact SafeNet Customer Support.
	LOCAL LED is solid red.	There is a loss of signal. The SFP/XFP is OK.
	LOCAL LED is off.	The SFP/XFP is not detected.
	NETWORK LED is solid red.	There is a loss of signal. The SFP/XFP is OK.
	NETWORK LED is off.	The SFP/XFP is not detected.
	ALARM LED is flashing amber or flashing red.	There are one or more unacknowledged alarms.
	ALARM LED is red.	There are one or more active, acknowledged alarms.
	TEMPERATURE LED is red.	The temperature is above 60° C. Contact SafeNet Customer Support.
	BATTERY LED is red.	The battery voltage is low. The battery is used for the tamper mechanism. If the battery dies and the power is interrupted the unit is tampered. Unit will have to be returned for battery replacement. Contact SafeNet Customer Support.
Log on	All administrator passwords are forgotten or lost.	Contact SafeNet Customer Support. Unit will have to be returned.

Category	**Sympton**	**Explanation and Possible Solutions**
	One of the administrator passwords is forgotten or lost.	Contact the network administrator for the SEE to reset the password.
	Not able to log in to the command line interface.	▪ Verify the password. Contact the device administrator to reset the password. ▪ Have the SMCII administrator connect to the device and reset the device's user password.
Configuration	The SEE and the SMCII are not communicating.	▪ Verify that an Ethernet cable is connected and properly seated in the 10/100 management port. ▪ Verify that the management port IP address is configured with the correct network. ▪ Check the management interface default gateway configuration. See the *Security Management Center II User's Guide*.
	The SEE's configuration has been erased with the **erase** command.	The flow of user data is disrupted until the SEE is reconfigured. To reconfigure the SEE, perform the following steps: 1. In SMCII, enter the default user and password. See Factory Default Parameters for the default values. 2. Follow the steps in "Configuring a Factory Delivered Unit" beginning with Loading a Certificate. The **erase** command does not reset the IP address to the factory default and does not require resetting.

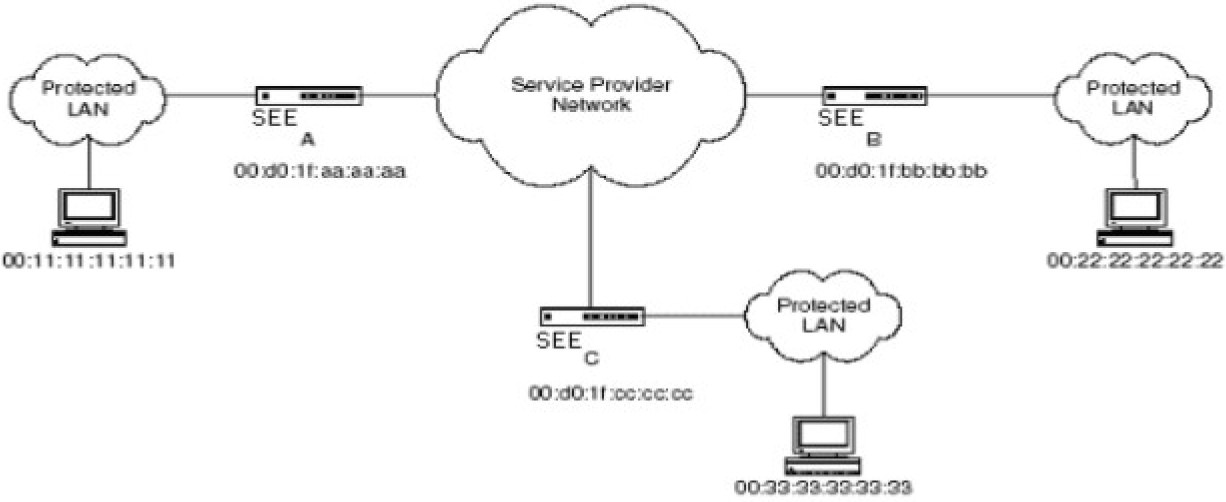
Power-up Self Tests Error Messages

The SEE performs power-up self tests to verify the integrity and correct operational functioning of the device. If the device fails a self test, it transitions to an error state and blocks all traffic on the data ports. Results from the power-up self tests are displayed on the LCD on the front panel. Information on the error messages displayed due to a failed self-test are listed in the table below.

Error Message	Class of Test	Test(s)
"Fatal system error Self-tests failed"	Software crypto failure	▪ 3DES_ENC_SW - Triple DES encryption, Software ▪ 3DES_DEC_SW - Triple DES decryption, Software ▪ DES_ENC_SW - DES encryption, Software ▪ DES_DEC_SW - DES decryption, Software ▪ RSA_PRIV_ENC - RSA Private Encryption ▪ RSA_PRIV_DEC - RSA Private Decryption ▪ RSA_PUB_ENC - RSA Public Encryption ▪ RSA_PUB_DEC - RSA Public Decryption ▪ SHA1 - SHA1 Hash ▪ SHA256 - SHA256 Hash ▪ RAND_BIT - Fail random bits ▪ RAND_POKER - Fail random poker
"SHA1 sw check failed System halted"	Software integrity check	▪ SW_INT

Network Troubleshooting

This section helps identify problems associated with unexpected behavior in the network that lies between the SafeNet Ethernet Encryptors using version 3.2.1 or greater. It will help the user determine if they have a true layer 2 Ethernet network or whether equipment in the network is observing or manipulating data in higher layers.



Ethernet Encryption Golden Rules

- The network between encryptors cannot modify the Ethernet MAC addresses.
- The network between encryptors may not discard frames based on L3 data (e.g., IP frame information) as this information is encrypted. Some layer 2 switches or network infrastructures may be designed to look at the IP portion of the header. If this is the case, an additional offset will be needed for the IP ethertype 0x0800. This offset can also be used when sniffing encrypted packets so the source and destination IP addresses are legible. See the *SMCII User's Guide* or this guide for modifying ethertype offsets.
- Transmission order MUST be preserved for line mode and multipoint MAC mode.
  QOS - this MUST not be between encryptors on the network side. QOS may reorder frames.
  L2 MPLS VPN - the MPLS control word MUST be enabled to guarantee transmission order.
- The network between encryptors cannot pass tag traffic with VLAN IDs to the encryptor network port that are not protected VLAN IDs on the local side of the encryptor.

Multipoint MAC Mode Considerations / Network Device

In multipoint mode, mutation is enabled by default, and as with line mode, the Injected NonMutant traffic is discarded. Having this set by default reduces the likelihood of network equipment interpreting packet data at higher layers (L3, IPv4 etc).

Note that in multipoint MAC mode (unlike line mode) the source and destination MAC pairs are observed, therefore no multicast traffic is considered part of the crypto-stream. Also note that the Pending tunnel (CI 1) is set to discard, and the ARP (0x806) EtherType is set to bypass for unicast traffic. This permits the successful operation of the auto-discovery process, while ensuring that unknown destination MAC address traffic is always discarded until secured by a remote encryptor.

Some multicast addresses are reserved and need to be bypassed by the encryptor to allow certain network protocols to function correctly. For example, protected OSPF routers will not get an OSPF full link state since multicast packets are discarded. Multicast traffic must be set to bypass for EtherType 0800, or Bypass Reserved Multicast Packets must be set to enable, when SEE devices are protecting routers with OSPF, or similar protocols deployed, to ensure proper link states between sites. See Bypass Reserved Multicast Addresses for the list of multicast addresses bypassed if the reserved multicast address bypass feature is enabled.

Encryptor Problems

The following configuration sequence should be performed on *each* encryptor, step by step. Between each step, check the end-to-end operation of the network for frame loss.

1. Ensure that the encryptors' configuration is set to the default condition.

   The following command causes an intentional reboot.

   SEE_A>**initcfg -a**

2. Ensure that Auto-Discovery is enabled.

   SEE_A>**autodisco -e**

3. Put the encryptors into bypass mode. (The default is either bypass or discard depending on the software version.)

   SEE_A>**global -b**

   Check the end-to-end operation of the network for frame loss. If no frame loss is present, proceed to the next step.

   If frame loss is present, there may be networking issues prior to the encryptors being inserted. All traffic should be bypassed so the encryptors behave as a bump in the wire.

