Netcrypt Bulk Encryptor Hardware Installation and Configuration Guide

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgements

Publication Disclaimer

Copyright

Contents

Safety Precautions

Read, Retain, and Follow These Instructions

Carefully read all safety and operating instructions before operating this product. Follow all operating instructions that accompany this product. Retain the instructions for future use. Give particular attention to all safety precautions.

Warning and Caution Icons

WARNING:

Avoid personal injury and product damage! Do not proceed beyond any icon until you fully understand the indicated conditions.

The following icons alert you to important information about the safe operation of this product:

You will find this icon in the literature that accompanies this product. This icon indicates important operating or maintenance instructions.

You may find this icon affixed to this product and in this document to alert you of electrical safety hazards. On this product, this icon indicates a live terminal; the arrowhead points to the terminal device.

You may find this icon affixed to this product. This icon indicates a protective earth terminal.

You may find this icon affixed to this product. This icon indicates excessive or dangerous heat.

You may find this symbol affixed to this product and in this document. This symbol indicates an infrared laser that transmits intensity-modulated light and emits invisible laser radiation and an LED that transmits intensity-modulated light.

Heed All Warnings

Adhere to all warnings on the product and in the operating instructions.

Avoid Electric Shock

Follow the instructions in this warning.

WARNING:

To reduce risk of electric shock, perform only the instructions that are included in the operating instructions. Refer all servicing to qualified service personnel.

Servicing

WARNING:

Avoid electric shock! Opening or removing the cover may expose you to dangerous voltages.

Do not open the cover of this product and attempt service unless instructed to do so in the operating instructions. Refer all servicing to qualified personnel only.

Cleaning, Water, Moisture, Open Flame

To protect this product against damage from moisture and open flames, do the following:

- Before cleaning, unplug this product from the AC outlet. Do *not* use liquid or aerosol cleaners. Use a dry cloth for cleaning.
- Do not expose this product to moisture.
- Do not place this product on a wet surface or spill liquids on or near this product.
- Do not place or use candles or other open flames near or on this product.

Ventilation

To protect this product against damage from overheating, do the following:

- This product has openings for ventilation to protect it from overheating. To ensure product reliability, do not block or cover these openings.
- Do not open this product unless otherwise instructed to do so.
- Do not push objects through openings in the product or enclosure.

Placement

To protect this product against damage from breakage, do the following:

- Place this product close enough to a mains AC outlet to accommodate the length of the product power cord.
- Route all power supply cords so that people cannot walk on, or place objects on, or lean objects against them. This can pinch or damage the cords. Pay particular attention to cords at plugs, outlets, and the points where the cords exit the product.
- Make sure the mounting surface or rack is stable and can support the size and weight of this product.

WARNING:

Avoid personal injury and damage to this product! An unstable surface may cause this product to fall.

When moving a cart that contains this product, check for any of the following possible hazards:

- Move the cart slowly and carefully. If the cart does not move easily, this condition may indicate obstructions or cables that you may need to disconnect before moving this cart to another location.
- Avoid quick stops and starts when moving the cart.
- Check for uneven floor surfaces such as cracks or cables and cords.

WARNING:

Avoid personal injury and damage to this product! Move any appliance and cart combination with care. Quick stops, excessive force, and uneven surfaces may cause the appliance and cart to overturn.

Fuse

When replacing a fuse, heed the following warnings.

WARNING:

Avoid electric shock! Always disconnect all power cables before you change a fuse.

WARNING:

Avoid product damage! Always use a fuse that has the correct type and rating. The correct type and rating are indicated on this product.

Grounding This Product (U.S.A. and Canada Only)

Safety Plugs

If this product is equipped with either a three-prong (grounding pin) safety plug or a two-prong (polarized) safety plug, do not defeat the safety purpose of the polarized or grounding-type plug. Follow these safety guidelines to properly ground this product:

- For a 3-prong plug (consists of two blades and a third grounding prong), insert the plug into a grounded mains, 3-prong outlet.

  Note: This plug fits only one way. The grounding prong is provided for your safety. If you are unable to insert this plug fully into the outlet, contact your electrician to replace your obsolete outlet.
- For a 2-prong plug (consists of one wide blade and one narrow blade), insert the plug into a polarized mains, 2-prong outlet in which one socket is wider than the other.

Note: If you are unable to insert this plug fully into the outlet, try reversing the plug. The wide blade is provided for your safety. If the plug still fails to fit, contact an electrician to replace your obsolete outlet.

Grounding Terminal

If this product is equipped with an external grounding terminal, attach one end of an 18-gauge wire (or larger) to the grounding terminal; then, attach the other end of the wire to an earth ground, such as an equipment rack that is grounded.

20050727 Headend/Rack

About This Guide

Introduction

This guide describes at a high level the capabilities, physical connections, applications, and operational theory of the Cisco Netcrypt Bulk Encryptor. It also provides installation, provisioning, operation, maintenance, and troubleshooting procedures, as well as technical specifications.

Purpose

This guide provides detailed specifications and component descriptions for the Netcrypt Bulk Encryptor. This guide also includes all of the procedures that enable you to install, provision, and operate the Netcrypt Bulk Encryptor within your DBDS. Call center personnel can use this guide to assist them with common troubleshooting procedures.

Scope

This guide discusses the following topics:

- Netcrypt Bulk Encryptor operational theory
- Descriptions of Netcrypt Bulk Encryptor functions
- Descriptions of Netcrypt Bulk Encryptor components
- Installation procedures
- Operation procedures
- Maintenance and repair procedures
- Troubleshooting guidelines
- Customer support information
- Netcrypt Bulk Encryptor technical specifications

Audience

This guide is written for system administrators of the Digital Broadband Delivery System (DBDS), operators of the Explorer Controller (EC), call center personnel, and system operators who are responsible for installing, operating, maintaining, and troubleshooting the Netcrypt Bulk Encryptor.

Document Version

This is the first formal release of this document.

1

Introducing the Netcrypt Bulk Encryptor

Introduction

This chapter provides a high-level overview of the capabilities, physical connections, applications, and operational theory of a Netcrypt Bulk Encryptor. This chapter also provides illustrations and descriptions of front and back panel components.

Use the information in this chapter to gain an understanding of NOBE operation that you can draw on when provisioning the unit or setting up sessions and connections on it. The information in this chapter can also help you effectively troubleshoot a Netcrypt Bulk Encryptor.

For technical specifications, see ***Technical Specifications*** (on page 105).

In This Chapter

Netcrypt Bulk Encryptor Functional Overview

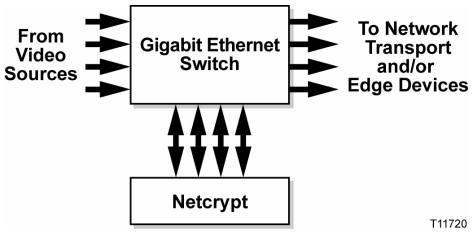
Powerful, Flexible High-Speed Encryption

The Netcrypt Bulk Encryptor is a powerful network-attached encryption device designed for broadcast and on-demand applications in systems that use MPEG transport over UDP, IP, and Ethernet. The unit is supported in DBDS System Release (SR) 2.6/3.6/4.1 and later. Output multicast for the Netcrypt Bulk Encryptor is supported in DBDS SR 2.7/3.7/4.2 and later.

Although compact, the Netcrypt Bulk Encryptor has a maximum throughput of 4 gigabits per second. It is capable of encrypting as many as 4000 input programs into a maximum of 4000 transport streams suitable for digital broadcast or multicast sessions.

Network-Attached Encryption

The unit is designed to be connected to a switch or router network using four Gigabit Ethernet (GbE) ports in bi-directional mode as shown in the following figure. In this application, the Quadrature Amplitude Modulation (QAM) modulator edge devices are connected to other ports on the GbE switch either directly or remotely through other network transport equipment. Clear data is sent to the unit for encryption, and encrypted data is sent back to the GbE switch for distribution through other ports. Any combination of ports can be used.



Physical Overview

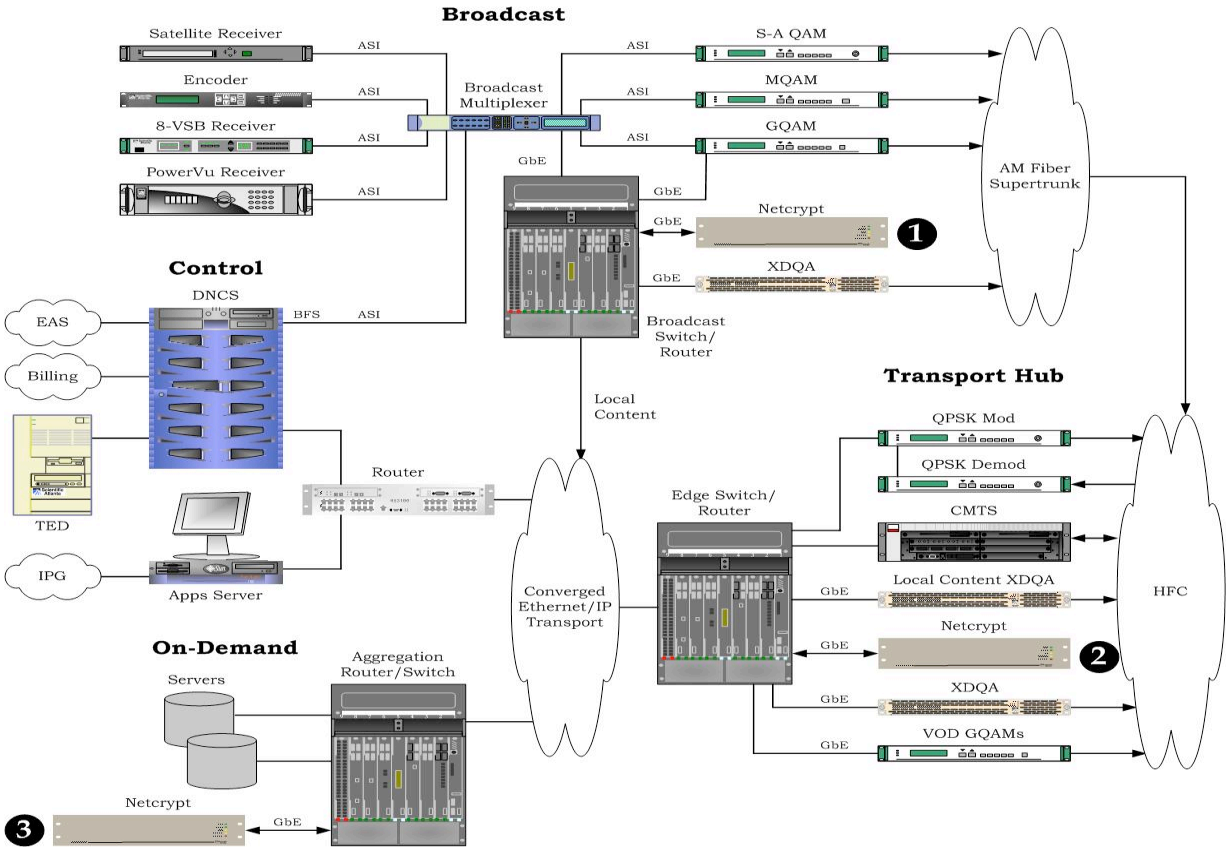
The back panel of the Netcrypt Bulk Encryptor has eight sockets for GbE connections. Four are supported today and four are not used. In addition to the GbE connectors, the back of the unit has two 10/100Base-T Ethernet ports. One of these ports is used for Application Server control of the unit. The other port is used only in systems that supplement the PowerKEY® Conditional Access (CA) system with other CA systems and is discussed further in ***SimulCrypt Support Option*** (on page 18) in the ***Theory of Operation*** (on page 4) section of this chapter.

The Netcrypt Bulk Encryptor takes up two rack units of space. Indicators on the front and back panels provide a concise, at-a-glance status of the unit. For more information, see ***Front Panel Overview*** (on page 21) and ***Back Panel Overview*** (on page 22).

System Use

Depending on the application and system architecture, the Netcrypt Bulk Encryptor can be used in either headends or hubs, as shown in the following illustration. With any-to-any network connectivity, a Netcrypt Bulk Encryptor located anywhere in the Network may be used to encrypt streams for broadcast or video-on-demand (VOD).

1. The Netcrypt Bulk Encryptor shown in the headend is used to encrypt broadcast streams that will be modulated in the xDQA below it or in the Local Content xDQA that is shown in the Transport Hub.
2. The Netcrypt Bulk Encryptor shown in the Transport Hub may be used for both VOD and local broadcast streams that are bound for either of the xDQAs in the Transport Hub.
3. The Netcrypt Bulk Encryptor shown here for an On-Demand application is used to encrypt VOD streams that are bound for the xDQA in the Transport Hub.



Theory of Operation

Introduction

As a network-attached bulk encryptor, the Netcrypt Bulk Encryptor was designed to benefit from the added flexibility of MPEG-2 transport over UDP/IP/GbE and to support single-program transport streams (SPTSs) as well as multi-program transport streams (MPTSs). It supports both table-based and session-based QAM modulators, multicast and unicast, and broadcast as well as interactive applications. This section reviews some of these concepts.

When referring to this section, keep in mind that the Netcrypt Bulk Encryptor is not restricted to operation with QAM modulators. QAM modulators provide a typical edge device for purposes of explaining its operation, and so this guide is written using QAM modulators as edge devices. Also, keep in mind that other types of IP edge devices—or even IP destination devices—may be used in conjunction with a Netcrypt Bulk Encryptor.

MPEG-2 Transport and Gigabit Ethernet

A key feature of MPEG-2 Transport is the ability to carry multiple programs over a single connection or RF carrier. The combination of one or more programs into a common stream is referred to as a transport stream. Each transport stream is uniquely identified by a transport stream identifier (TSID). Programs in a transport stream must all travel together. That is, they must all go from the same source to the same destinations. Recombining programs into new transport streams in order to add new content or send programs to different destinations requires MPEG multiplexing, as illustrated on the following page.

MPEG multiplexing is ideally suited for broadcast systems where a group of programs is statically combined and sent to a common modulator. However, in newer applications, such as VOD and switched broadcast video, programs frequently come and go, and destinations frequently change. Each time a re-multiplexing of transport streams occurs, a great deal of MPEG-layer processing must be performed. Program numbers (PNs) and packet identifiers (PIDs) must be remapped in order to avoid duplication. Program-specific information (PSI), including the program association tables (PATs) and program map tables (PMTs), must be reconstructed in order to reflect this remapping. Receivers must be notified of changes. Frequent MPEG re-multiplexing can be expensive, slow, and a barrier to network and application flexibility.