4. For each ethertype, put all protocols into bypass as shown in the following example for ethertype 05ff. (The data displayed, default ethertypes, and the default values depend on the software version.)

```
SEE_A>ethertypes -e
Enter Ethertype [(O)ther, Value (Hex)]: 05ff
Encryption offset (hex): [0]
Offset Enable: <(Y)es | (N)o>: [No]
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Follow CI] B
Multicast Action: <(D)iscard | (B)ypass>: [Bypass]
Broadcast Action: <(D)iscard | (B)ypass>: [Bypass]
Edited Ethertype

SEE>ethertypes

           Offset Encryption
Ethertype  Enable Offset     Unicast   Multicast Broadcast
---------  ------ ---------- --------- --------- ---------
05ff       N      0          Bypass    Bypass    Bypass
0800       N      0          Bypass    Bypass    Bypass
0806       N      0          Bypass    Bypass    Bypass
Other      N      0          Bypass    Bypass    Bypass

4 Records in Ethertype table
```

5. Put the encryptors into secure mode.

```
SEE_A>global -e
```

6. Confirm that the tunnels are in the up state and that the addresses were learned correctly.

```
SEE_A>tunnels

Interface (tunnel/CI) MAC address  : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa

CI   Origin     Action   State    Peer Name        Remote Encryptor MAC
---- --------   -------- -------- ---------------- --------------------
0001 PENDING    Bypass   Up       N/A
0002 System     Discard  Up       N/A
0003 System     Bypass   Up       N/A
0004 Automatic  Secure   Up       SEE_B            00:d0:1f:bb:bb:bb

SEE_A>netmacs

Network Mac       CI
----------------- ----
00:d0:1f:bb:bb:bb 0004
00:22:22:22:22:22 0004
2 Valid records

SEE_A>locmacs

Local Mac
-----------------
00:11:11:11:11:11
1 Valid record
```

7. Enable the encryption offset for IPv4 (0x0800), set the encryption offset to 20 bytes, and set the unicast policy to FollowCI.

   Encryption offset is entered using its hex value.

```
SEE_A>ethertypes -e
Enter Ethertype [(O)ther, Value (Hex)]: 0800
Encryption offset (hex): [0] 14
Offset Enable: <(Y)es | (N)o>: [No] Y
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Bypass] F
Multicast Action: <(D)iscard | (B)ypass>: [Bypass]
Broadcast Action: <(D)iscard | (B)ypass>: [Bypass]
Edited Ethertype
```

```
SEE>ethertypes

           Offset Encryption
Ethertype  Enable Offset     Unicast   Multicast Broadcast
---------  ------ ---------- --------- --------- ---------
05ff       N      0          Bypass    Bypass    Bypass
0800       Y      14         UseCI     Bypass    Bypass
0806       N      0          Bypass    Bypass    Bypass
Other      N      0          Bypass    Bypass    Bypass


4 Records in Ethertype table
```

   Check the end-to-end operation of the network for frame loss. If no frame loss is present, proceed to the next step.

   If frame loss is present, a network element between the encryptors may be performing some policy based on layer 4 information. This is not expected behavior of a layer 2 service. Please contact your service provider.

8. Change the encryption offset to 12 bytes for IPv4 (0x0800).

   Encryption offset is entered using its hex value.

```
SEE_A>ethertypes -e
Enter Ethertype [(O)ther, Value (Hex)]: 0800
Encryption offset (hex): [14] c
Offset Enable: <(Y)es | (N)o>: [Yes]
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [FollowCI]
Multicast Action: <(D)iscard | (B)ypass>: [Bypass]
Broadcast Action: <(D)iscard | (B)ypass>: [Bypass]
Edited Ethertype
```

```
SEE>ethertypes

          Offset Encryption
Ethertype Enable Offset     Unicast   Multicast Broadcast
--------- ------ ---------- --------- --------- ---------
05ff      N      0          Bypass    Bypass    Bypass
0800      Y      c          UseCI     Bypass    Bypass
0806      N      0          Bypass    Bypass    Bypass
Other     N      0          Bypass    Bypass    Bypass

4 Records in Ethertype table
```

   Check the end-to-end operation of the network for frame loss. If no frame loss is present, proceed to the next step.

   If frame loss is present, a network element between the encryptors may be performing an IPv4 header checksum calculation. This is not expected behavior of a layer 2 service. Please contact your service provider.

9. Change the encryption offset to 0 bytes for IPv4 (0x0800).

```
SEE_A>ethertypes -e
Enter Ethertype [(O)ther, Value (Hex)]: 0800
Encryption offset (hex): [c] 0
Offset Enable: <(Y)es | (N)o>: [Yes]
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [FollowCI]
Multicast Action: <(D)iscard | (B)ypass>: [Bypass]
Broadcast Action: <(D)iscard | (B)ypass>: [Bypass]
Edited Ethertype
```

```
SEE>ethertypes
```

```
           Offset Encryption
Ethertype  Enable Offset     Unicast   Multicast Broadcast
---------  ------ ---------- --------- --------- ---------
05ff       N      0          Bypass    Bypass    Bypass
0800       N      0          UseCI     Bypass    Bypass
0806       N      0          Bypass    Bypass    Bypass
Other      N      0          Bypass    Bypass    Bypass

4 Records in Ethertype table
```

Check the end-to-end operation of the network for frame loss. If no frame loss is present, proceed to the next step.

If frame loss is present, a network element between the encryptors may be performing some form of IPv4 header parsing. This may be in the form of calculating the IPv4 header checksum, checking if the IPv4 header checksum is 0xffff and replacing it with 0x0000 or parsing the TOS (type of service) field under high network load conditions. This is not expected behavior of a layer 2 service. Please contact your service provider.

10. Enable the Other Ethertype. This will encrypt all other protocols.

```
SEE_A>ethertypes -e
Enter Ethertype [(O)ther, Value (Hex)]: O
Encryption offset (hex): [0]
Offset Enable: <(Y)es | (N)o>: [No]
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Bypass] F
Multicast Action: <(D)iscard | (B)ypass>: [Bypass]
Broadcast Action: <(D)iscard | (B)ypass>: [Bypass]
Edited Ethertype
```

```
SEE>ethertypes
```

```
           Offset Encryption
Ethertype  Enable Offset     Unicast   Multicast Broadcast
---------  ------ ---------- --------- --------- ---------
05ff       N      0          Bypass    Bypass    Bypass
0800       N      0          UseCI     Bypass    Bypass
0806       N      0          Bypass    Bypass    Bypass
Other      N      0          UseCI     Bypass    Bypass

4 Records in Ethertype table
```

Check the end-to-end operation of the network for frame loss.

If frame loss is present, a protocol other than IPv4 is interrupting the encryption stream. It is recommended to contact the network architect or to 'sniff' your network traffic to understand what other protocols are being used.

Test Modes

Line Mode

- Traffic should not be injected into the crypto stream (stp, cdp etc.). These must be set to bypass or discard in order to remove the identified traffic from the crypto stream.
- The resolution of policy is by ethertype only. If a particular ethertype is being injected into the network and the same ethertype is being run over the link, the device would be unable to differentiate between the frames and it would loose crypto sync.
- Re-ordering (QoS, etc.) between the encryptors is not allowed.
- To avoid STP issues in line mode, 05ff multicast must be set to discard or bypass.
- It may be necessary to set the offset to 20 bytes for ethertype 0800.

Testing Line Mode

Network testing is performed using the **initcfg** command test levels. The test levels are explained in the Initcfg Command topic.

Mutation is enabled by default in line mode. Consequently, the non-mutant action becomes relevant and is set to discard. Mutation protects against the inspection of known traffic types by network equipment in the encrypted segment. This prevents the potential for the network to drop what it considers are corrupted packets at Layer 3 and above. Discarding non-mutant values ensures that traffic injected in the encrypted segment of the network will be discarded by the encryptor. If this is not set to discard, it is possible to corrupt the crypto-stream and observe occasional packet corruption.

To test the line mode configuration, perform the following steps:

1. Enable line mode by typing the **line -e** command.
2. Verify the line mode defaults by typing the **ethertypes** command. (This command is optional.)
3. Verify the policy settings by typing the **policy** command. (This command is optional.)
4. Run test level 1 by typing the **initcfg -1** command.
5. Review the Ethertypes table by typing the **ethertypes** command.
6. Review the policy settings by typing the **policy** command.
7. Set the encryptor to secure data by typing the **global -e** command.
8. Run test levels 2 through 4 by typing the **initcfg -***N* command. After running each test level, review the policy settings by typing the **policy** command and review the Ethertypes table by typing the **ethertypes** command.

Multipoint Mode

- Re-ordering (QoS, etc.) between the encryptors is not allowed.

Testing Multipoint Mode

Network testing is performed using the **initcfg** command test levels. The test levels are explained in the Initcfg Command topic.

In multipoint mode, mutation is enabled by default. As with line mode the Injected NonMutant traffic is discarded. Having this set by default reduces the likelihood of network equipment interpreting packet data at higher layers (L3 IPv4, etc).

The Pending tunnel (CI 1) is set to discard, and the ARP (0x806) ethertype is set to bypass for unicast traffic. This permits the successful operation of the auto-discovery process, while ensuring that unknown destination MAC address traffic is always discarded until secured by a remote encryptor.

To test the multipoint mode configuration, perform the following steps:

1. Verify the encryptor is in the default state by typing the **initcfg-a** command.
2. Verify the Connection Identifier table by typing the **tunnels** command. (This command is optional.)
3. Verify the multipoint mode defaults by typing the **ethertypes** command. (This command is optional.)
4. Run test level 1 by typing the **initcfg -1** command.
5. Review the Connection Identifier table by typing the **tunnels** command.
6. Review the Ethertypes table by typing the **ethertypes** command.
7. Run test level 2 by typing the **initcfg -2** command.
8. Review the Connection Identifier table by typing the **tunnels** command.
9. Review the Ethertypes table by typing the **ethertypes** command.

Technical Support Information

When gathering system details for Technical Support, be sure to include the output of the following commands:

- history
- help
- version
- certificate
- linkspeed
- autodisco
- vlan
- policy
- ethertypes
- tunnels
- alarm
- audit
- event

For a complete list of commands, see the "Command Reference" book or the Help Command.

Alarms and Traps

The SafeNet Encryptor devices share common definitions for alarm and traps, which are listed in the following tables.

The majority of alarms are covered by a single alarmRaised trap, containing the following alarm ID and associated text with the format ‘Alarm set + text’. Unless explicitly stated when alarms are cleared a trap is also generated with the text: ‘Alarm cleared + text’ as shown below.

Some newer alarm definitions have unique traps defined for each alarm as outlined in the next table. All traps generated from the encryptor are sent in the clear. The SNMP agent sends a generic COLD START trap on power-up. For information on managing trap destinations, see the *Security Management Center II User’s Guide.*

The following traps are alarms that are forwarded to trap managers contained in the trap destination list. These traps are sent as SNMPv2 traps when an alarm condition is set. These traps are resent every 0.5 seconds while an alarm is active and not acknowledged. The table below lists the id number, message, and name.

OID: 1.3.6.1.4.1.3534.3.1.1.3.1.1
alarmRaised NOTIFICATION-TYPE
OBJECTS { sysLocalTime, sysAlarmDescr }
"An alarm was raised by the encryptor."

ID Number	Message	Name
000	System temperature alarm	ALARM_SYS_TEMP
001	System battery low warning	ALARM_RTC_BATTERY
002	Configuration battery low warning	ALARM_SRAM_BATTERY
003	System noise source failure	ALARM_SYS_NOISE
004	Local link down	ALARM_LOCAL_LINK (set)
004	Local link up	ALARM_LOCAL_LINK (cleared)
005	Network link down	ALARM_NETWORK_LINK (set)
005	Network link up	ALARM_NETWORK_LINK (cleared)
006	Invalid certificate alarm	ALARM_INVALID_CERTIFICATE
007	System power-up tests failed	ALARM_SELF_TESTS_FAILED
008	System log is full	ALARM_SYSTEM_LOG_FULL
009	Audit log is full	ALARM_AUDIT_LOG_FULL
010	Local interface loss of signal	ALARM_LOCAL_LOS
011	Local interface loss of frame	ALARM_LOCAL_LOF
012	Local interface loss of cell delineation	ALARM_LOCAL_LCD
013	Local interface AIS	ALARM_LOCAL_AIS
014	Local interface FERF	ALARM_LOCAL_FERF
015	Local interface RAI (Yellow)	ALARM_LOCAL_RAI
016	Local interface line RDI	ALARM_SONET_LOCAL_LINE_RDI
017	Local interface line AIS	ALARM_SONET_LOCAL_LINE_AIS
018	Local interface path RDI	ALARM_SONET_LOCAL_PATH_RDI
019	Local interface path AIS	ALARM_SONET_LOCAL_PATH_AIS
020	Network interface loss of cell delineation	ALARM_NETWORK_LCD

ID Number	Message	Name
021	Network interface AIS	ALARM_NETWORK_AIS
022	Network interface FERF	ALARM_NETWORK_FERF
023	Network interface RAI (Yellow)	ALARM_NETWORK_RAI
024	Network interface loss of signal	ALARM_NETWORK_LOS
025	Network interface loss of frame	ALARM_NETWORK_LOF
026	Network interface line RDI	ALARM_SONET_NETWORK_LINE_RDI
027	Network interface line AIS	ALARM_SONET_NETWORK_LINE_AIS
028	Network interface path RDI	ALARM_SONET_NETWORK_PATH_RDI
029	Network interface path AIS	ALARM_SONET_NETWORK_PATH_AIS
030	Transmit Underrun	ALARM_TRANSMIT_UNDERRUN
031	WARNING - Certificate will expire in less than 28 days	ALARM_CERT_EXPIRES_IN_28_DAYS
032	WARNING - Certificate will expire in less than 21 days	ALARM_CERT_EXPIRES_IN_21_DAYS
033	WARNING - Certificate will expire in less than 14 days	ALARM_CERT_EXPIRES_IN_14_DAYS
034	WARNING - Certificate will expire in less than 7 days	ALARM_CERT_EXPIRES_IN_7_DAYS
035	WARNING - Certificate will expire in less than 6 days	ALARM_CERT_EXPIRES_IN_6_DAYS
036	WARNING - Certificate will expire in less than 5 days	ALARM_CERT_EXPIRES_IN_5_DAYS
037	WARNING - Certificate will expire in less than 4 days	ALARM_CERT_EXPIRES_IN_4_DAYS
038	WARNING - Certificate will expire in less than 3 days	ALARM_CERT_EXPIRES_IN_3_DAYS
039	WARNING - Certificate will expire in less than 2 days	ALARM_CERT_EXPIRES_IN_2_DAYS
040	WARNING - Certificate will expire in less than 24 hours	ALARM_CERT_EXPIRES_IN_24_HOURS
041	Certificate has expired and is no longer valid	ALARM_CERT_EXPIRED
042	Power supply A (Top) not present	ALARM_TOP_POWER_REMOVED
043	Power supply A (Top) failure (3V3 rail)	ALARM_TOP_3V3_RAIL_FAIL
044	Power supply A (Top) failure (5V rail)	ALARM_TOP_5V0_RAIL_FAIL
045	Power supply A (Top) failure (12V rail)	ALARM_TOP_12V_RAIL_FAIL
046	Power supply A (Top) 48 volt supply not present	ALARM_TOP_48V_RAIL_FAIL
047	Power supply A (Top) alarm - exceed temperature limit	ALARM_TOP_TMP_FAIL
048	Power supply B (Bottom) not present	ALARM_BOT_POWER_REMOVED
049	Power supply B (Bottom) failure (3V3 rail)	ALARM_BOT_3V3_RAIL_FAIL
050	Power supply B (Bottom) failure (5V rail)	ALARM_BOT_5V0_RAIL_FAIL
051	Power supply B (Bottom) failure (12V rail)	ALARM_BOT_12V_RAIL_FAIL
052	Power supply B (Bottom) 48 volt supply not present	ALARM_BOT_48V_RAIL_FAIL
053	Power supply B (Bottom) alarm - exceed temperature limit	ALARM_BOT_TMP_FAIL
054	Interface FPGA alarm - exceed temperature limit	ALARM_FPGA_TMP_FAIL

ID Number	Message	Name
055	FPGA datapath reset	ALARM_FPGA_DATAPATH_RESET
056	Encryptor link is down	ALARM_LINK
057	Local link down due to Link Loss Forwarding (LLF)	ALARM_LOCAL_LLF (set)
057	Local link recovered from LLF	ALARM_LOCAL_LLF (cleared)
058	Network link down due to Link Loss Forwarding (LLF)	ALARM_NETWORK_LLF (cleared)
058	Network link recovered from LLF	ALARM_NETWORK_LLF (cleared)
059	Encryptor converted to QKD Failure Mode	ALARM_QKD_FAIL (set)
059	Encryptor recovered from QKD Failure Mode	ALARM_QKD_FAIL (cleared)
060	WARNING – Default user credentials detected	ALARM_DEFAULT_USER
061	WARNING: V2 Certificate required for group key encryption (Multicast/VLAN)	ALARM_V2_CERT_REQUIRED
062	Power supply removed, turned off or faulty	ALARM_POWER_REMOVED

The following traps are sent as SNMPv2 traps with an Enterprise trap object identifier (OID) 1.3.6.1.4.1.3534.3.1.1.3.1.