Carrying MPEG-2 Transport over UDP, IP, and GbE adds a new dimension of flexibility. By using new "tags," such as destination UDP port or IP multicast address, transport streams can be distinguished. This enables carrying multiple transport streams on a single "wire." Transport streams may be recombined and split without the need for multiplexing. Using standard IP/Ethernet switches and routers, you can add and drop programs, and connect any source to any destination without "MPEG-aware" processing.

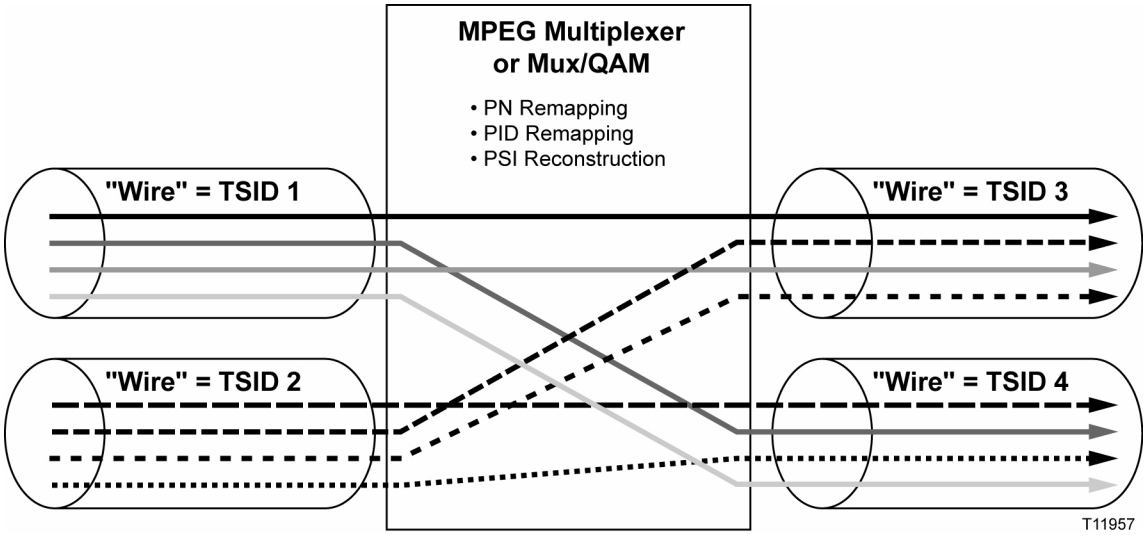
- **Single-Program Transport Streams.** If programs within a transport stream must all travel together (unless re-multiplexed), but transport streams may be combined and split without requiring multiplexing, then for some applications it is preferable to carry only a single program in a transport stream. For example, in applications such as VOD, each program may be created or ended individually. Each program output from a VOD server may be headed to a different QAM modulator. If each program is in its own SPTS, then no multiplexing is needed between the VOD server and QAM. For VOD, the SPTSs are typically distinguished by unique destination UDP ports.

  Similarly, in switched broadcast applications, it is advantageous to handle programs individually. Each program is assigned its own transport stream such that they can be individually selected for carriage over a QAM modulator. Switched broadcast SPTSs are usually distinguished by unique IP multicast addresses. The term "broadcast" is, strictly speaking, a misnomer here since, in fact, these are multicasts and not full broadcasts.

- **Multi-Program Transport Streams.** MPTSs are the traditional method of carrying programs in a transport stream. The MPTS continues to be useful, for example, at the RF output of a QAM modulator. Asynchronous Serial Interfaces (ASI) support only one transport stream, so the only way to carry multiple programs is an MPTS. MPTSs are also useful for carrying a statistically-multiplexed group of channels from a multiplexer to a QAM modulator, either over an ASI link (as shown in the figure on the following page) or even over UDP/IP/GbE.

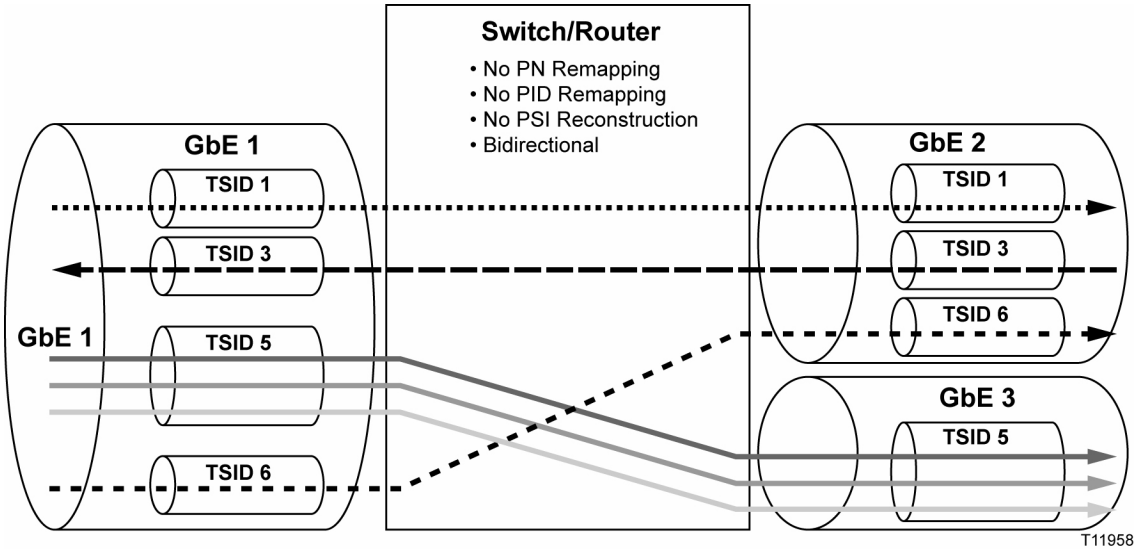
Programs Entering a Multiplexer on Two Separate Interfaces

The following figure shows a number of programs (represented as solid and dotted lines) coming into a multiplexer on two separate ASI interfaces. Each interface carries one MPTS. These are labeled TSID 1 and 2. Two output MPTS interfaces are also shown. In the case of a multiplexer, the output interfaces could be ASI as well. In another example, the MPEG multiplexer could be part of a QAM modulator, and TSIDs 3 and 4 may be on two RF carriers. In either case, since MPTSs are being recombined, MPEG multiplexing is required, including remapping of PNs, PIDs, and reconstruction of PSI.



Programs Entering a Switch/Router on Three GbE Interfaces

The following figure shows a switch/router with three GbE interfaces. Note that each interface is bi-directional and some of the streams are flowing into the switch/router and some out on the same interfaces (TSIDs). Also note that, in this example, there is a mix of SPTSs and one MPTS (shown as TSID 5). All of the transport streams are individually switchable to other interfaces, regardless of whether they contain SPTSs or MPTSs. As long as all of the programs on the MPTS travel together, no re-multiplexing is required. No PN or PID remapping is required, and no PSI reconstruction is required.



Support for Table-Based QAMs

QAM modulators can generally be divided into two types based on how streams are mapped from input to output of the modulator.

- **Session-based QAM modulators.** In session-based QAM modulators (SB-QAMs), such as our Gigabit QAM (GQAM) modulator, the mapping of input streams to output carrier, MPEG PN, and PIDs is dynamically controlled and assigned at session-setup time. SB-QAMs allow the ultimate flexibility and mapping control for SPTSs and MPTSs over GbE. Session-based mapping more easily accommodates both IP unicasts and multicasts.

- **Table-based QAM modulators.** In table-based QAM modulators (TB-QAMs), such as our eXtra Dense QAM Array (xDQA), the destination UDP port number of an input stream is mapped to an output carrier, MPEG PN, and PIDs based on a table or formula. This mapping is not dynamically altered in anticipation of individual streams. TB-QAMs do not require communications with a controller for input to output mapping to occur just prior to the arrival of each new stream.

Because of the need for session-based provisioning in order to encrypt in the QAM modulators, our DBDS has always included dynamic input-to-output mapping as part of the session-based provisioning of SB-QAMs. In our traditional DBDS, these mappings are assigned by the Application Server, which acts as the Session and Resource Manager (SRM).

With a Netcrypt Bulk Encryptor, however, a DBDS can support TB-QAMs, which do not perform dynamic input-to-output mapping. Instead, tables are input to the Application Server as described in ***Add Table-Based QAM Information to the Application Server*** (on page 53). At session setup, the Application Server then assigns a destination IP address and destination UDP port at the output of the Netcrypt Bulk Encryptor so that the streams arrive at the correct TB-QAM and are then autonomously mapped by the TB-QAM to the desired output according to its table. This process is the same whether the streams are broadcast or VOD streams. However, note that although the Netcrypt Bulk Encryptor supports MPTSs as well as SPTSs, table-based mapping on some TB-QAMs limits this application to SPTSs only.

Broadcast Applications

In order to encrypt a broadcast stream using a Netcrypt Bulk Encryptor, operators use the Application Server to set up an encrypted Continuous Feed (CF) session on the Netcrypt Bulk Encryptor. The bulk encryptor supports both single-program transport streams (SPTSs) as well as multi-program transport streams (MPTSs). It also supports IP unicast as well as IP multicast addresses at either input or output. However, some TB-QAM modulators currently support only unicasts.

By default, a Netcrypt Bulk Encryptor bocks all programs for which there is no session. However, it is possible for a Netcrypt Bulk Encryptor to pass all programs in a specified transport stream, unencrypted, by creating a Transport Stream Route (TSR), as described in ***Unicast and Multicast Behavior*** (on page 14). It is also possible to pass individual programs “in the clear” by creating unencrypted CF sessions.

At CF session setup time, a number of address and header information must be provided. This information is summarized in ***Summary of Addresses and Stream Header Information*** (on page 16).

VOD Applications

In a VOD application, the information for addressing of streams at the input and output of the Netcrypt Bulk Encryptor is exchanged at Exclusive Session (ES) setup time through DSM-CC-compliant and SSP2.3-compliant session signaling. Note that in order to properly route traffic through a Netcrypt Bulk Encryptor, the Application Server provides the GbE port IP address of the Netcrypt Bulk Encryptor to the VOD server. The VOD server must accept this address and use it in the destination IP address field of the content for that session. This address is given to the VOD server in an Ethernet Interface Resource descriptor as part of the AddResourceConfirm message per the SSP 2.3 standard. For more information, see ***Summary of Addresses and Stream Header Information*** (on page 16).

Note also that only unicast SPTSs are required for VOD. MPTSs are not required for VOD. Multicasts are not required for VOD.

Network Considerations

The network considerations discussed in this section help operators understand both the operation of the Netcrypt Bulk Encryptor and the data that operators must enter in the Application Server when provisioning the unit or setting up sessions and connections on it.

GbE Transport Network Clouds: Specifying Netcrypt Bulk Encryptor-to-QAM Connectivity

It is possible to design a network so that any Netcrypt Bulk Encryptor can reach any QAM modulator. However, for a variety of reasons, such as the physical or logical locations of bulk encryptors, the network design, limitations of transport networks, or load balancing, some networks may require that connectivity be restricted. With SR 2.6/3.6/4.1 and later, the Application Server uses a “GbE transport” concept and tool to specify and limit network connectivity.

As the following illustration shows, network connectivity between each Netcrypt Bulk Encryptor and other devices in the network is specified by creating one or more “GbE transport” networks or “clouds” on the Application Server. Note that the GbE transport cloud is a logical concept, not a physical device. A cloud may be composed of one or more switches, routers, and transport devices. Any-to-any physical connectivity may exist, yet the Application Server will not configure a connection where a GbE transport cloud does not indicate connectivity. In the examples that follow, all ports on Netcrypt Bulk Encryptors are connected to the same GbE transport clouds. In reality they may be connected to different clouds. When two or more ports are connected to the same cloud, the Application Server balances the session load among the commonly connected ports. In reviewing the following examples, keep in mind that the methods described in the examples can be combined in new and different ways not covered in the examples.

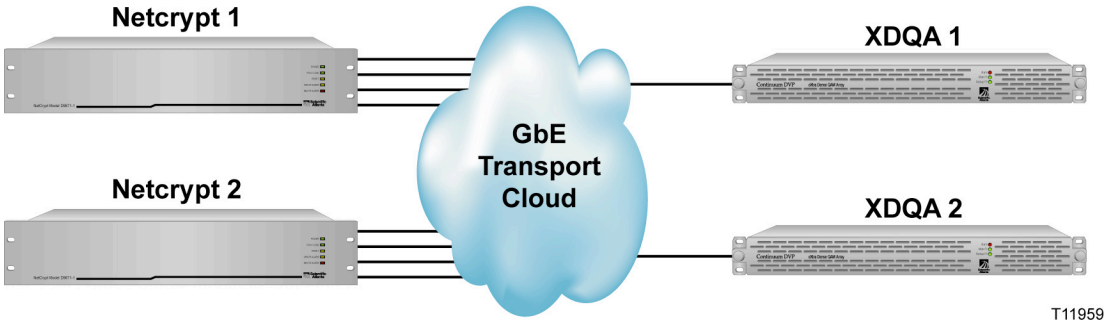
Using GbE Transport Clouds to Specify Any-to-Any Connectivity

Any-to-any connectivity would be specified by creating one GbE transport cloud and connecting every port of every Netcrypt Bulk Encryptor and QAM modulator to that cloud, as shown in the first example below.

Each port of a Netcrypt Bulk Encryptor must be connected to ports on one or more GbE Transport clouds.

Each GbE Transport cloud may have an arbitrary number of ports.

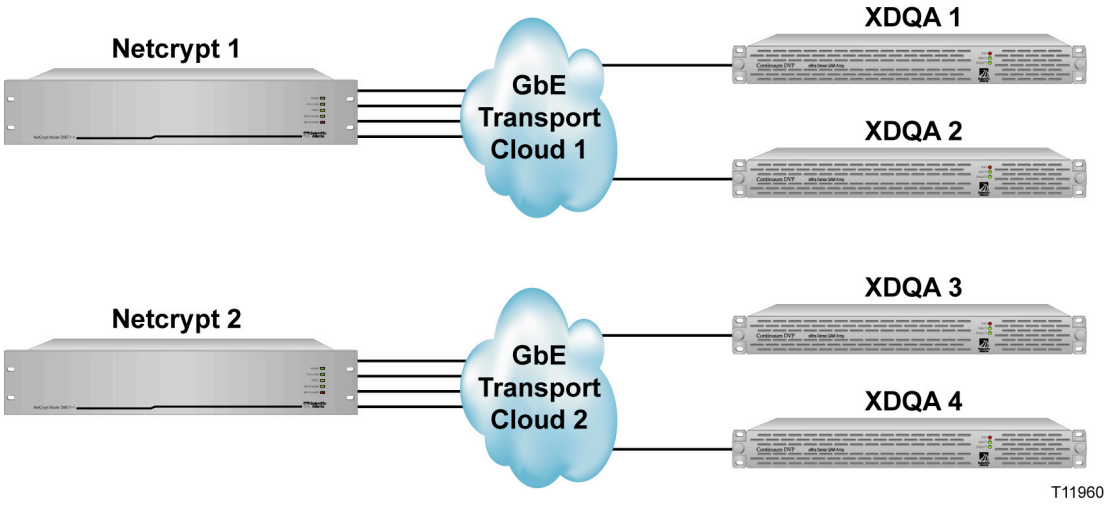
Each QAM (session-based or table-based) that is reachable from a GbE Transport cloud must also be connected to a port on one or more clouds.