OID	Message	Name
1.3.6.1.4.1.3534.3.1.1.3.1.2	Link Up condition detected on network port.	eventNetworkLinkUp
1.3.6.1.4.1.3534.3.1.1.3.1.3	Link Down condition detected on network port.	eventNetworkLinkDown
1.3.6.1.4.1.3534.3.1.1.3.1.4	Link Up condition detected on local port.	eventLocalLinkUp
1.3.6.1.4.1.3534.3.1.1.3.1.5	Link Down condition detected on local port.	eventLocalLinkDown
1.3.6.1.4.1.3534.3.1.1.3.1.6	Encryptor Link is Up (signifies both local and network ports are up).	eventEncryptorLinkUp
1.3.6.1.4.1.3534.3.1.1.3.1.7	Encryptor Link is Down (signifies one or both of the local or network ports is down).	eventEncryptorLinkDown
1.3.6.1.4.1.3534.3.1.1.3.1.8	A successful login has occured on the CLI for the encryptor.	eventLogIn
1.3.6.1.4.1.3534.3.1.1.3.1.9	A user has logged out of the CLI interface on this encryptor.	eventLogOut
1.3.6.1.4.1.3534.3.1.1.3.1.10	A failed attempt to log in to the CLI interface on this encryptor. A failed attempt is classified as three successive failed login attempts.	alarmLogInFailed
1.3.6.1.4.1.3534.3.1.1.3.1.11	A unit cold start has occurred. *The standard net-snmp coldstart trap will be received in addition to the coldstart or warmstart traps listed in this table. This net-snmp trap should be ignored as it relates to the SNMP stack state and not the platform state.*	eventColdStart
1.3.6.1.4.1.3534.3.1.1.3.1.12	A warmstart has occurred. Typically requested from a CLI or SNMP operation.	eventWarmStart
1.3.6.1.4.1.3534.3.1.1.3.1.15	Includes the OID of the certificateDaysLeft for the relevant certificate.	certificateExpiry
1.3.6.1.4.1.3534.3.1.1.3.1.16	Notification of a change in the FIPS mode, including the new fipsMode.	fipsModeChange

Event Messages

A list of all the event log messages is contained in the table below.

Message
$file Authenticated OK
<*device-name*> : Failed to achieve key update (restarting)
2nd upgrade stopped (upgrade already running)
Alarm set: WARNING: V2 Certificate required for group key encryption (Multicast/VLAN)
AES Engine self-test FAILED
AES128 Decrypt self-test FAILED
AES128 Decrypt self-test passed
AES128 Encrypt self-test FAILED
AES128 Encrypt self-test passed
AES256 Decrypt self-test FAILED
AES256 Decrypt self-test passed
AES256 Encrypt self-test FAILED
AES256 Encrypt self-test passed
Alarm set | cleared: <Alarm message>
Assumed master of group <*group id*> and will distribute keys using certificate #2 only.
Authenticating/Decrypting $file
Certificate is not current
Certificate load – Admin account information required
Certificate load - encryptor not in certificate mode
Certificate load - received public key doesn't match that sent
Certificate load - received signature not valid
Certificate load - received unknown digest type
Certificate load - rsa decrypt error
Configuring Hardware Crypto Passed
Crypto Pre load test
DES168 (3 key) Decrypt self-test FAILED
DES168 (3 key) Decrypt self-test passed
DES168 (3 key) Encrypt self-test FAILED
DES168 (3 key) Encrypt self-test passed
Detected card removal
Detected card removal or unit erase operation
Event log was corrupt and had to be recreated

Message
Extracting files from $file.
Failure destroying Master Keys
Failure Generating System Master Key
Failure migrating System Master Key
Failure migrating User CSPs
Failure opening master key device(s)
Forced password lexical checking on
FPGA Firmware Integrity self-test FAILED
FPGA Firmware Integrity self-test passed
FW Crypto Selftest Failed.
FW Crypto Selftest Passed.
Generated New System Master Key
Hardware Random Noise Generator self-test FAILED
Hardware Random Noise Generator self-test passed
Hardware Random statistical check FAILED
Hardware Random statistical check passed
HMAC-SHA1 self-test FAILED
HMAC-SHA1 self-test passed
HMAC-SHA256 self-test FAILED
HMAC-SHA256 self-test passed
Joined group <*group id*> and exchanged group key using certificate #2.
Line ACK not authenticated
Logged into console: <User ID>
Logged out of console: <User ID>
No RTC battery
Password failed lexical check
Retrieving file $IMAGE_NAME
RSA Engine self-test FAILED
RSA key pair consistency FAILED
RSA key pair consistency passed
RSA-1024 Private Key Decrypt self-test FAILED
RSA-1024 Private Key Decrypt self-test passed
RSA-1024 Private Key Encrypt self-test FAILED
RSA-1024 Private Key Encrypt self-test passed
RSA-1024 Public Key Decrypt self-test FAILED

Message
RSA-1024 Public Key Decrypt self-test passed
RSA-1024 Public Key Encrypt self-test FAILED
RSA-1024 Public Key Encrypt self-test passed
Self-tests FAILED
Self-tests passed
Session established
Session FAILED - address compression failure
Session FAILED - address overlaps existing connection
Session FAILED - Certificate version mismatch
Session FAILED - hash algorithm mismatch
Session FAILED - No V1 certificate loaded
Session FAILED - No V2 certificate loaded
Session FAILED - received certificate is not current
Session FAILED - remote CA authentication failure on flow 1
Session FAILED - remote CA authentication failure on flow 2
Session FAILED - signature algorithm mismatch
Session FAILED - this unit's certificate is not current
Session key update received
Session key update sent
SHA-1 self-test FAILED
SHA-1 self-test passed
SHA-256 self-test FAILED
SHA-256 self-test passed
Software Integrity self-test FAILED
Software Integrity self-test passed
STP monitoring removing local MAC entries"
System manual shutdown
System Power Up
System started
System startup (warmstart | coldstart)
Upgrade successful.
User account expired due to inactivity:
User account information is weak – Rejected
X9.31 Random Number Generator self-test FAILED
X9.31 Random Number Generator self-test passed

Audit Messages

A list of all the audit log messages is contained in the table below.

Message
<user>: Auto session discovery changed: Multicast/VLAN ENABLED
<user>: Auto session discovery changed: Multicast/VLAN DISABLED
<user>: CI/Tunnel Keyupdate interval changed to <num> minutes
<user>: Configuration: VLAN alternate ethertype changed to <value>
<user>: Configuration: VLAN Primary ethertype changed to <value>
<user>: Global Connection mode changed to VLAN Connection Mode.
<user>: Inband management VLAN tag change request - added <entry> <value>
<user>: Inband management VLAN tag change request - changed <entry> to <value>
<user>: Inband management VLAN tag change request - deleted <entry>
<user>: MAC change Notification. No space to add new MAC entry
<user>: New SNMP trap destination added: index <index>, <IP address>, <enabled | disabled>
<user>: Password enhanced mode: disabled
<user>: Password enhanced mode: enabled
<user>: Password failed reuse history check - Authentication Password
<user>: Password minimum numerical characters: <value>
<user>: Trap destination deleted: index <index>, <IP address>, <enabled | disabled>
Account inactive timeout period set to <timeout-period >
Acknowledged active alarm : <alarm-description>
Acknowledged inactive alarm : <alarm-description>
Alarm trap period set to <timeout-period>
Audit log was corrupt and had to be recreated
Audit log wrapping disabled
Audit log wrapping enabled
Auto session discovery changed: DISABLED
Auto session discovery changed: ENABLED
Bypass of reserved Multicast changed to DISABLED
Bypass of reserved Multicast changed to ENABLED
Certificate authenticate failure : <certificate-info>
Certificate loaded by user
Cleared audit log
Cleared system log
CLI prompt set to <prompt>