Using GbE Transport Clouds to Control and Manage Network Connectivity

In a physical network implementation, any QAM may be reachable from a particular Netcrypt Bulk Encryptor. Nevertheless, limiting a Netcrypt Bulk Encryptor to a subset of QAMs through the use of GbE transport clouds may be useful for load-balancing, traceability, or other reasons. This is illustrated in the example below. Here, the Application Server will only use Netcrypt Bulk Encryptor1 for streams bound for XDQA1 or XDQA2. Similarly, Netcrypt Bulk Encryptor2 will only be used for streams bound for XDQA3 or XDQA4.

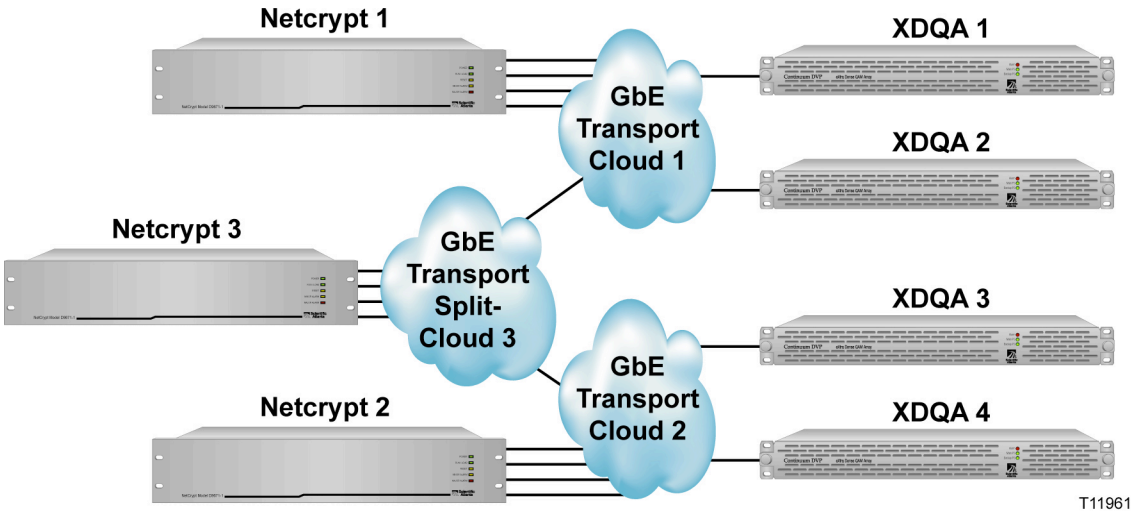
In this example, the Netcrypt Bulk Encryptors may be physically located either in the headend or at hubs along with their corresponding xDQAs. However, regardless of their physical location and connectivity, through the specification and use of Application Server GbE Transport Network Clouds, operators have a method for fine-grain control of Netcrypt Bulk Encryptor bandwidth.



Using GbE "Splitter Transport Clouds" for Centralized and Distributed Network Bulk Encryptors

In a centralized/distributed architecture, it may be desirable to use both centralized and distributed Netcrypt Bulk Encryptors. This may be accomplished using a "splitter cloud" as shown in the example below.

In the example shown, the choice of Netcrypt Bulk Encryptor1 or Netcrypt Bulk Encryptor3 for streams bound for cloud1 is ambiguous. The Application Server will attempt to balance the load between these Netcrypt Bulk Encryptors and also between Netcrypt Bulk Encryptor3 and Netcrypt Bulk Encryptor2 for content bound for cloud2.

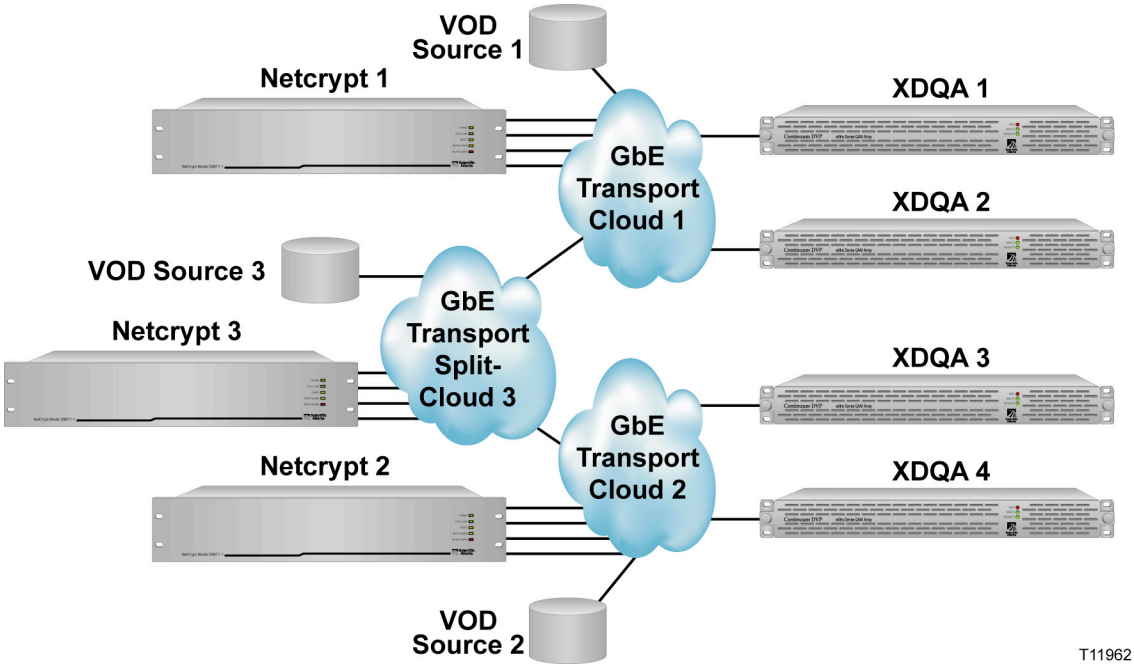


Using GbE Transport Clouds and Splitter Clouds for VOD Applications

It is possible to more tightly control the use of Netcrypt Bulk Encryptors by connecting sources to the GbE Transport Networks as shown in the example below. In this case, the GbE port IP addresses of the VOD pumps are entered into the Application Server when connecting pump ports to GbE Transport Network ports.

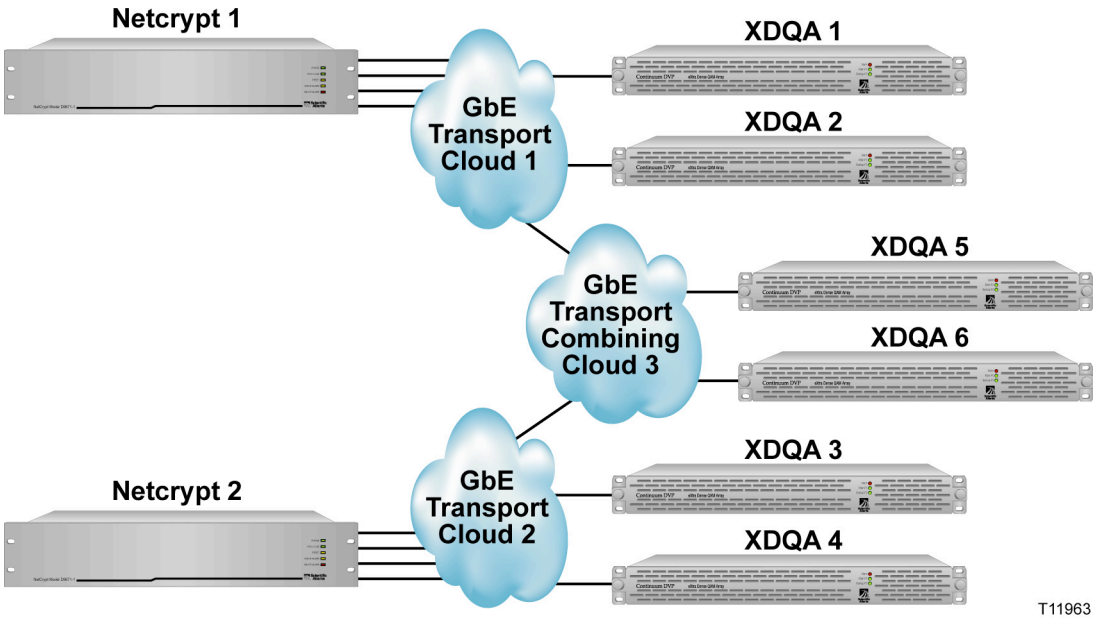
In this case, the Application Server will use Netcrypt Bulk Encryptor 3 only for streams coming from VODSource3. Similarly it will use Netcrypt Bulk Encryptor1 for streams coming from VODSource1 and so on.

The problem with this method is that not all VOD servers specify their selected source ports to the Application Server when a VOD session is set up. If a VOD server fails to specify the source IP address for a stream, the ambiguity will not be resolved and the Application Server will respond to the VOD server with the IP address of any Netcrypt Bulk Encryptor it chooses given the connectivity that has been specified.



Using a GbE Transport Combining Cloud

The following example illustrates the use of GbE Transport Networks as "combiners." Here, Netcrypt Bulk Encryptor1 or Netcrypt Bulk Encryptor2 may be selected by the Application Server for streams bound for XDQA5 or XDQA6.



Creating GbE Transport Clouds on the Application Server

When a GbE transport cloud is created on the Application Server, it must be given a name. Space is also provided to enter a control IP address (not a port IP address). This address is not used by the Application Server and simply provides a convenient place to save and retrieve this information should the operator wish to ping or telnet to a router or switch for monitoring or diagnostic purposes.

Host Network Behavior

The network behavior of the Netcrypt Bulk Encryptor is that of a host, not a router. That is, unicast content that passes through the Netcrypt Bulk Encryptor must be addressed to the Netcrypt Bulk Encryptor, not to the ultimate destination, such as a set-top or other edge device.

Address fields of IP headers that send content through a Netcrypt Bulk Encryptor illustrate the host behavior of the Netcrypt Bulk Encryptor.

Unicast content that passes through a Netcrypt Bulk Encryptor has the IP address of that Netcrypt Bulk Encryptor in the destination IP address field of the IP header.

Unicast content output from a Netcrypt Bulk Encryptor has the IP address of that Netcrypt Bulk Encryptor in the source IP address field of the IP header, and the IP address of the QAM modulator in the destination IP address field of the IP header.

T11972

Layer 2/3 Networks and Address Resolution Protocol

The Netcrypt Bulk Encryptor follows standard network rules and uses Address Resolution Protocol (ARP) to resolve required MAC addresses:

- In bi-directional Layer 2 networks, QAM modulators must respond to ARP requests.
- In Layer 3 networks, the assigned gateway must respond to ARP requests.

QAM modulators on the other side of one-way transport networks must be assigned IP addresses on different networks than the Netcrypt Bulk Encryptor. Per network rules, this will cause the Netcrypt Bulk Encryptor to issue an ARP request using its gateway IP address — not the IP address of a QAM modulator. In this case, the gateway, which may be the transport network, must support ARP.

It is recommended to connect the Netcrypt GbE ports to a Layer 3 router, as opposed to a Layer 2 switch. It is best to assign IP addresses out of separate subnets. The use of a /30 subnet mask minimizes wasted IP addresses. If the GbE interfaces are placed in the same Layer 3 VLAN, then the routing switch requires static MAC addresses

If Netcrypt GbE ports are connected to a Layer 2 switch, then static MAC addresses must be used in the switch due to the "one-way" nature of most MPEG traffic.

Unicast and Multicast Behavior

IP unicast and IP multicast addresses are supported at either or both of the Netcrypt Bulk Encryptor input and output for sessions and Transport Stream Routes (TSRs). Streams may be received by the Netcrypt Bulk Encryptor as unicast and output as multicast or vice versa.

The current release of the Netcrypt Bulk Encryptor does support Internet Group Management Protocol, Version 2 (IGMPv2).

Netcrypt Bulk Encryptor Ports

As shown to the right, the Netcrypt Bulk Encryptor has four active GbE ports. There is a MAC address assigned to each port. Operators must assign an IP address to any port they have provisioned on the Application Server. In a Layer 3 (routed) network, operators must provide a gateway IP address for any port they provision on the Application Server.

The first four ports of Netcrypt Bulk Encryptor are active GbE ports. These ports behave independently. Content coming in on any one port is processed and leaves using the same port. Routing between ports is not supported.

Note: GbE ports 5 to 8 are not active.

GbE Headroom

In designing a content routing and transport network, operators should provide some amount of headroom at all GbE ports. Bursty traffic can cause the instantaneous Ethernet frame arrival rate to exceed 1 Gb/s, even when the average rate is well below this. When this occurs, the switch or router will buffer some of the frames up to the memory capacity of the dedicated or shared buffer on the switch/router. When this capacity is exceeded, the switch/router discards the frames. As a result, it is possible to experience video glitching and macroblocking even though the switch/router and Netcrypt Bulk Encryptor all can handle the full GbE rate. The required amount of headroom can vary between 0 to 40 percent of the port capacity, or even more, depending on the burstiness of the source or VOD server.