Message
Configuration: CI table Error. Default Entries not found.
Configuration: CI table Error. Default line mode entry not found.
Configuration: CI table Re-Initialized.
Configuration: Global settings reset to default
Configuration: Global vars and EtherType table Re-Initialized.
Configuration: Local Link monitoring forcing unit into Discard on LinkDown.
Configuration: MAC table Re-Initialized.
Configuration: MPLS alternate ethertype changed to <mpls-alt>
Configuration: VLAN alternate ethertype changed to <vlan-alt>
Configuration Reset and Reboot executed: Ethernet global settings reset to default
Configuration Reset and Reboot executed: Ethernet settings reset to defaults.
Configuration Reset and Reboot executed: Ethernet settings set to Test (Level 1)
Configuration Reset and Reboot executed: Ethernet settings set to Test (Level 2)
Configuration Reset and Reboot executed: Ethernet settings set to Test (Level 3)
Configuration Reset and Reboot executed: Ethernet settings set to Test (Level 4)
Configuration Reset and Reboot executed: Ethernet Tunnel/CI and MAC settings reset to defaults
Configuration Reset and Reboot executed: Ethernet Tunnel/CI and MAC settings reset to defaults for line mode
Connection started : <session-info>
Connection stopped : <session-info>
Ethertype default broadcast action changed: BYPASS
Ethertype default broadcast action changed: DISCARD
Ethertype default broadcast action changed: FOLLOW CI
Ethertype default broadcast action changed: unknown
Ethertype default multicast action changed: BYPASS
Ethertype default multicast action changed: DISCARD
Ethertype default multicast action changed: FOLLOW CI
Ethertype default multicast action changed: unknown
Ethertype default offset usage changed: IGNORE OFFSET
Ethertype default offset usage changed: USE OFFSET
Ethertype default unicast action changed: BYPASS
Ethertype default unicast action changed: DISCARD
Ethertype default unicast action changed: FOLLOW CI
Ethertype default unicast action changed: unknown
Ethertype Entry Added. <eth-type-info>
Ethertype Entry Deleted. <eth-type-info>

Message
Ethertype Entry Edited. <eth-type-info>
Ethertype Notification. Illegal broadcast ethertype action. Must be discard or bypass
Ethertype Notification. Illegal multicast ethertype action. Must be discard or bypass
Ethertype Notification. Mutation to value 0xFCOF is reserved and maynot be used!
Ethertype Notification. No space to add new Ethertype
Gateway address set : <sys-ip-gateway>
Global Crypto mode changed: Algorithm = AES; Mode = CFB; Key Length = 256.
Global Crypto mode changed: Algorithm = AES; Mode = CTR; Key Length = 256.
Global mode changed: BYPASS
Global mode changed: BYPASS - no certificate
Global mode changed: DISCARD
Global mode changed: DISCARD - no certificate
Global mode changed: SECURE-MULTI
Inband gateway enable set to disabled
Inband gateway enable set to enabled
Inband Gateway IP address set to <inband-gateway-ip-address>
Inband IP address set to <inband-ip-address>
Inband management disabled
Inband management enabled
Inband management VLAN tagging disabled
Inband management VLAN tagging enabled
Inband management VLAN tag set to <vlan_hdr>
Inband network IP mask set to : <inband-ip-mask>
Interface corrected HCS error count cleared
Interface uncorrected HCS error count cleared
Interframe gap changed: REPEATER
Interframe gap changed: STANDARD
IP address set : <sys-ip-address>
Keypad disabled
Keypad enabled
Led test mode disabled
Led test mode enabled
Line mode changed: DISABLED
Line mode changed: ENABLED
Link configuration changed:

Message
Link configuration on local port changed:
Link configuration on network port changed:
Link control changed: Failed - requested non achievable linkspeed!
Link control changed: Link Autonegotiation DISABLED
Link control changed: Link Autonegotiation ENABLED
Link control changed: Link configuration change
Link Loss Forwarding changed to Bidirectional
Link Loss Forwarding changed to Disabled
Link Loss Forwarding changed to Local port
Link Loss Forwarding changed to Network port
Link Loss Forwarding changed to unknown
LLF on connection status (line mode) is disabled
LLF on connection status (line mode) is enabled
Local Link monitoring changed: DISABLED
Local Link monitoring changed: ENABLED
Local Time set to : <date-and-time>
MAC Address Entry Added. <mac-info>
MAC Address Entry Deleted. <mac-info>
MAC Address Entry Edited. <mac-info>
MAC change Notification. Cannot delete MAC belonging to Encryptor. Delete Tunnel to remove entry
MAC change Notification. Cannot edit MAC address for record. Delete and add new record.
MAC change Notification. Cannot manually add MAC records to pending tunnel.
MAC change Notification. Can only re-assign tunnel for netmac pending entries.
MAC change Notification. Failed to delete existing MAC address from pending tunnel
MAC change Notification. Illegal request to add remote MAC to Pending Tunnel!
MAC change Notification. Illegal request to assign MAC to non-existant tunnel
MAC change Notification. Illegal request to move remote MAC to non-existant tunnel
MAC change Notification. Illegal request to move remote MAC to Pending Tunnel
MAC change Notification. Local MAC table flushed
MAC change Notification. MAC table add failed. MAC already exists in Local MAC table: <mac-info>
MAC change Notification. MAC table add failed. MAC already exists in Network MAC table: <macinfo>
MAC change Notification. MAC table add failed. MAC already exists in Network (Pending) MAC table: <mac-info>
MAC change Notification. MAC table edit failed. MAC already exists in Local MAC table: <mac-info>
MAC change Notification. MAC table edit failed. MAC already exists in Network (Pending) MAC table: <mac-info>
MAC change Notification. MAC table edit failed. MAC already exists in Remote MAC table: <mac-info>

Message
MAC change Notification. Network MAC table flushed
MAC change Notification. Network MAC table flushed [for CI <ci>]
MAC change Notification. No space to add new MAC entry
Management session inactive timeout period set to <timeout-period >
Manual reboot issued
Manual reboot issued : mode: erase & restart
Manual reboot issued : mode: halt
Manual reboot issued : mode: restart
MPLS bypass changed: DISABLED
MPLS bypass changed: ENABLED
Network IP mask set : <sys-ip-netmask>
New certificate received from CA
New certificate requested
New MAC processing changed: BYPASS
New MAC processing changed: DISCARD
Number of stacked VLAN id(s) Notification. Entries exist in the Vlan Tunnels table, unable to change vlan stacked setting
Observe Pending action on ingress changed to DISABLED
Observe Pending action on ingress changed to ENABLED
Password lexical checking disabled
Password lexical checking enabled
Password reuse history size set to <reuse-size>
Session added : <session-info>
Session deleted : <session-info>
Session edited : <session-info>
Shim insertion rate changed to <xxx>
Shim MTU overflow prevention change to <xxx>
SNAP observe PID as ethertype changed: DISABLED
SNAP observe PID as ethertype changed: ENABLED
SNMP Privacy Mode has been [enabled|disabled]
SNMP V1 read only access disabled
SNMP V1 read only access enabled
STP monitoring changed to DISABLED
STP monitoring changed to ENABLED
System log wrapping disabled
System log wrapping enabled

Message
Three failed login attempts - console locked
Trap handler address set to <trap-handler-address>
Tunnel (CI) Entry Added. <enet-ci-info>
Tunnel (CI) Entry Deleted. <enet-ci-info>
Tunnel (CI) Entry Edited. <enet-ci-info>
Tunnel (CI) Entry Started. <enet-ci-info>
Tunnel (CI) Entry Stopped. <enet-ci-info>
Tunnel (CI) Notification. Cannot add more tunnels in line mode!
Tunnel (CI) Notification. Cannot delete System or System Pending CI Entries
Tunnel (CI) Notification. Cannot delete tunnels in line mode!
Tunnel (CI) Notification. Cannot set SYSTEM tunnel action to encrypt!
Tunnel (CI) Notification. No space to add new tunnel
Tunnel (CI) Notification. Tunnel with remote MAC address already exists
Tunnel Keep Alive changed to DISABLED
Tunnel Keep Alive changed to ENABLED
Unit erased to factory default
USB Port Lock Status changed to [locked|unlocked]
User account added : <user-info>
User account deleted : <user-info>
User account edited : <user-info>
User account made inactive: <User ID>
Valid Certificate not loaded. Cannot change to secured mode.
VLAN header bypass changed: DISABLED
VLAN header bypass changed: ENABLED

This page intentionally left blank.

Specifications

System Features

Cryptography	▪ AES algorithm - 256 bit key ▪ Cipher Feedback (CFB) mode or Counter (CTR) mode (10 GbE device supports CTR mode only)
Interfaces	**FastEthernet** ▪ SFP electrical modules - 10/100/1000BASE-T RJ-45 **GbE** ▪ SFP electrical modules - 10/100/1000BASE-T RJ-45 ▪ SFP fiber modules: Single-mode - 1310 nm, Multi-mode - 850 nm **10 GbE** ▪ XFP Multi-Source Agreement (MSA) compliant fiber modules
Key Management	▪ RSA public key - supports key sizes of 1024 and 2048 bits ▪ Automatic session key update ▪ Authenticated using certificates
Management	▪ Serial: RS-232 ▪ Ethernet: 10/100 RJ-45 ▪ SNMPv3 using Diffie-Hellman Key Exchange with AES 128
Audit Support	▪ Alarm table ▪ Audit log recording secure connections and configuration changes ▪ Event log recording interface status
Network	▪ Ethernet II, IEEE 802.3 ▪ Jumbo frame support (up to 10,000 bytes) ▪ VLAN, MPLS transparency
Performance	**FastEthernet, GbE, and 10 GbE** ▪ Full-duplex operation ▪ Cut-through data streaming with partial processing for low latency vs. store and forward architecture ▪ Key change without interruption

Connections	**VLAN Mode** ▪ FastEthernet and GbE – 512 group connections minus the number of configured bypass MAC addresses ▪ 10 GbE – 64 group connections minus the number of configured bypass MAC addresses **MAC Mode** ▪ FastEthernet and GbE – 512 combined unicast tunnels and group connections ▪ 10 GbE – 64 combined unicast tunnels and group connections ▪ 3 tunnels reserved for system sessions *Due to MAC table and tunnel constraints on the 10 GbE device, multipoint topologies that include 10 GbE devices require that all SEE devices have only routers attached to their local ports when configured for multipoint MAC mode. This includes 1GbE devices in a multipoint topology with 10 GbE devices.*
Indicators	▪ Two line 20 character LCD ▪ LEDs indicating secure status, system operation, local interface, network interface, alarm status, temperature, battery status, and power ▪ LEDs for interface Tx/Rx
Physical Security	▪ Protected storage of encryption keys and user passwords ▪ Tamper resistant metal case
Accreditations	▪ Common Criteria EAL 4 (in process) ▪ FIPS PUB 140-2, Level 3 (in process)

Mechanical

FastEthernet and GbE	**Size**	Width: 17 inches; 432 millimeters Depth: 11.1 inches; 282 millimeters Height: 1.6 inches; 41 millimeters
	Weight	10 pounds; 4.5 kilograms
10 GbE	**Size**	Width: 17 inches; 432 millimeters Depth: 14 inches; 356 millimeters (with handles) Height: 5.1 inches; 130 millimeters
	Weight	19.9 pounds; 9.0 kilograms

Environmental

Operating temperature	5° C to 40° C
Operating humidity	20 to 80% RH @ 40° C operating temperature
Operating altitude	0 to 1980m AMSL

AC Power

FastEthernet, GbE, and 10 GbE	AC Power Input	100 V, 50 Hz 240 V, 60 Hz
	Power Consumption	115 watts
	Current Draw	1.1 amps at 120 VAC 0.85 amps at 240 VAC

DC Power

FastEthernet, GbE, and 10 GbE	DC Power Input	-40.5 to -72 VDC
	Power Consumption	40 watts
	Current Draw	0.83 amps at -48 VDC

Transceiver Specifications

FastEthernet and GbE

Electrical SFP Interface

- Line Frequency: 125 MHz
- Tx Output Impedance: 100 Ohm
- Rx Input Impedance: 100 Ohm

GbE

Optical Interfaces

- Shortwave - these lasers work with up to 500 meters of multi-mode fiber.
- Longwave - these lasers work with up to 5000 meters of single-mode fiber.

	Shortwave: 850 nm	**Longwave: 1310 nm**
Tx	Wavelength: 830 to 860 nm Power: -9 to -3 dBm	Wavelength: 1270 to 1360 nm Power: -5 to 0 dBm
Rx	Wavelength: 770 to 860 nm Power: -20 dBm	Wavelength: 1270 to 1600 nm Power: 0 to -22 dBm

10 GbE

XFP Support for 3U units

- The 10GbE optical interface has been designed to accept MSA compliant XFPs.
- The applicable standard for 10GbE optical devices is IEEE802.3ae.
- The 10GbE SEE was qualified with XFP optical devices that meet the standards in the following table.

	10GBase-LR	**10GBase-ER**
Wavelength	1310 nm	1550 nm
Tx	-8.2 to +0.5 dBm	-4.7 to +4 dBm
Rx	-14.4 to +0.5 dBm	-15.8 to -1 dBm

FIPS Mode Operation Guidance

Overview

This section provides information for crypto officers to install, configure, and operate the SafeNet Ethernet Encryptor (SEE) in FIPS mode.

There are two pertinent user groups for the SEE:

- **Crypto Officers** – One or more crypto officers will operate the SEE performing administrative operations. Details are provided in this document and the *Security Management Center II User's Guide*.
- **Network Users** – Multiple users may make use of the services of the SEE when sending data across the unsecured public network. However, users do not access the cryptographic services directly. Rather, two or more encryptors are used to establish secure connections across the unsecured public network, thus extending the reach and scope of the protected network. The encryptors provide services like key generation and encryption/decryption as needed based on their configuration. The cryptographic module is essentially transparent to the users.

Crypto officers are the only class of users that can modify any settings. Therefore, the guidance information in this section pertains only to crypto officers. This section does not provide guidance for users of the systems.

General Operation

The default device configuration has SNMPv3 privacy enabled and FIPS mode on. In this configuration, all SNMP management traffic between the device and the SMCII management application is AES encrypted. This protects any user account updates sent from SMCII to the device.

Because SNMPv3 privacy is an integral part of the device's FIPS mode operation, two steps are required to disable it. The device must first have FIPS mode disabled. Any attempt to disable SNMPv3 privacy without first disabling FIPS mode will result in a command error. Similarly, once privacy is disabled, FIPS mode cannot be re-enabled until after privacy is re-enabled.

Crypto Officer Guidance

On receiving the SEE, perform the following steps:

1. Inspect the encryptor for signs of tampering. Check that the tamper evident tape and the covers of the device do not show any signs of tampering. If tampering is detected, return the device to the manufacturer.
2. Inspect the label on the bottom of the SEE to ensure it is the correct FIPS approved version of the hardware. See the table below for the part numbers.

Do not install the encryptor if it shows signs of tampering or has an incorrect label. Contact your organization's security officer for instructions on how to proceed.

Part Number	Product Description
RoHS Compliant Systems	
943-51130-XXX	SEE, 100 MBPS, AES, V3.4, ROHS
943-51131-XXX	SEE, 100 MBPS, AES, V4.X, ROHS
943-51150-XXX	SEE, 1 GBPS, AES, V3.4, ROHS
943-51151-XXX	SEE, 1 GBPS, AES, V4.X, ROHS
943-53270-XXX	SEE, 10GBPS, AES, V3.4, ROHS
943-53271-XXX	SEE, 10GBPS, AES, V4.X, ROHS
943-53371-XXX	SEE, 10GBPS, AES, V4.X, ROHS

Part Number	Product Description
Legacy Systems	
943-10012-XXX	SEE, 100 MBPS, AES, V3.2, ROHS
943-10013-XXX	SEE, 1GBPS, AES, V3.2, ROHS
Legend for -XXX: -001: AC power -007: DC power -201: Dual AC power -207: Dual DC power	

See the NIST website for a list of current part numbers.

If the device does not show signs of tampering and has a correct label, proceed to Configuration.

Configuration

Configuration instructions are provided in “Configuring a Factory Delivered Unit.” Be sure to use the settings and steps provided in this section to constrain the configuration actions so that the device is not compromised during the configuration phase. This approach ensures the device boots properly and enters FIPS 140-2 approved mode.