MPEG Transport Layer Rules

The Netcrypt Bulk Encryptor is intended as a network device. Although as a transport stream encryptor it is necessary to perform some operations at the MPEG transport layer, the intent is to minimally alter the transport streams. The following list describes some rules of MPEG transport layer operation to which the Netcrypt Bulk Encryptor adheres:

- By default, the Netcrypt Bulk Encryptor blocks all input streams and programs from appearing at the output. It passes only streams and programs for which there exists either a defined session (broadcast or VOD) or one of the new Transport Stream Route (TSR) structures. The TSR concept has been added to the Application Server and Netcrypt Bulk Encryptor to enable an operator to instruct a Netcrypt Bulk Encryptor to pass all programs within a single or multi-program transport stream from a specified set of input addresses (unicast or multicast) to a specified set of output addresses.
- If sessions are created for fewer than all of the programs in an MPTS, then only the programs for which sessions are created are passed. PSI is altered to correctly reflect the programs that appear at the output. An exception to this would exist if the program in the session was also a part of a TSR.
- If a TSR is created, and subsequently a session is set up to encrypt a program within the same transport stream, then the output destination addresses must be the same. Otherwise the session setup will fail. The same applies to the reverse order of session setup and TSR creation.
- The Netcrypt Bulk Encryptor performs insertion of Entitlement Control Messages (ECMs) into encrypted streams for which sessions have been set up. It performs the required modifications of the PSI to reflect this.
- An SPTS coming in remains an SPTS going out. Multiple SPTSs cannot be combined to create an MPTS in the Netcrypt Bulk Encryptor.
- An MPTS coming in may go out as an SPTS if a session is created for only one program in the MPTS.
- No changes are applied to Program Clock References (PCRs)
- The Netcrypt Bulk Encryptor performs no remapping of MPEG PNs or PIDs.
- The Netcrypt Bulk Encryptor performs no dejittering. This function is handled by the edge QAM modulator. The selected QAM modulator must perform dejittering of any source jitter, GbE/IP encapsulation jitter and any jitter introduced by transport, routers, and switches.
- Because no remapping of MPEG PIDs occurs in the Netcrypt Bulk Encryptor, in order to prevent MPEG PID conflicts when ECMs are inserted, a range of PIDs must be reserved for ECM use in the Netcrypt Bulk Encryptor. Sources must not be allowed to use PIDs in this range. The range is entered in the Application

Server when operators add a Netcrypt Bulk Encryptor to the Application Server. See ***Provision a Netcrypt Element on the Application Server*** (on page 48) for instructions on reserving ECM PIDs.

- The operator must allow some bandwidth overhead for the insertion of ECMs. Note that the standard encoding bit rates today allow for ECM insertion in QAM modulators and are also appropriate for use with the Netcrypt Bulk Encryptor.

Summary of Addresses and Stream Header Information

This section lists some of the address and header information that must be provided to the Netcrypt Bulk Encryptor at TSR creation or CF or ES session setup. This information is also useful should system administrators need to use a GbE sniffer to inspect the UDP and IP headers of a stream.

Netcrypt Bulk Encryptor Input Stream Addresses and Headers

Broadcast CFs or TSRs using unicast

Source UDP Port:	Not used.
Source IP Address:	The value of the port sending the MPEG data to the Netcrypt.
Destination UDP Port:	■ **SPTS:** Uniquely defines input. stream ■ **MPTS:** Required along with the MPEG PN to uniquely identify a program. **Note:** Entered into the Application Server at session-setup time.
Destination IP Address:	Uses the Netcrypt Bulk Encryptor's own port IP address for the selected GbE port
MPEG PN:	■ **SPTS:** Required. PN of incoming MPEG stream. ■ **MPTS:** Required along with the Destination UDP port to uniquely define an input program. **Note:** Entered into the Application Server at session-setup time.

Broadcast CFs or TSRs using Source-Specific Multicast (SSM)

Source UDP Port:	Not used.
Source IP Address:	Not required.
Destination UDP Port:	Not required.
Destination IP Address:	A Class D Group Destination IP Address (GDA) **Note:** Entered into the Application Server at session-setup time

MPEG PN:	■ **SPTS:** Required. PN of incoming MPEG stream. ■ **MPTS:** Required along with the GDA to uniquely define an input program. **Note:** Entered into the Application Server at session-setup time.

Broadcast CFs or TSRs using any-source multicast

Source UDP Port:	Not used.
Source IP Address:	Not required.
Destination UDP Port:	Not required.
Destination IP Address:	A Class D GDA. Entered into the Application Server at session-setup time
MPEG PN:	■ **SPTS:** Required. PN of incoming MPEG stream. ■ **MPTS:** Required along with the GDA to uniquely define an input program. Entered into the Application Server at session-setup time

VOD Exclusive Sessions (always unicast SPTS)

Source UDP Port:	Not used.
Source IP Address:	**Optional:** May be provided to the Application Server by the VOD server at session-setup time
Destination UDP Port:	Provided to the VOD server by the Application Server at session-setup time, per SSP2.3
Destination IP Address:	Provided to the VOD server by the Application Server at session-setup time, per SSP2.3
MPEG PN:	Not required; usually set to zero

Netcrypt Bulk Encryptor Output Stream Addresses and Headers

Broadcast CFs or TSRs using unicast

Source UDP Port:	Not used.
Source IP Address:	The IP address of the selected Netcrypt Bulk Encryptor output port
Destination UDP Port:	■ **SB-QAM:** Uniquely defines an SPTS stream **Note:** Along with a PN, this identifier defines a program within the MPTS stream. ■ **TB-QAM:** Selected by the Application Server from the QAM mapping table in order to achieve the required RF carrier, PN, and PIDs at the output of the QAM
Destination IP Address:	IP address of the GbE port on the destination QAM modulator

Broadcast CFs or TSRs using Source-Specific Multicast (SSM)	
Source UDP Port:	Not used.
Source IP Address:	The IP address of the selected Netcrypt Bulk Encryptor output port
Destination UDP Port:	Entered into the Application Server at session-setup time. Not required to identify stream
Destination IP Address:	The GDA. Entered into the Application Server at session-setup time

Broadcast CFs or SRs using any-source multicast	
Source UDP Port:	Not used.
Source IP Address:	The IP address of the selected Netcrypt Bulk Encryptor output port
Destination UDP Port:	Entered into the Application Server at session-setup time. Not required to identify stream
Destination IP Address:	The GDA. Entered into the Application Server at session-setup time

VOD Exclusive Sessions	
Source UDP Port:	Not used.
Source IP Address:	The IP address of the selected Netcrypt Bulk Encryptor output port
Destination UDP Port:	■ **SB-QAM:** Uniquely defines an SPTS stream ■ **TB-QAM:** Selected by the Application Server from the QAM mapping table in order to achieve the required RF carrier, PN, and PIDs at the output of the QAM
Destination IP Address:	■ IP address of the GbE port on the destination QAM modulator ■ Provided to the Netcrypt Bulk Encryptor by the Application Server at session-setup time

Note A: The Source IP address is set when the Netcrypt Bulk Encryptor is provisioned on the Application Server.

Note B: Only unicasts are supported when using TB-QAM modulators.

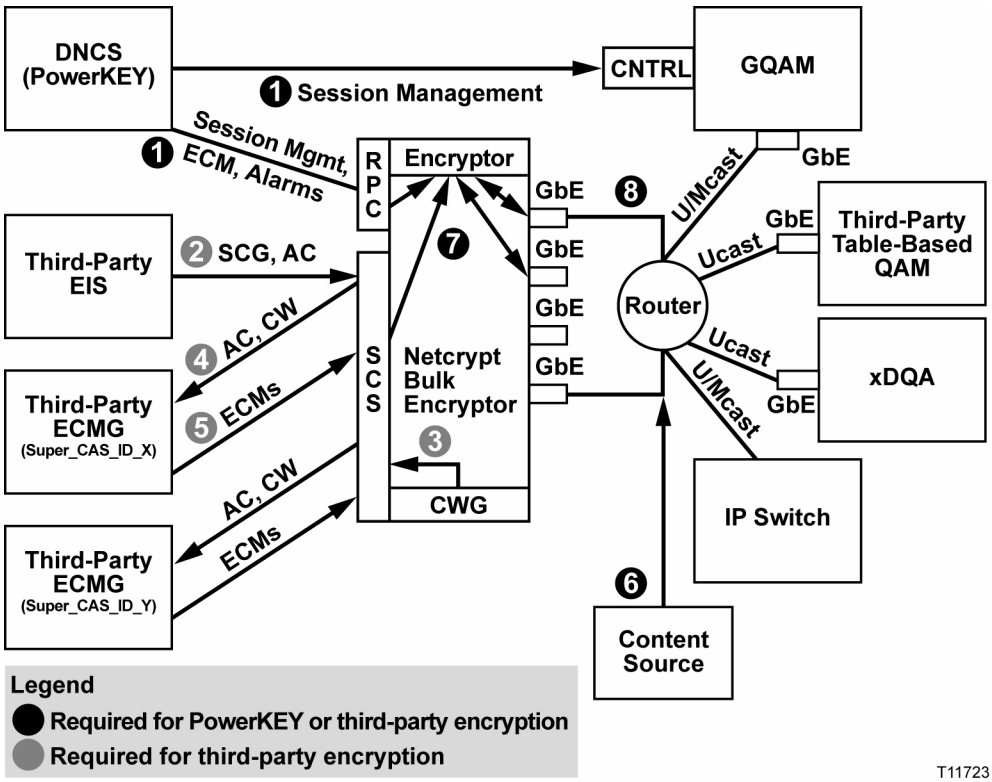
SimulCrypt Support Option

When using the SimulCrypt support option, a Netcrypt Bulk Encryptor can be deployed in a system whose hosts do not support PowerKEY decryption. This option allows the unit to supplement the PowerKEY CA system, which is always required for operation, with up to two third-party CA systems.

A Netcrypt Bulk Encryptor unit uses SimulCrypt encryption to simultaneously encrypt streams using more than one CA system. However, simultaneous encryption is not required for VOD where a stream is bound for only one set-top. For this reason, as well as for performance penalties that may occur in the extra communication paths and external components, simultaneous encryption is not recommended or supported for VOD.

When using the SimulCrypt support option, control connections are made to a Netcrypt Bulk Encryptor using the ETHB 10/100 Base-T port. This port requires an IP address assignment that is on a different IP network than the IP address assigned to the ETHA 10/100 Base-T control port, which connects the unit to the Application Server.

The following diagram shows each stage of the transport stream creation and encryption process in systems using the SimulCrypt option. Here, the ETHA port is indicated by the Remote Procedure Call (RPC) interface, and the ETHB port is indicated by the SimulCrypt Synchronizer (SCS) interface. Numbers in the diagram correspond to numbers in the table on the following page, which describe each stage of the stream creation and encryption process.



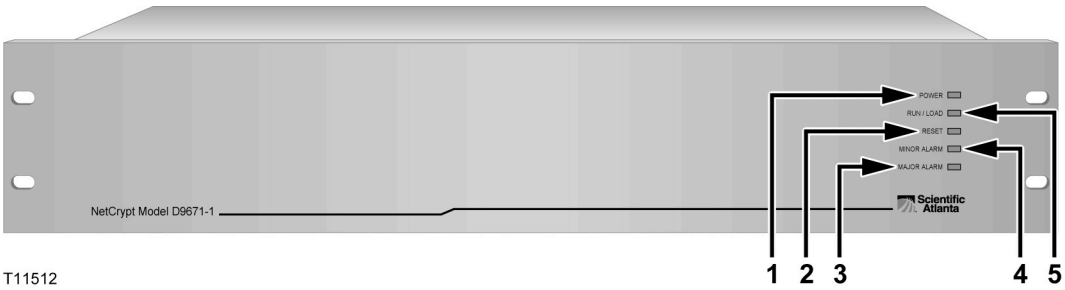
The following table describes how transport streams are encrypted when using the SimulCrypt option.

Stage	Description
1	The Application Server sends a create session request to the RPC interface on the Netcrypt Bulk Encryptor to create a PowerKEY session on the unit and delivers ECMs to this interface. The destination of the transport stream to be encrypted determines how the Application Server manages the stream: ■ If the destination is a GQAM, the Application Server creates a session on the GQAM as well, but never delivers ECMs to the GQAM because a GQAM does not encrypt Netcrypt Bulk Encryptor traffic. ■ If the destination is a TB-QAM, the mapping table of the TB-QAM provides the Application Server with the UDP port, program number, and physical output so that the Application Server is able to instruct the Netcrypt Bulk Encryptor as to the specific unicast destination of a given stream. Operators define mapping-table data for TB-QAMs when they provision TB-QAMs on the Application Server. See ***Add Table-Based QAM Information to the Application Server*** (on page 53) for more information. **Note:** If only PowerKEY is required, such as for VOD, this flow continues at stage 6.
2	If broadcast traffic requires third-party encryption, the Event Information Scheduler (EIS) sends Scrambling Control Group (SCG) provisioning messages—one message for each third-party encryption system. **Note:** A maximum of two supplemental CA systems are allowed in a Netcrypt Bulk Encryptor setting.
3	When the SCS interface receives an SCG provisioning message, it requests a control word (CW) from its Control Word Generator (CWG).
4	The SCS requests ECM computation from each required Entitlement Control Message Generator (ECMG) that applies by providing the access criteria (AC) and CW in a CW_provision message. The SCS continually requests ECM computation at a configured rate.
5	The ECMG provides the ECM streams.
6	The transport stream is fed through one of the GbE inputs of the Netcrypt Bulk Encryptor.
7	The Netcrypt Bulk Encryptor applies the appropriate encryption.
8	The Netcrypt Bulk Encryptor unicasts or multicasts the transport streams as UDP packets to the appropriate destination.

Front Panel Overview

Front Panel Diagram

This illustration shows the front panel components of the Netcrypt Bulk Encryptor. The following table describes the labeled components.



Front Panel Indicators

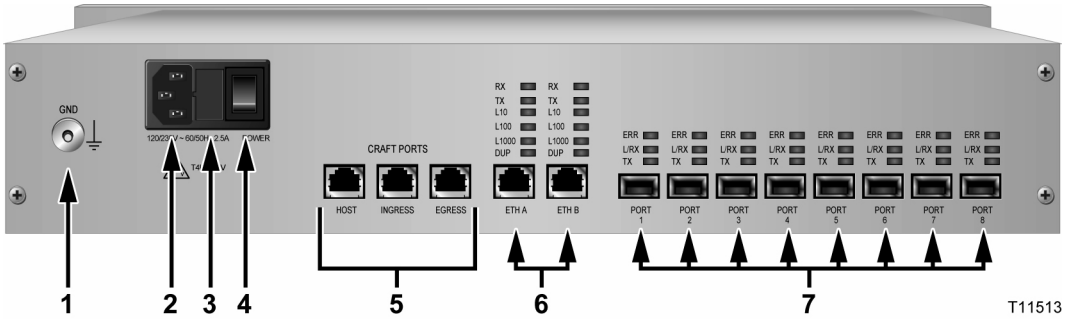
The following table provides front panel alarm and component descriptions that correspond to each number in the preceding labeled diagram of each type of Netcrypt Bulk Encryptor.

Item	Indicator	Description
1	POWER (green)	Turns solid green when the unit is receiving power
2	RUN/LOAD (green)	■ Turns solid green during normal run mode. ■ Blinks green during code downloads.
3	RESET (yellow)	Turns yellow when the Netcrypt Bulk Encryptor is reset from the Application Server or when it is reset from the back panel (by turning power off and on again).
4	MINOR ALARM (yellow)	Turns yellow for a minor alarm condition. Minor alarms indicate a less critical error condition. The Netcrypt Bulk Encryptor may continue to operate with some loss of functionality. The LED turns off when all minor alarms have cleared.
5	MAJOR ALARM (red)	Turns red for a major alarm condition. Major alarms occur for hardware or software conditions that indicate a serious disruption of service or the malfunctioning or failure of important circuits. The LED turns off when all major alarms have cleared.