Be sure to operate in a protected/secure environment during the initial configuration. When starting up the SEE for the first time, use the front panel to configure the device for network connectivity and SMCII to perform the configuration operations.

1. Power on the unit.
   The SEE automatically verifies the authenticity of its firmware each time it boots. If the firmware has been illegitimately modified, the SEE will halt and indicate it has been irrecoverably tampered. In this case, the SEE must be returned for repair.
2. Verify the network configuration and configure the SEE’s Ethernet management port settings if necessary.
3. Assign the SEE an IP address, Netmask, and Gateway address.
4. Add the SEE to the SMCII database using SMCII.
5. Load a certificate.
   At this point the device is certified; the **ENT** key on the front panel is disabled; and the default factory account has been removed.
6. Configure the interface to interoperate with the operational network. Using SMCII, complete the following:
   a. Configure the Link Settings.
   b. Configure the Global Policy Settings.
7. If required, configure the unit for inband management.

At this point the device is ready to be deployed.

Key Management

Protection of User Data Traffic

The encryptor must be authenticated by the SMCII to enable management operations (other than setting encryptor date/time and IP address). As a result of authentication, the encryptor will have a private/public key pair and a certificate containing the public key. The certificate is signed by the SMCII that issued the authentication operation.

User data is protected through encryption of secure connections. Each connection has an associated Master Session Key (MSK) and Session Key (SK). The MSK is used to protect the transport of future session keys. The encryptor sends its certificate when a secure connection is being established. The encryptor verifies that the received certificate is within the validity lifetime and is signed by the SMCII that issued its own certificate. If the certificate verification fails, the connection establishment process is terminated immediately. Session keys are used to encrypt user data distributed in key update messages. Certificates are used to authenticate the connection prior to establishment of the connection and its associated keys.

Protection of Management Traffic

Local management of the encryptor is possible via the serial port. These operations are authenticated by user id and password. Remote management connections are both authenticated and encrypted within the SNMPv3 protocol. AES encryption based on Diffie-Hellman key agreement is used to encrypt IP communication between the management station and the encryptor.

Key Types

The SEE manages several types of keys. These cryptographic keys are generated within the unit and cannot be manually entered or loaded. Plaintext keys are never exposed outside the SEE. Session keys are distributed only in enciphered format. The following cryptographic keys are generated by the SEE.

System Master Key

The System Master Key (SMK) protects critical security parameters (CSPs). The System Master Key is generated when the encryptor is authenticated by the SMCII.

The 168-bit Triple DES SMK is generated internally and stored in a battery backed RAM (BBRAM) device. If the unit is tampered, the BBRAM power is automatically disconnected which zeroizes the SMK and renders the enciphered CSPs unrecoverable.

System Private/Public Key Pair

The System Private/Public Key is used for:

- confidentiality during certificate installation from the SMCII.
- remote entity authentication during connection negotiation.
- ciphering of confidential parameters during connection negotiation.

The System Private/Public Key pair is generated internally. The encrypted System Private/Public Key pair is stored in flash memory. A new System Private/Public Key pair is generated each time the encryptor is authenticated by the SMCII.

Master Session Key

The MSK is a key used between security agents for encrypting and decrypting session keys after initial connection establishment. An MSK is generated internally for each secure connection and is valid for the life of the connection.

To develop the MSK, 256-bit random values are selected by both the initiator and responder. These 256-bit values are encrypted and exchanged with the public key of the recipient. The exchanged values are decrypted and concatenated to form the MSK. The concatenation is performed as follows: the initiator value forms the most significant or leftmost half, and the responder value forms the least significant or rightmost half.

Session Key

Session keys are the keys used by the encryption algorithm for the data confidentiality service. The two security agents involved in a security exchange randomly create session keys, and they are encrypted and transferred using the security message exchange protocol. Session keys for confidentiality are created using a random number generator and are encrypted with the public key of the recipient.

A session key is generated internally for each data flow path in a secure connection, one for the Initiator-Responder path and another for the Responder-Initiator path. An SK is generated and distributed at the key update interval.

Session Key Update Protocol

The session key update protocol involves two processes: exchanging a new session key between the initiator and responder, and changing over from the old session key to the new session key. The first process is referred to as session key exchange (SKE) and the second process is referred to as session key changeover (SKC).

In order to change keys at high speeds, without disrupting service to the end user, two session keys are required: a current-key and a next-key. The next-key is delivered from the source to the destination using the SKE message. The destination stores the next-key in a separate memory location until needed. The key number fields in the SKE message are used to identify the next-key (with respect to the current key). The actual changeover occurs when the SKC message is sent.

Session Key Exchange Process

The SKE message is used to securely transfer the next session key from the source to the destination. Each key update uses a sequential key number for synchronization between the source and destination as well as for cryptographic protection. A 32-bit numbering scheme is used, which means that 2^{32} -1 session key updates can be performed on a connection before the key number wraps around. The next session key is encrypted using the MSK obtained during secure call establishment.

Other Critical Security Parameters

In addition to keys, the SEE maintains several CSPs.

User Password

Each management account has a user id and password associated with it. These confirm the authenticity of a user attempting to manage the encryptor.

Management Channel Privacy

Privacy is implemented through FIPS-compliant SNMPv3 management channel security using Diffie-Hellman key agreement and AES encryption.

Interaction

The encryptor generates a master session key, initial session key, and initialization vector (IV) for the secure connection. The encryptor encrypts the keys and IV using the public RSA key of the other encryptor.

The encryptor decrypts the received message using its private key to recover the master session key, initial session key, and IV. The decrypted keys and IV are then loaded into the decryption module at an address corresponding to the connection. Ethernet frames transmitted or received will now be encrypted or decrypted using the session key for that particular connection.

Compliance

The SafeNet Ethernet Encryptor is in full compliance with all of the following at the time of manufacture.

Contact your SafeNet sales representative for more details on the standards supported by this product.

⚠ **CAUTION**

Changes or modifications to this product not expressly approved by SafeNet, Inc. could void the user's authority to operate this equipment.

Cryptography

- Designed to National Institute of Standards and Technology (NIST), FIPS 140-2, Level 3.
- National Institute of Standards and Technology (NIST), FIPS 197, November 2001, Advanced Encryption Standard (AES).

Common Criteria

The SafeNet Ethernet Encryptor is assessed to and complies with Common Criteria EAL4. (in process)

Emissions/Immunity

- Federal Communications Commission (FCC) Rules and Regulations, Part 15 (Spurious Radiation) for Class B devices.
- SafeNet, Inc. declares that this product conforms to the EMC Directive 89/336/EEC.

FCC Notice to Users

Federal Communications Commission (FCC) Rules require that you be notified of the following.

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

Industrie Canada

This Class B digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Industrie Canada Warning Statement

This digital apparatus does not exceed the Class B limits for radio noise from digital apparatus as set out in the Radio Interference Regulations of IC Canada.

Product Safety

- Complies with UL 60950, CSA 60950, EN 60950, and IEC 60950 (CB Scheme).
- SafeNet, Inc. declares that this product conforms to the Low Voltage Directive 73/23/EEC.

Product Compatibility

While every effort has been made to verify operation of this product with many different communications products and networks, SafeNet, Inc. makes no claim of compatibility between its products and other vendors' equipment. It is assumed that users have thoroughly evaluated this product's performance in the communications environment in which it will be used.

Safety Considerations

The following general safety precautions must be observed during all phases of operation and service of this product. Failure to comply with these precautions or with specific warnings elsewhere in this User's Guide willfully violates standards of design, manufacture, and intended use of the product. SafeNet, Inc. assumes no liability for the customer's failure to comply with these requirements.

- This product must be grounded. In the event of a short circuit, grounding reduces the risk of electrical shock by providing an escape wire for the current.
- We recommend that you use preferred power—a dedicated power circuit with an assigned circuit breaker.
- The product's AC power cord ends in a three-pole grounding plug. Do not use a three-pole to two-pole adapter with the plug. Verify that the outlet you intend to use is properly installed and grounded; the outlet used must comply with the National Electric Code (NEC) NFPA70 (1990) in U.S. A. or other local and national or international applicable codes.
- Do not install or operate this product in the presence of flammable gases or fumes. Operation of any electrical instrument in such an environment constitutes a definite safety hazard.
- With the exception of a user serviceable fuse (on units with DC power supply modules) and AC power supply modules (on the 10 GbE dual AC model), no user maintained or adjustable components are present within this product. Do not attempt to service this equipment except under the direction of SafeNet. Only SafeNet-authorized service personnel should service this equipment. The potential for electrical shock exists within the enclosures at all times unless the equipment is unplugged.
- ⚠ MULTIPLE POWER SOURCES - Disconnecting both power supply inputs will result in immediate power off. Disconnect both power supply inputs before servicing with the cover removed.