Back Panel Overview

Back Panel Components

This illustration shows the back panel components of the Netcrypt Bulk Encryptor. The following table describes the labeled areas.



Back Panel Components

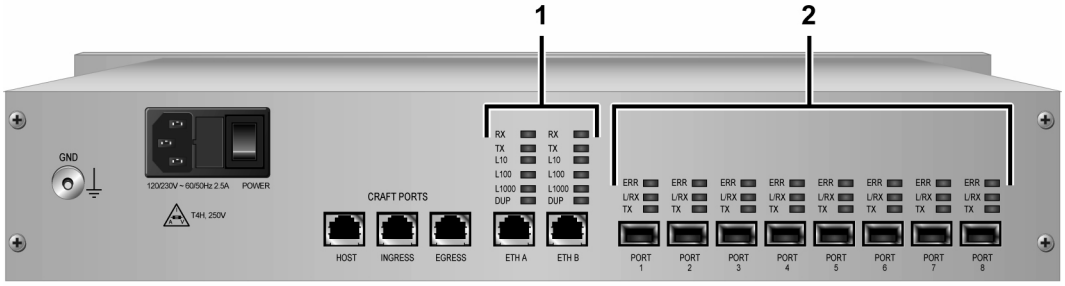
The following table describes the back panel components of the Netcrypt Bulk Encryptor.

Item	Component	Description
1	GND	Ground screw or grounding the Netcrypt Bulk Encryptor
2	AC Power Inlet	100–240 VAC 50/60 Hz 2.5 A
3	Fuse Holder	Two 4.0 A SLO BLO 250 V fuses (Cisco part number 188106)
4	Power Switch	On/off rocker-type power switch
5	CRAFT PORTs	■ **HOST:** RS-232 serial port using an RJ-45 jack ■ **INGRESS:** RS-232 serial port using an RJ-45 jack ■ **EGRESS:** RS-232 serial port using an RJ-45 jack
6	10/100/1000BASE-T port (2)	■ **ETHA:** Ethernet port shares data with Application Server Ethernet hub. ■ **ETHB:** Ethernet port is not used with the Netcrypt Bulk Encryptor.

Item	Component	Description
7	Active GbE Transceiver Ports (4), Port 1 to Port 4	Each GbE transceiver port (CH0 to CH7) is capable of transmitting and receiving MPEG transport stream data in UDP/IP over the GbE interface. By inserting a Small Form-factor Pluggable (SFP) module into a GbE port, you can use duplex multimode or single-mode fiber optic cables or Category 5e or better copper cables. **Notes:** ■ A total of 8 SFP sockets are provided: Ports 1 to 4 are active today. Ports 5 to 8 are not used. ■ There are four SFP modules included with a Netcrypt Bulk Encryptor unit. They are selected when ordering the Netcrypt Bulk Encryptor and are shipped with the Netcrypt Bulk Encryptor. Extra SFP modules may be ordered separately.

Back Panel Indicators

This illustration shows the back panel indicators for the Netcrypt Bulk Encryptor.



Back Panel Indicators

The following table describes the back panel indicators of the Netcrypt Bulk Encryptor.

Item	Indicator	Description
1	DUP	Lights to indicate that the link is operating in full duplex mode.
	L1000	Lights to indicate a traffic speed of 1000 Mbps (GbE).
	L100	Lights to indicate a traffic speed of 100 Mbps (fast Ethernet).
	L10	Lights to indicate a traffic speed of 10 Mbps (Ethernet).
	TX	Lights when transmitting data.
	RX	Lights when receiving data.

Item	Indicator	Description
2	TX	Blinks when transmitting data.
	L/RX	■ Lights when a valid Ethernet link connection exists. ■ Blinks when receiving data.
	ERR	Lights when an error is detected on the link.

2

Installing the Netcrypt Bulk Encryptor

Introduction

This chapter describes how to install the Netcrypt Bulk Encryptor into a rack and how to connect the unit to the other components within the DBDS.

Note: See ***Technical Specifications*** (on page 105) for additional technical specifications and requirements to help you install and configure the Netcrypt Bulk Encryptor in your system.

In This Chapter

Netcrypt Bulk Encryptor Installation Overview

ffIntroduction

This section summarizes the tasks required to install a Netcrypt Bulk Encryptor in a DBDS. The following sections in this chapter provide detailed instructions for completing the tasks summarized here.

Important: Read this entire guide before installing the Netcrypt Bulk Encryptor so that you are able to safely perform all installation tasks. When reading this guide, give particular attention to all safety statements.

Before You Begin

Before you begin, make certain that you have completed the following tasks:

- You have obtained a copy of your network map.
- You have access to the online help for your system release.
- You or your system administrator has installed Netcrypt software onto the Application Server.

Note: For assistance installing Netcrypt software on the Application Server, see *Netcrypt Bulk Encryptor Software Installation Instructions* (part number 78-4021238-01).

Enabling Netcrypt for SDV

Switched Digital Video (SDV) is a technique that recaptures wasted access network bandwidth by delivering selected services only where and when users are actually requesting service. The Netcrypt Bulk Encryptor receives SDV content from the Digital Content Manager (DCM) staging processor and encrypts that content based on the Application Server control. The Netcrypt Bulk Encryptor feature must be enabled on your Application Server before you can provision SDV services.

See *Provisioning the DNCS to Support SDV Services User Guide for System Release 2.8/3.8/4.3* (part number 78-4024447-01) for more information about setting up the Netcrypt Bulk Encryptor for SDV services.

Overview of Tasks Required to Install a Netcrypt Bulk Encryptor in a DBDS

The following instructions summarize the tasks required to install a Netcrypt Bulk Encryptor in a DBDS. This chapter provides detailed instructions for each task.

Important: When connecting cabling, allow enough cable length to be able to slide the Netcrypt Bulk Encryptor out of the rack for repairs. Sufficient cable length allows you to make some repairs without powering off the unit and disrupting services to customers.

1. Verify that your system meets the installation requirements.
2. Unpack and inspect the unit.
3. Record the Media Access Control (MAC) addresses from the label on the underside of each Netcrypt Bulk Encryptor and provide this information to the person who will provision the unit on the Application Server. Typically, a system administrator or Application Server operator is responsible for provisioning hardware devices on the Application Server.
4. Install the Netcrypt Bulk Encryptor into a rack.
5. Connect the Netcrypt Bulk Encryptor to an earth ground and then the power cord.
6. Connect theNetcrypt Bulk Encryptor to the Application Server through the ETHA Ethernet port.
7. If the Netcrypt Bulk Encryptor uses the SimulCrypt support option, connect the bulk encryptor to the SCS interface through the ETHB Ethernet port.
8. Connect the GbE ports according to your network wiring diagram.
9. Define the MPEG input sources, add service groups (if using VOD or xOD), and provision the Netcrypt Bulk Encryptorr using Application Server Element Provisioning according to your network wiring diagram.
10. Power on the Netcrypt Bulk Encryptor.

    Note: When power is applied to the unit for the first time, Netcrypt software is automatically downloaded from the Application Server to the unit.
11. Ensure that the Netcrypt Bulk Encryptor boots correctly and check for alarms at the Application Server.
12. Use one of the following methods to verify the output of the Netcrypt Bulk Encryptor:
    - Use an Ethernet analyzer to verify the output of the Netcrypt Bulk Encryptor.
    - Use a local DHCT to verify the output of the QAM edge device that is connected to the Netcrypt Bulk Encryptor.

Unpack and Inspect the Netcrypt Bulk Encryptor

Carrier's Responsibility

We thoroughly inspect and carefully pack all products before shipment. The carrier is responsible for safe shipping and delivery.

Important: Retain all boxes for future equipment shipping needs. The boxes are designed for shipping the Netcrypt Bulk Encryptor.

Unpacking and Inspecting Procedure

Follow these steps to unpack and inspect the Netcrypt Bulk Encryptor.

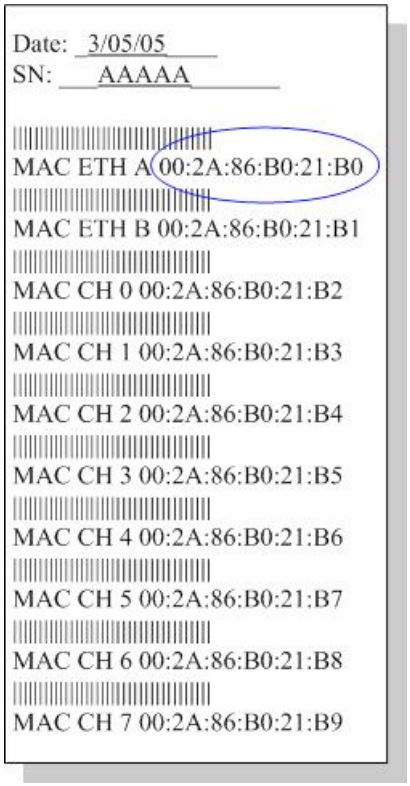
1. Review the Safety Precautions portion of this guide (page vi).
2. Inspect the shipping carton for visible damage.
3. Open the shipping carton.
4. Remove all packing material.
5. Inspect the product for visible damage.
6. Inspect for loose items that may indicate concealed damage.
7. Inspect for missing parts using the packing slip as a guide.
8. Now that you have finished unpacking and inspecting the Netcrypt Bulk Encryptor, record the Media Access Control (MAC) GbE addresses so that you or your system administrator has easy access to this information. Go to ***Record the MAC Addresses*** (on page 29).

Record the MAC Addresses

This section contains instructions for recording the MAC and GbE addresses so that you or your system administrator has easy access to this information. These addresses are needed to provision (configure) the Netcrypt Bulk Encryptor on the Application Server.

Locating the MAC Address

A label similar to the following example is on the underside of the Netcrypt Bulk Encryptor and contains the MAC addresses. As this example shows, each MAC address contains 12 characters.



Recording the MAC Address

Follow these steps to record the MAC addresses so they are readily available to provision the Netcrypt Bulk Encryptor on the Application Server.

1. If you have not already done so, unpack and inspect the Netcrypt Bulk Encryptor. See ***Unpack and Inspect the Netcrypt Bulk Encryptor*** (on page 28).
2. Locate the label containing the MAC addresses on the underside of the Netcrypt Bulk Encryptor chassis.
3. Record GbE MAC addresses here:

- GbE MAC Address 1 _____
- GbE MAC Address 2 _____
- GbE MAC Address 3 _____
- GbE MAC Address 4 _____
- GbE MAC Address 5 _____
- GbE MAC Address 6 _____
- GbE MAC Address 7 _____
- GbE MAC Address 8 _____

4 Record the Application Server Control (ETHA) MAC address here:

_____

5 Record the SCS Interface (ETHB) MAC address here:

_____

Note: A connection to the SCS interface is required only when a Netcrypt Bulk Encryptor supports the SimulCrypt support option. For more information about this option, see ***SimulCrypt Support Option*** (on page 18).

6 Now that you have recorded the MAC addresses, you are ready to install the Netcrypt Bulk Encryptor into a rack. Go to ***Install the Netcrypt Bulk Encryptor Into a Rack*** (on page 31).

Install the Netcrypt Bulk Encryptor Into a Rack

The front bezel of the Netcrypt Bulk Encryptor mounts to the front of the equipment rack. The Netcrypt Bulk Encryptor fits into an Electronic Industries Alliance (EIA) RS-310 rack mount.

Installation Requirements

This section lists the power, rack, and environmental conditions necessary for installing and operating the Netcrypt Bulk Encryptor.

Power Requirements Table

The following table describes the power specifications for the Netcrypt Bulk Encryptor.

Item	Specification
Supply Voltage	100–240 VAC 50/60Hz 2.5 A
Fuses, two	4.0 A SLO BLO 250 V AC
Line Frequency	47 to 63 Hz
Power Required	300 VA (maximum)
Power Dissipated	275 Watts (maximum)
In Current	■ 35 amps maximum, Vin = 100 VAC ■ 75 amps maximum, Vin = 240 VAC

Rack Requirements Table

The following table lists the rack requirements for the Netcrypt Bulk Encryptor.

Item	Specification
Rack Mount Type	EIA RS-310
Height	3.5 in./88.9 mm
Width	19 in./482.6 mm
Depth	22.5 in./571.5 mm
Weight	24.5 lb/11.10 kg

Environmental Requirements Table

The following table lists the environmental requirements for the Netcrypt Bulk Encryptor.

Item	Specification
Operating Temperature	0°C (32°F) to 50°C (122°F) **CAUTION:** **Avoid damage to this product! Your warranty is void if you operate this product above the maximum specified operating temperature.** **Do not obstruct air vents or fan vents on the sides of the unit. Otherwise damage can occur to the unit.** **Important:** You must use the supplied notched rack mounts (Cisco part numbers 734845 and 734846) to mount the Netcrypt Bulk Encryptor in the rack. These rack mounts allow correct air circulation through the unit.
Storage Temperature Range	-10°C (14°F) to 70°C (158°F)
Operating Humidity	5% to 95%, non-condensing
Vibration Susceptibility	No data errors with a chassis vibration of 0.5 Gs. No data errors with a vibration frequency of 10 Hz to 400 Hz
Electrostatic Shock Susceptibility	No damage sustained from five discharges of 15 KV IEC electrostatic discharge model (150pF + 150 W) to all exposed connections

Installing the Netcrypt Bulk Encryptor into a Rack

Follow these steps to install a Netcrypt Bulk Encryptor into a rack.

CAUTION:

- **Do not tangle or strain interconnecting cables.**
- **Use the notched rack mounts that are supplied to provide additional support and to allow correct air circulation through the unit. Do not obstruct the air vents or fan vents on the sides of the unit. Otherwise, damage can occur to the unit.**

1. Install the rack mounts.

   Important: You must use the supplied rack mounts (Cisco part numbers 734845 and 734846). We recommend that you use four mounting screws per rack unit so that a total of eight screws secure each set of rack mounts for the Netcrypt Bulk Encryptor. These rack mounts provide additional support along with the following:

   - A stationary assembly that attaches to the rack, but not to the Netcrypt Bulk Encryptor, and supports the unit when it is inside the rack

- Correct air circulation through the unit

  Note: Using the supplied rack mounts as described above allows you to stack Netcrypt Bulk Encryptors without requiring ventilation space between them.

2 Place the Netcrypt Bulk Encryptor in the rack on the rack mounts.

3 Insert a mounting screw through each of the four-bezel mounting holes on the front panel of the Netcrypt Bulk Encryptor and then into the rack.