Laser Information and Safety

Optical SFPs are a Class 1 Laser and safety precautions need to be followed per FDA/CDRH and IEC-825-1 regulations.

Lithium Battery

The SafeNet Ethernet Encryptor unit contains a 3V lithium coin cell battery.

⚠ **CAUTION**

The 3V lithium coin cell battery and the components containing a lithium battery are NOT customer replaceable parts. Do not attempt to recharge the battery. Do not expose the lithium battery by opening the component. Do not dispose of the component by fire. Damage to the equipment may result.

⚠ **WARNING**

The lithium battery could explode if mistreated.

The Safety status of the points of interconnection to other equipment is declared as follows:

a) SELV Circuits

i) REMOTE

ii) DTE port

b) TNV Circuits

i) DCE port

Electrostatic Discharge

As with all electronic devices, the operator must guard against Electrostatic Discharge (ESD). Use of proper ESD management techniques (ESD flooring, wrist straps, etc.) will prevent potential damage to the unit. It is strongly recommended to eliminate the potential of ESD during the following procedures:

- installing the unit in a rack
- replacing a power supply module
- replacing a fuse

RoHS / WEEE

SafeNet Ethernet Encryptors are RoHS-5 compliant. SEEs that are taken out of service should not be discarded with ordinary waste. Follow the WEEE or other directives that apply in your country.

This page intentionally left blank.

Glossary

A

action
Bypass, encrypt/decrypt, or discard frame.

Address Resolution Protocol (ARP)
A protocol which is used to map an IP address to a physical machine's address that is recognized in the local network. The ARP specification is defined in RFC 826.

address type
A state to indicate unicast, multicast, or broadcast MAC addresses.

Advanced Encryption Standard (AES)
A symmetric algorithm (same key for encryption and decryption) using block encryption of 128 bits in size, supporting key sizes of 128, 192, and 256 bits.

AES
See Advanced Encryption Standard.

ARP
See Address Resolution Protocol.

authentication
Verifies the source of a message.

B

block cipher
Type of symmetric (secret key) encryption algorithm that encrypts a fixed length block of plaintext at a time. With a block cipher, the same plaintext block always encrypts to the same ciphertext block, under the same key.

BPDU
See Bridge Protocol Data Unit.

Bridge Protocol Data Unit (BPDU)
Data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

broadcast frame
A frame that has a destination address of 0xFFFFFFFFFFFF.

C

CA
See Certifying Authority.

CBC
See Cipher Block Chaining.

certificate
Digital document that binds an entity to a public key. An entity can be a PC, a router, a server, the SEE, or some other network device. Certificates ensure that the keys and identity of the bearer are valid by means of a third-party trust.

Certifying Authority (CA)
Trusted organization that accepts certificate applications, authenticates applications, issues certificates, and maintains status information about certificates.

Cipher Block Chaining (CBC)
Method of using a block cipher in which two identical plaintext blocks encrypt to different ciphertexts.

ciphertext
Message that has been encrypted so that only an authorized recipient can read it.

CLI
See Command Line Interface.

Command Line Interface (CLI)
Text-based user interface to a device. The SEE has a CLI.

confidentiality
Ensures that the content of the message (user data) has not been revealed.

connection
A logical link between a pair of encryptors. A connection consists of one or more MAC address connections. In this document, the terms connection and tunnel are used interchangeably.

connection identifier
An id number for a connection between two encryptors.

D

Data Encryption Standard (DES)
U.S. FIPS standard that defines the Data Encryption Algorithm. The DES algorithm is a symmetric block cipher with a block size of 64 bits and a key length of 64 bits (8 are parity bits). Triple DES (3DES or TDES) is the most accepted variant of the original algorithm.

DES
See Data Encryption Standard.

Diffie-Hellman key exchange
Method for key exchange between two parties that allows two autonomous systems to exchange a secret key over an untrusted network without prior shared secrets.

digital signature
Electronic signature used to authenticate both a message and the signer. A digital signature must be difficult to repudiate and must protect the integrity of the information being signed. By encrypting a digest of a message with the private key, authentication can later be performed by applying the public key to an encrypted digest (digital signature) and comparing the result to the digest of the message.

Digital Signature Standard (DSS)
Standard for digital signatures using the DSA public key algorithm and the SHA-1 hash algorithm.

DSS
See Digital Signature Standard.

E

encryption
Scrambles and unscrambles data between two communication endpoints. The encryption process turns an original plaintext message that anyone can read into an encrypted ciphertext message that can be read only by an authorized recipient.

Ethertype
Ethertype is a field in the Ethernet networking standard used to indicate which protocol is being transported in an Ethernet frame.

I

Initialization Vector (IV)
A sequence of random bytes appended to the front of the plaintext before encryption by a block cipher. Adding the initialization vector to the beginning of the plaintext eliminates the possibility of having the initial ciphertext block the same for any two messages. For example, if messages always start with a common header their initial ciphertext would always be the same, assuming that the same cryptographic algorithm and symmetric key was used. Adding a random initialization vector eliminates this from happening.

integrity
Integrity ensures that the content of a message has not been altered.

IV
See Initialization Vector.

M

MAC address
See Media Access Control address.

manual keying
Method of distributing externally generated cipher keys that are used to protect traffic. This method does not scale well and is unsuitable for large installations.

Media Access Control (MAC) address
A six-byte hardware address that uniquely identifies each node of a network. A MAC address provides a fail-safe method for specifying the recipient of data sent over a LAN, as well as allowing for unique identification of the device itself.

MPLS
See MultiProtocol Label Switching.

MultiProtocol Label Switching
A label switching mechanism that combines the performance of packet forwarding based on layer 2 switching with the intelligence of layer 3 routing.

P

PKI
See Public Key Infrastructure.

plaintext
Original, unencrypted message that anyone can read.

private key
In public key cryptography, a key is known only to its owner. It is used to sign and decrypt messages.

public key
In public key cryptography, the key included in the certificate that verifies signatures and encrypts messages.

public key cryptography
Type of cryptography in which different keys are used for encryption and decryption. The public key is public, but the private key is known only to its owner. Any entity that possesses the public key can encrypt a message so that only a single recipient (the owner of the private key) can decrypt it. The two parties do not need to share any secret information.

Public Key Infrastructure (PKI)
Use of key pairs, certificates, certificate authorities, and certificate repositories when using public key cryptography.

R

RSA algorithm
An asymmetric public key algorithm used to enable security operations like digital signatures and key distribution. An RSA operation is a modular exponentiation. The computation is performed by a series of modular multiplications.

S

SDH
See Synchronous Digital Hierarchy.

Secure Hash Algorithm (SHA)
U.S. standard for a cryptographically strong hash algorithm, designed by the National Security Agency (NSA) and defined by NIST.

Secure Socket Layer (SSL)
Security protocol commonly used in e-commerce applications. The security services that SSL provides are encryption, message authentication, server authentication, and client authentication.

SHA
See Secure Hash Algorithm.

SONET
See Synchronous Optical Network.

Spanning Tree Protocol (STP)
A link management protocol that is part of the IEEE 802.1 standard for media access control bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops), but establishes the redundant links as a backup if the initial link should fail.

SSL
See Secure Socket Layer.

STP
See Spanning Tree Protocol.

Synchronous Digital Hierarchy (SDH)
ITU–T defined world standard of transmission whose base transmission level is 52 Mbps (STM–0) and is equivalent to SONET's STS–1 transmission rate.

Synchronous Optical Network (SONET)
A fiber optic network in a ring topology; a standard for optical transport that defines optical carrier levels and their electrically equivalent synchronous transport signals.

T

transform
Defines the transformation applied to the data to secure it. This includes the encryption algorithm, security protocols, key sizes and how they are derived, and the transformation process.

tunnel
See connection.

V

Virtual Local Area Network (VLAN)
A virtual local area network (VLAN) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment. VLANs are configured through software rather than hardware making them extremely flexible. The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames.

Virtual Private Network (VPN)
Network that uses encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

VLAN
See Virtual Local Area Network.

VPN
See Virtual Private Network.

Index