4 Firmly tighten each mounting screw.

5 Now that you have mounted the bulk encryptor into a rack, you are ready to connect a power source to the Netcrypt Bulk Encryptor. Go to ***Connect an AC Power Source*** (on page 34).

Connect an AC Power Source

This section contains instructions for connecting an earth ground and an AC power source to the Netcrypt Bulk Encryptor.

WARNING:

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into the laser beam or view the beam directly with optical instruments. Doing so may pose an eye hazard.

Connecting an Earth Ground

Important: Make certain to allow enough cable length to be able to slide the Netcrypt Bulk Encryptor out of the rack for repairs. Sufficient cable length allows you to make some repairs without powering off the unit and disrupting services to customers.

Follow these steps to connect an earth ground to the Netcrypt Bulk Encryptor.

1. Place a ground wire onto the ground lug (marked **GND**) on back of the Netcrypt Bulk Encryptor; then, use your fingers to tighten the ground lug to secure the ground wire.
2. Connect the other end of the ground wire to the rack or earth ground.

Connecting an AC Power Source

Important: Make certain to allow enough cable length to be able to slide the Netcrypt Bulk Encryptor out of the rack for repairs. Sufficient cable length allows you to make some repairs without powering off the unit and disrupting services to customers.

Perform the following steps to connect a power source to the Netcrypt Bulk Encryptor.

1. Verify that the power switch on the back of the unit is placed in the **Off** position.
2. Connect the power cord to the power inlet on the back of the unit.
3. Connect the other end of the power cord to an AC electrical outlet.
4. Keep the power switch in the **Off** position until you are ready to power on the unit.
5. Now that you have connected the power source to the unit, you are ready to begin connecting the ETHA Ethernet port. Go to ***Connect the ETHA Ethernet Port for Application Server Control*** (on page 35).

Connect the ETHA Ethernet Port for Application Server Control

Description

In order to operate properly, the Netcrypt Bulk Encryptor must be connected to the Application Server control network. This connection allows operators and system administrators to use the Application Server to perform software downloads, provision the Netcrypt Bulk Encryptor, set up sessions, monitor alarms, and check system performance. The unit cannot operate autonomously without this connection.

Note: Connect the ETHA Ethernet port for Application Server control to an Ethernet hub, switch, or router as part of the Application Server control network. Do not connect this port directly to an Application Server workstation or another PC.

Connecting the ETHA Etehrnet Port for Application Server Control

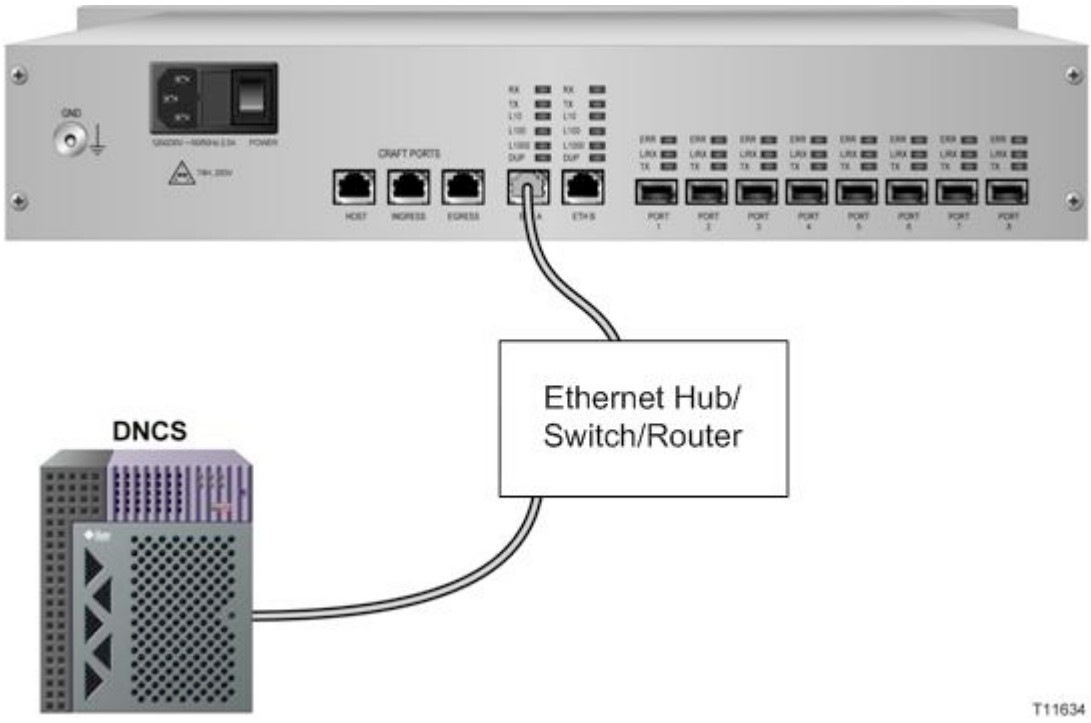
Important: Make certain to allow enough cable length to be able to slide the Netcrypt Bulk Encryptor out of the rack for repairs. Sufficient cable length allows you to make some repairs without powering off the unit and disrupting services to customers.

Follow these steps to connect the Netcrypt Bulk Encryptor to the Ethernet network.

1. Connect the ETHA port on Application Server directly to the control network hub, switch, or router.
2. Connect the 10/100BASE-T port on the Netcrypt Bulk Encryptor to the Ethernet hub, switch, or router, using Ethernet 10/100BASE-T wiring with RJ-45 connectors.

   Note: Use a screened or shielded cable, CAT-5 or better.
3. Does this Netcrypt Bulk Encryptor use the SimulCrypt support option?
   - If **no**, go to ***Connect the GbE Ports*** (on page 37).
   - If **yes**, go to ***Connect the ETHB Ethernet Port for the SimulCrypt Support Option*** (on page 43).

The following illustration shows an example of a 10/100BASE-T Ethernet connection to the Application Server. With this connection, you can establish communication between the Application Server and a Netcrypt Bulk Encryptor that has been provisioned on the Application Server.



Connect the GbE Ports

Description

The Netcrypt Bulk Encryptor uses four GbE bi-directional ports to transmit and receive MPEG-2 transport streams encapsulated in User Datagram Protocol/Internet Protocol (UDP/IP) over Ethernet. These ports are labeled Port 1 to Port 4 on the back of the Netcrypt Bulk Encryptor. Ports 5 to 8 are not used.

The Netcrypt Bulk Encryptor is intended for network-attached operation as described in ***Netcrypt Bulk Encryptor Functional Overview*** (on page 2). Bidirectional ports allow input and output streams to share the same ports between the Netcrypt Bulk Encryptor and a network element, such as a switch or router. This section lists typical input source and output devices.

Important: The Netcrypt Bulk Encryptor must be connected to an input source or output device through a switch or router. The Netcrypt Bulk Encryptor is not intended for direct connection to a content source, such as a VOD server, or to an output device, such as a QAM modulator.

Input Devices (Sources)

The Netcrypt Bulk Encryptor is compatible with MPEG-2 data in UDP/IP over GbE, such as from the following types of GbE-compliant transmitting devices:

- VOD servers
- Satellite receivers
- Ad insertion equipment
- Statistical multiplexers and other MPEG stream groomers with GbE outputs

Output Devices

After receiving and encrypting (if necessary) MPEG-2 programs, the Netcrypt Bulk Encryptor unicasts or multicasts MPEG-2 data to the following types of GbE-compliant receiving devices:

- TB-QAM modulators that are GbE-compliant, such as the eXtra Dense QAM Array (xDQA)
- Other edge devices supporting MPEG-2 transport streams encapsulated in UDP/IP/Ethernet

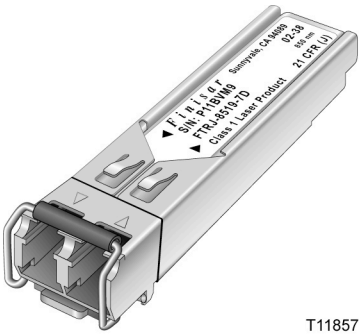
SFP Module Provides Flexibility for Cable Connections

By inserting an SFP module into a GbE port, you can use either of the following types of fiber optic or copper cables:

- **Fiber optic cables:** 850 nm or 1350 nm fiber optic cables
- **Copper cables:** Category 5e (CAT5e) or better cables

Note: SFP modules are hot-insertable and hot-removable. Removing an SFP module does not interrupt the operation of streams carried on other modules.

SFP Fiber Optic Module



T11857

SFP Copper Module

T11856

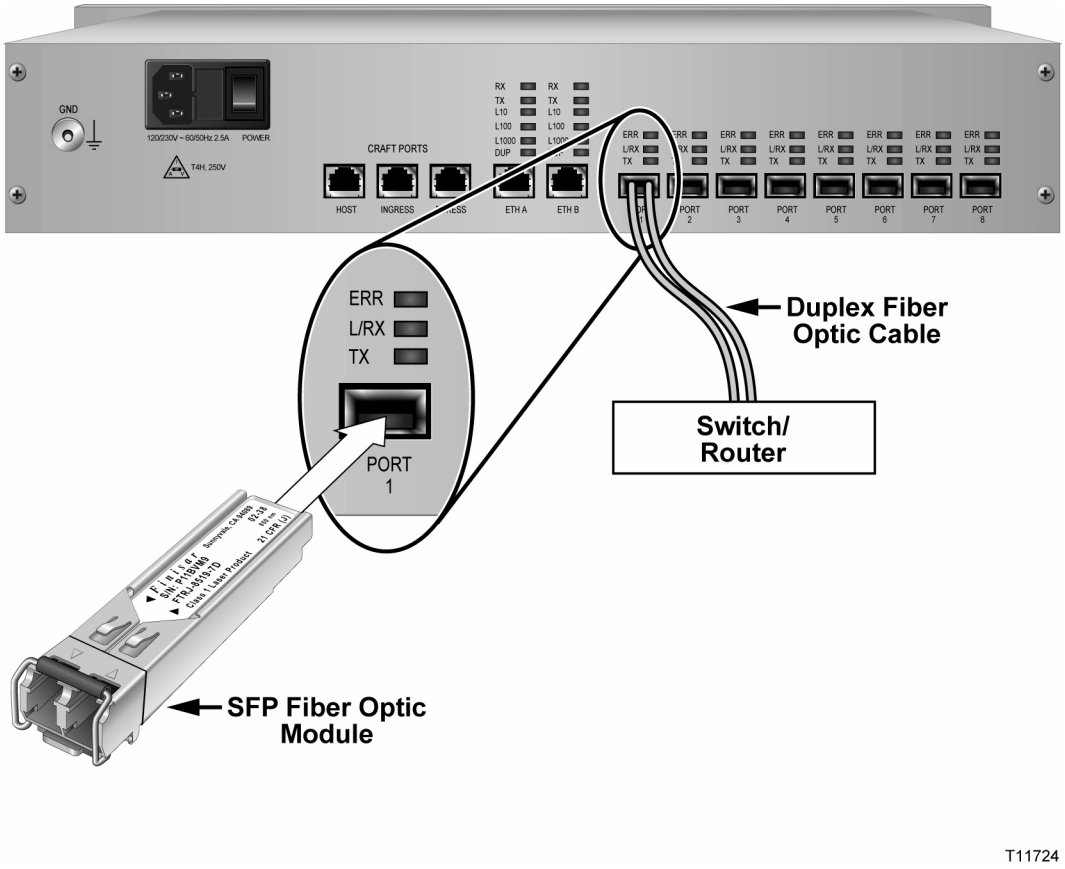
Connecting the GbE Ports

This section describes how to connect both input and output devices to GbE bi-directional ports using duplex fiber optic or copper cables.

Duplex Fiber Optic Connections

The following illustration shows an example of a GbE connection for the Netcrypt Bulk Encryptor using duplex fiber optic cables. As the illustration shows, the Netcrypt Bulk Encryptor must be connected to an input source or output device through a switch or router. Do not directly connect the Netcrypt Bulk Encryptor to a content source (such as a VOD server) or to an output device (such as a QAM modulator).

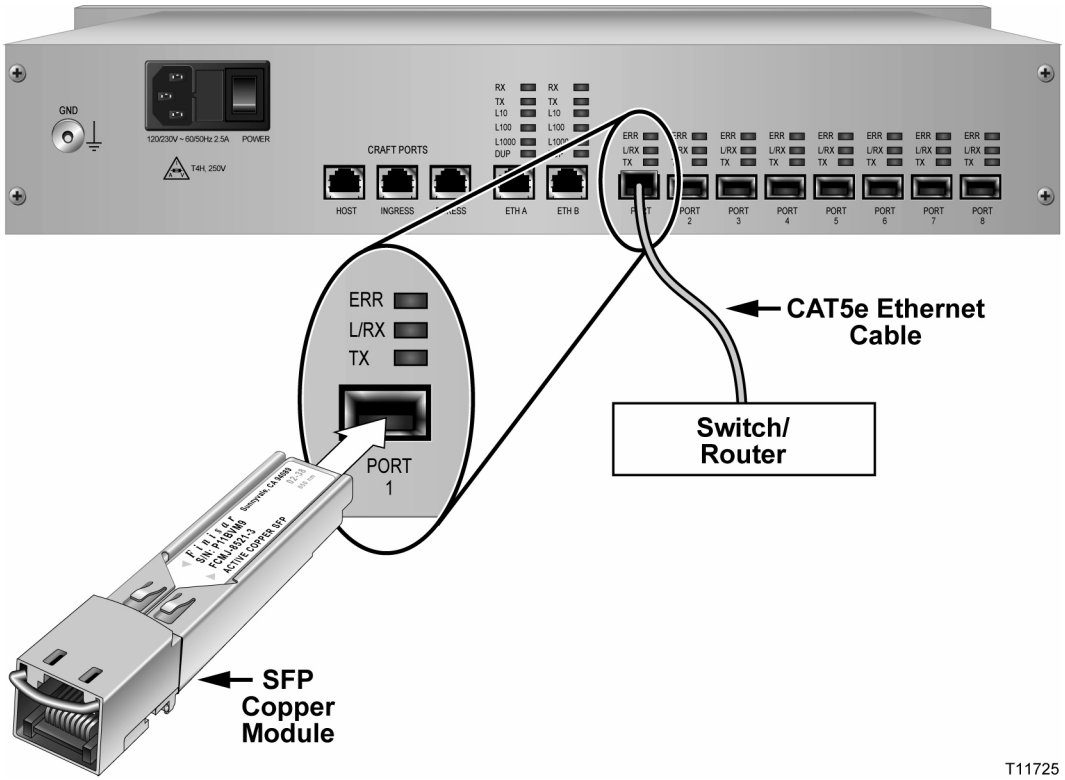
Important: Make certain to allow enough cable length to be able to slide the Netcrypt Bulk Encryptor out of the rack for repairs. Sufficient cable length allows you to make some repairs without powering off the unit and disrupting services to customers.



Category-5e Copper Connections

The following illustration shows an example of a GbE connection for the Netcrypt Bulk Encryptor using CAT5e copper cables. As the illustration shows, the Netcrypt Bulk Encryptor must be connected to an input source or output device through a switch or router. Do not directly connect the Netcrypt Bulk Encryptor to a content source (such as a VOD server) or to an output device (such as a QAM modulator).

Important: Make certain to allow enough cable length to be able to slide the Netcrypt Bulk Encryptor out of the rack for repairs. Sufficient cable length allows you to make some repairs without powering off the unit and disrupting services to customers.



To Connect Input and Output Devices to GbE Ports

Follow these instructions to connect input and output devices to GbE ports using fiber optic or copper cables.

Important! Make certain to allow enough cable length to be able to slide the Netcrypt Bulk Encryptor out of the rack for repairs. Sufficient cable length allows you to make some repairs without powering off the unit and disrupting services to customers.

WARNING:

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into the laser beam or view the beam directly with optical instruments. Doing so may pose an eye hazard.

Note: SFP modules are hot-insertable and hot-removable, which means you can remove and replace an SFP module without powering down the bulk encryptor or interrupting encryption functions. In addition, removing an SFP module does not interrupt the operation of streams carried on other modules.

1 Remove the SFP module from its protective packaging.

2 Insert the SFP module into one of the four active GbE ports until the module clicks firmly in place.

The first four ports of Netcrypt Bulk Encryptor are active GbE ports. GbE ports 5 to 8 are not used.

3 If necessary, remove the rubber dust plug from the SFP module port, and store it for later use.

4 Follow these instructions to connect the Netcrypt Bulk Encryptor to the switch or router:

- **Fiber-optic SFP modules.** Insert the fiber-optic duplex connector into the SFP module. Then insert the other end of the fiber-optic cable into a fiber-optic receptacle on the switch or router.
- **Copper SFP modules.** Insert the RJ-45 cable connector into the SFP module. Then insert the other end of the cable into an RJ-45 receptacle on the switch or router.

5 To connect another SFP module to another GbE port, repeat steps 1 to 4.

6 Has the Netcrypt Bulk Encryptor been provisioned in the Application Server?

- If **yes**, go to step 7.
- If **no**, contact your system administrator or Application Server operator and request that the Netcrypt Bulk Encryptor be provisioned in the Application Server.

Notes:

– System administrators or Application Server operators typically provision a Netcrypt Bulk Encryptor in the Application Server at the same time that they load Netcrypt software onto the Application Server.

– See ***Provisioning the Netcrypt Bulk Encryptor and Associated Devices*** (on page 45) for assistance provisioning the Netcrypt Bulk Encryptor on the Application Server.

7 Has Netcrypt software been loaded onto the Application Server?

- If **yes**, go to step 8.
- If **no**, contact your system administrator or Application Server operator and request that Netcrypt software be loaded onto the Application Server.

Note: See *Netcrypt Bulk Encryptor Software Installation Instructions* (part number 78-4021238-01) for instructions on installing Netcrypt software on the Application Server.

8. Turn power on to the Netcrypt Bulk Encryptor by moving the **Power** switch on the back of the unit to the **ON** position. The Netcrypt Bulk Encryptor automatically downloads the Netcrypt software from the Application Server to the bulk encryptor.
9. Verify the output of the Netcrypt Bulk Encryptor by using one of the following methods:
   - Use an Ethernet analyzer (sometimes referred to as an Ethernet sniffer) to verify the output of the Netcrypt Bulk Encryptor. For assistance, see the documentation provided by the vendor of the Ethernet analyzer.
   - Use a local DHCT to verify the output of the QAM edge device that is connected to the Netcrypt Bulk Encryptor.

Connect the ETHB Ethernet Port for the SimulCrypt Support Option

Introduction

When using the SimulCrypt support option, the Netcrypt Bulk Encryptor shares data with a third-party CA system through the second Ethernet port (ETHB). This port provides an SCS interface that allows a third-party CA protocol to run on the Netcrypt Bulk Encryptor in conjunction with PowerKEY encryption.

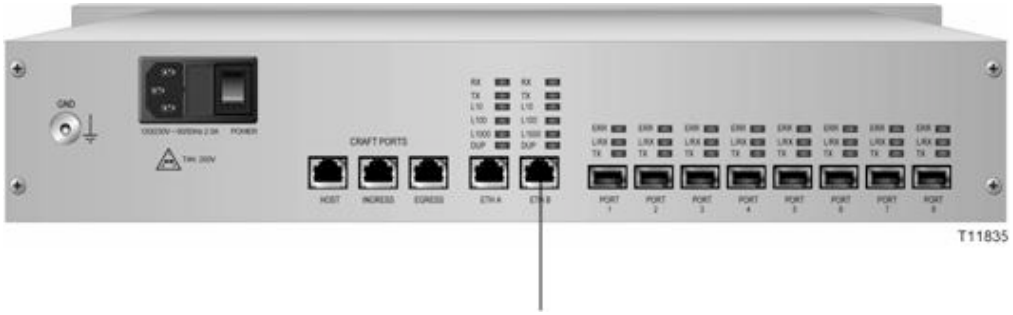
Connecting the ETHB Ethernet Port for the SimulCrypt Support Option

Important: Make certain to allow enough cable length to be able to slide the Netcrypt Bulk Encryptor out of the rack for repairs. Sufficient cable length allows you to make some repairs without powering off the unit and disrupting services to customers.

Follow these steps to connect the Netcrypt Bulk Encryptor to the ETHB port for optional SimulCrypt support.

1. Connect the ETHB port on the Netcrypt Bulk Encryptor to the third-party conditional access device using CAT-5 Ethernet 10/100BASE-T wiring with RJ-45 connectors.
2. After connecting the ETHB port for the SimulCrypt support option, connect the GbE bi-directional ports. Go back to ***Connecting the GbE Ports*** (on page 38).

The following illustration shows the location of the 10/100BASE-T ETHB port used for optional SimulCrypt support.



Connect third-Party CA equipment to this port when the SimulCrypt support option is used.

3

Provisioning the Netcrypt Bulk Encryptor and Associated Devices

This chapter provides instructions for using new windows, buttons, and other tools on the Application Server to provision (configure) a Netcrypt Bulk Encryptor as a DBDS network element. This chapter also provides instructions for provisioning devices that provide data to a Netcrypt Bulk Encryptor as well as devices that receive data from a Netcrypt Bulk Encryptor.

Notes:

- See ***Technical Specifications*** (on page 105) and consult your network wiring diagram when you provision the bulk encryptor to ensure a proper allocation of bandwidth.
- See the Application Server online help for more information about the Application Server and operating the Application Server software.

In This Chapter

Provisioning Overview

This section provides an overview of how to provision a Netcrypt Bulk Encryptor on the Application Server. It also describes how to provision devices that provide data to a Netcrypt Bulk Encryptor and the devices that receive data from a NOBE.

Why Provision a Netcrypt Bulk Encryptor?

Provisioning a Netcrypt Bulk Encryptor establishes communication between the Application Server and the bulk encryptor and allows the bulk encryptor to automatically download software from the Application Server. Without Application Server control, the Netcrypt Bulk Encryptor is inoperable.

Before You Begin

Before you begin provisioning a Netcrypt Bulk Encryptor and its associated devices, first make certain that you have completed the following tasks:

- You have verified that the Netcrypt Bulk Encryptor is installed and is powered down.
- You have obtained a copy of your network map.

Note: If you cannot locate your network map, contact Cisco Services for assistance.

Overview of Provisioning a Netcrypt Bulk Encryptor and Associated Devices

Follow these steps to provision a Netcrypt Bulk Encryptor and its associated devices.

1. Make certain that all the devices you will provision have been installed in your headend or hub. If necessary, see the vendor's document for assistance in installing these devices.
2. Provision one MPEG Source element for each device that provides the Netcrypt Bulk Encryptor with data. The Application Server uses the generic term MPEG Source to represent any device that generates MPEG output, such as a VOD server or broadcast multiplexer.

   Note: For assistance provisioning an MPEG Source element, refer tosee the Application Server online help.
3. Provision a Netcrypt element by completing the following tasks.

   Note: These tasks are described in detail in ***Provision a Netcrypt Element on the Application Server*** (on page 48).

   a. Add a Netcrypt element to the Application Server, but do not place the element online.

   b. Provision the Ethernet ports on the Netcrypt element.

   c. If you are using the SimulCrypt support option, provision the Netcrypt element for this option.

d Verify that the Netcrypt Bulk Encryptor has successfully booted, and place the Netcrypt element online.

4 Add the following elements to the Application Server according to your system configuration:

- If the Netcrypt Bulk Encryptor provides input to TB-QAMs, such as an xDQA, enter information about the TB-QAMs into the Application Server. For assistance, see ***Add Table-Based QAM Information to the Application Server*** (on page 53).
- If the Netcrypt Bulk Encryptor feeds GQAM modulators, the Application Server can be used to supply GQAM modulator provisioning parameters. For assistance with GQAM modulators, see the Application Server online help.

5 Provision GbE transport network elements to specify the connectivity between a Netcrypt Bulk Encryptor and other devices, such as TB-QAMs or GQAMs. For assistance, see ***Create GbE Transport Network Elements*** (on page 58).

6 After provisioning a Netcrypt Bulk Encryptor and its associated devices, set up CF sessions and TSRs on the Netcrypt Bulk Encryptor. For assistance, see ***Setting Up CF Sessions and Transport Stream Routes on a Netcrypt Bulk Encryptor*** (on page 65).

Provision a Netcrypt Element on the Application Server

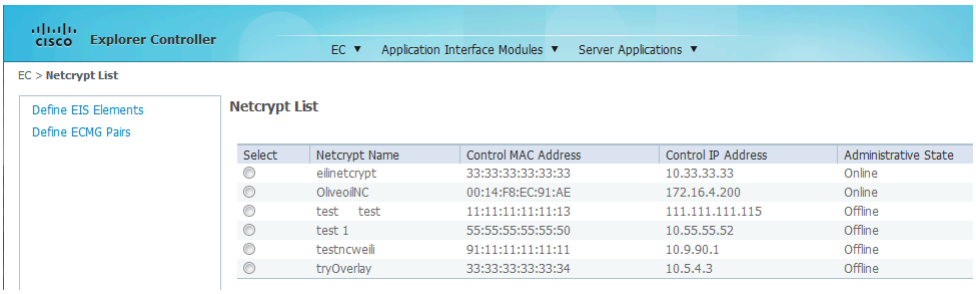
This section provides instructions for completing each of the following tasks that are required to provision a Netcrypt element on the Application Server. Provisioning a Netcrypt element on the Application Server establishes communication between the Application Server and the Netcrypt Bulk Encryptor. Without Application Server control, the Netcrypt Bulk Encryptor is inoperable.

1. Add a Netcrypt element to the Application Server, but do not place the element online.
2. Provision the Ethernet ports on the Netcrypt element.
3. If you are using the SimulCrypt support option, provision the Netcrypt element for this option.
4. Verify that the Netcrypt Bulk Encryptor has successfully booted, and place the Netcrypt element online.

Adding a Netcrypt Element to the Application Server

Follow these instructions to add a Netcrypt element to the Application Server.

1. Click **EC** and then select **Netcrypt** under the Network Element Provisioning area. The Netcrypt List window opens and shows the Netcrypt elements that have been provisioned on the Application Server.



2. Click **Add**. The New Netcrypt window opens.
3. Follow these instructions to enter data in the fields of the Netcrypt Provisioning area on the New Netcrypt window:
   - **Netcrypt Name** – Enter a name for the unit that is consistent with the naming scheme used on your network map. We recommend that you establish a naming scheme that allows you to easily identify the unit and where it resides. For example, a name of **NBE43hub1** could represent a Netcrypt Bulk Encryptor whose IP address ends in 43 and processes data for Hub 1.

     Note: You can use up to 20 alphanumeric characters in this field.
   - **Administrative State** – Leave this set to **Offline** for now. Later, when the Netcrypt Bulk Encryptor is completely provisioned and successfully booted, you will set this to Online.

- **Netcrypt MAC Address –** Enter the MAC Address of the control port (ETHA) for this Netcrypt Bulk Encryptor. Make certain to separate each pair of characters in the 12-character address with a colon, for example 00:00:00:00:00:00.

  Note: This address was recorded in ***Recording the MAC Address*** (on page 29) by the person who installed the Netcrypt Bulk Encryptor in the headend or hub.

- **Netcrypt IP Address –** Enter the IP address of the control port (ETHA) for this Netcrypt Bulk Encryptor. (You can obtain this address from your network map or from your system administrator.)
- **Subnet Mask –** Enter the subnet mask for this subnet.
- **Model Type –** Select the model type for this Netcrypt Bulk Encryptor.
- **Default Gateway –** If your system uses a default gateway, enter the IP address of your default gateway. This is required for a network using routers (layer 3).
- **Headend –** Select the headend where this Netcrypt Bulk Encryptor resides.
- **Configuration File –** Do not change the default setting (nc.config) entered in this field.

  Note: When power is applied to the Netcrypt Bulk Encryptor for the first time, or when the unit rebooted, it uses the nc.config file to determine if the correct version of code has been installed on the unit. If the Netcrypt Bulk Encryptor determines that an incorrect version of code has been installed, it requests that the correct code be downloaded.

4 Leave the fields in the Constraints area of the New Netcrypt window with their default settings:

- **Max Session Count (Default: 4000) –** Maximum number of sessions this Netcrypt Bulk Encryptor will support.
- **Nominal Session Capacity (Default: 4000) –**The number of sessions that trigger a Session Capacity Exceeded (major) alarm.
- **Alarm Threshold % (Default: 80) –** The number of sessions that trigger an alarm when the Netcrypt Bulk Encryptor reaches 80% of its rated session capacity.
- **Severity Level (Default: WARNING) –**The type of alarm triggered when the Netcrypt Bulk Encryptor reaches its alarm threshold percent.
- **Application Server Msg Timeout (seconds) (Default: 30) –** Number of seconds allowed for messages to be sent from the Netcrypt Bulk Encryptor to system components that do not use PowerKEY CA, such as the EIS and ECMGs.

  Note: The settings in the Constraints area are required only for Netcrypt Bulk Encryptors that use the SimulCrypt Support option.

5 Follow these instructions to enter data in the fields of the Reserved ECM PID Range area on the New Netcrypt window:

- **Start of Reserved PIDs –** Enter the first PID that you want to reserve. For example, if you want to reserve PIDs 99 to 103, type 99 in this field.
- **Number of Reserved PIDs –** Enter the number of PIDs that you want to reserve. For example, if you want to reserve PIDs 99 to 103, enter 5 in this field.

Note: Reserving PIDs prevents a PID conflict by instructing the bulk encryptor to use reserved PIDs for ECM insertion. If a PID from the reserved range is used in existing streams, a PID conflict may occur. For more information, see ***MPEG Transport Layer Rules*** (on page 15).

6 Click **Save**. The New Netcrypt window closes and the Netcrypt element you saved appears in the list.

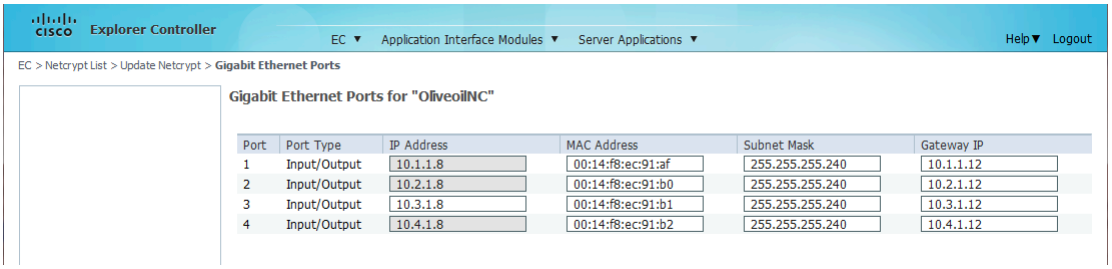
7 Continue provisioning this Netcrypt element by configuring the Ethernet ports for this bulk encryptor. Go to ***Provisioning Gigabit Ethernet Ports for a Netcrypt Element*** (on page 50).

Provisioning Gigabit Ethernet Ports for a Netcrypt Element

After the Netcrypt element is listed in the Netcrypt List window, follow these instructions to provision the Gigabit Ethernet ports for the Netcrypt element you added to the New Netcrypt window.

1 From the Netcrypt List window, select the Netcrypt Bulk Encryptor whose ports you want to configure, and click **Edit**. The Update Netcrypt window opens for this Netcrypt element.

2 Click **Ethernet Ports**. The Gigabit Ethernet ports window opens for the Netcrypt element you have added to the Application Server. The window is similar to the following example.



3 Follow these instructions to configure the Ethernet ports by entering data in the fields that do not already contain data:

- **IP Address –** Enter the IP address assigned to each GbE port that this Netcrypt Bulk Encryptor uses.
- **MAC Address –** Enter the MAC address of each GbE port that this Netcrypt Bulk Encryptor uses. Make certain to separate each pair of characters in the 12-character address with a colon, for example 00:00:00:00:00:00.
- **Subnet Mask –** If your system uses a subnet mask and it does not appear in this field, enter the subnet mask that this port uses.

- **Gateway IP –** If your system uses routers, enter the gateway IP address for each GbE port.

4 Click **Save**. The Application Server saves the information you entered and updates the window to display the ports you defined.

5 Continue provisioning the Netcrypt Bulk Encryptor according to your system configuration:

- If this Netcrypt Bulk Encryptor does not use the SimulCrypt option, provisioning for this bulk encryptor is complete, and it is ready to be placed online. Go to ***Placing a Netcrypt Bulk Encryptor Online*** (on page 51).
- If this Netcrypt Bulk Encryptor uses the SimulCrypt support option, configure the bulk encryptor for this option. Go to ***Provision a Netcrypt Bulk Encryptor for the SimulCrypt Support Option*** (on page 61).

Placing a Netcrypt Bulk Encryptor Online

After you have configured the GbE ports that the Netcrypt Bulk Encryptor uses and, if necessary, have configured the unit for the SimulCrypt support option, place the Netcrypt element online in the Application Server. The process applies to a Netcrypt Bulk Encryptor that has successfully booted and is capable of communicating with the Application Server, that is, the bulk encryptor can be reached by sending a ping.

Important: If this Netcrypt Bulk Encryptor was just installed in your headend or hub and you are placing it online for the first time, make certain that the unit has completed its boot process and downloaded the Netcrypt software before placing the Netcrypt Bulk Encryptor online. (The Netcrypt Bulk Encryptor automatically downloads Netcrypt software when power is applied to the unit.)

Follow these instructions to place a Netcrypt Bulk Encryptor that has successfully booted online in the Application Server.

1 Did you confirm that this Netcrypt Bulk Encryptor has successfully booted?

- If **yes**, go to step 2.
- If **no**, verify that the Netcrypt Bulk Encryptor has successfully booted.

2 In the path at the top of the window, click **Update Netcrypt**. The Update Netcrypt Element window opens for this Netcrypt Bulk Encryptor.

3 In the Netcrypt Provisioning area, set the Administrative State to **Online** and click **Save**. The Application Server saves this change and places the unit online.

4 Do you need to provision another Netcrypt element on the Application Server?

- If **yes**, click Netcrypt List in the path at the top of the window and begin provisioning another Netcrypt element on the Application Server. For assistance, go to ***Provision a Netcrypt Element on the Application Server*** (on page 48).
- If **no**, you have provisioned elements for all the Netcrypt Bulk Encryptors in your system. Click **Exit** to close the Netcrypt List window.

5 Now that you have provisioned this Netcrypt Bulk Encryptor, continue provisioning related elements according to your system configuration as follows:

- If this Netcrypt Bulk Encryptor feeds a TB-QAM, such as the xDQA, add information about the TB-QAM to the Application Server. For assistance, go to ***Add Table-Based QAM Information to the Application Server*** (on page 53).
- If the Netcrypt Bulk Encryptor feeds GQAM modulators, provision the GQAM modulators on the Application Server. For assistance, see the Application Server online help.

  Note: When you have provisioned the GQAM modulator elements, provision the GbE transport network elements that specify connectivity between the Netcrypt Bulk Encryptor and other elements. For assistance, see ***Create GbE Transport Network Elements*** (on page 58).

Add Table-Based QAM Information to the Application Server

This section provides instructions for completing the following tasks that are required in order to add TB-QAM modulator information to the Application Server. The Application Server uses this information to direct program streams to a TB-QAM that a Netcrypt Bulk Encryptor feeds.

1. Add a TB-QAM modulator element to the Application Server.
2. Enter the RF parameters for a TB-QAM modulator.
3. Enter the mapping table for a TB-QAM modulator.

Although adding TB-QAM information to the Application Server is very similar to provisioning elements on the Application Server, the results are different: Unlike most Application Server elements, the Application Server does not control TB-QAMs. Instead, the Application Server uses the information you have entered about TB-QAMs to direct program streams to TB-QAMs when required.

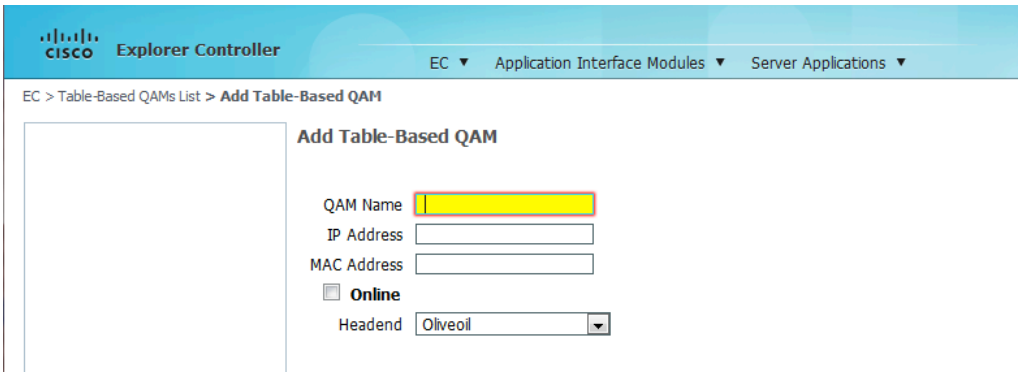
For more information on TB-QAM modulators, see ***Support for Table-Based QAMs*** (on page 7).

Adding a TB-QAM Modulator Element to the Application Server

Follow these instructions to add a TB-QAM modulator element to the Application Server.

Note: Adding a TB-QAM modulator element to the Application Server does not allow the Application Server to provision or communicate with the TB-QAMs you add. Instead, the Application Server uses the information you enter to direct program streams to TB-QAM modulators when required.

1. Click **EC** and then select **Table-Based QAM** under the Network Element Provisioning area. The Table-Based QAMs List window opens.
2. Click **Add**. The Add Table-Based QAM window appears, similar to the following example.



3 Follow these instructions to enter data in the fields of the Add Table-Based QAM window:

- **QAM Name** – Enter a name for the TB-Modulator that is consistent with the naming scheme used on your network map. We recommend that you establish a naming scheme that allows you to easily identify the TB-QAM modulator and where it resides. For example, a name of **xDQA43hub1** could represent a TB-QAM modulator whose IP address ends in 43 and processes data for Hub 1.
- **IP Address** – Enter the IP address of the GbE interface for this TB-QAM modulator. (You can obtain this address from your network map or from your system administrator.)
- **MAC Address** – Enter the MAC Address of the GbE interface for this TB-QAM modulator. Make certain to separate each pair of characters in the 12-character address with a colon, for example 00:00:00:00:00:00.
- **Online** – Click the Online option to place the TB-QAM modulator online.
- **Headend** – Click the Headend arrow and select the headend where this TB-QAM modulator resides.

4 Click **Save**. An Alert window displays to let you know that the Application Server saved the information.

5 Click **OK**. The Alert window closes and the Table-Based QAMs List window updates to show the TB-QAM modulator in the list.

6 Now that you have added the TB-QAM modulator to the Application Server, configure the RF parameters for the TB-QAM modulator. Go to ***Enter RF Output Information Into the Application Server*** (on page 54).

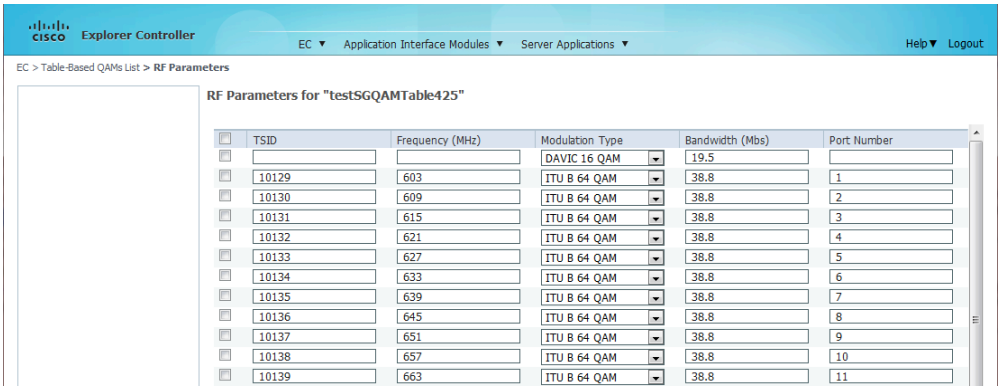
Enter RF Output Information Into the Application Server

Follow these instructions to enter the RF ouptput configuration information for this TB-QAM modulator into the Application Server.

1 In the Table-Based QAM window, select a filter to view table-based QAMs.

2 Select the TB-QAM modulator that you just added and click **Configure RF Parameters**. The RF Parameters window opens for this TB-QAM modulator.

3 Click **Add**. New data fields appear similar to the following example:



TSID	Frequency (MHz)	Modulation Type	Bandwidth (Mbs)	Port Number
		DAVIC 16 QAM	19.5	
10129	603	ITU B 64 QAM	38.8	1
10130	609	ITU B 64 QAM	38.8	2
10131	615	ITU B 64 QAM	38.8	3
10132	621	ITU B 64 QAM	38.8	4
10133	627	ITU B 64 QAM	38.8	5
10134	633	ITU B 64 QAM	38.8	6
10135	639	ITU B 64 QAM	38.8	7
10136	645	ITU B 64 QAM	38.8	8
10137	651	ITU B 64 QAM	38.8	9
10138	657	ITU B 64 QAM	38.8	10
10139	663	ITU B 64 QAM	38.8	11

4 Follow these instructions to enter data in the new data fields:
   - **TSID –** Enter the TSID that has been assigned to the RF carrier to uniquely identify the output transport stream. This number is used by DHCTs to automatically identify their service groups.
   - **Frequency –** Enter the frequency assigned for this port (carrier).
   - **Modulation Type –** Enter the type of modulation that has been set for this port (carrier).
   - **Bandwidth –** Enter the bandwidth that you want to assign to this port (carrier).
   - **Port Number –** Enter a number for this port (carrier). For example, a TB-QAM with 16 carriers would have ports 1 through 16.
5 Click **Save**. The Table-Based QAM RF Parameters window updates to show the settings for this RF channel.
6 Repeat steps 3 through 5 to configure additional RF ports (carriers) for this TB-QAM modulator. When you are done, go to step 7.
7 In the path at the top of the window, click **Table-Based QAMs List** to return to the Table-Based QAMs List window.
8 Now that you have entered the RF output information for this TB-QAM, enter the mapping table for this TB-QAM into the Application Server. Go to ***Enter the Mapping Table of a TB-QAM*** (on page 55).

Enter the Mapping Table of a TB-QAM

This section provides instructions on entering mapping tables for TB-QAMs into the Application Server. Mapping tables are provided by the QAM manufacturer and are used to define static "session pipes" through a TB-QAM. They map a set of destination UDP port numbers at the input to the TB-QAM to a set of MPEG program numbers and PIDs on specific carriers at the output of the TB-QAM. For more information on mapping tables, see ***Support for Table-Based QAMs*** (on page 7).

Note: The terms RF "carrier" and output "port" are used interchangeably on the Application Server when referring to the output of a QAM modulator. The Application Server is unaware of physical ports on a QAM modulator and how many carriers are present on those physical ports. However, it is important that all carriers on a physical output port of a modulator be assigned to the same service groups.

Follow these instructions to enter the mapping table for a TB-QAM modulator into the Application Server.

1 Select the TB-QAM modulator whose mapping table you want to configure, and click **Configure Session Data**. The Table-based Session Data window opens for the TB-QAM modulator you selected.

2. Do you want to use an automated method to enter the mapping table for this TB-QAM modulator?
   - If **no**, go to step 11 to enter the table manually.
   - If **yes**, go to step 3 to upload a comma separated value file (.csv) and have the Application Server map the streams for you.

     Important: Each line of the .csv file must list values for the following parameters that the TB-QAM modulator uses to map each transport stream. The values must be listed in the following order from left to right, and each value must be separated by a comma. For example, 1, 1, 1, 1, 51, 47.
     - UDP port number: 1 in this example
     - Output port carrier number: 1 in this example
     - Program number: 1 in this example
     - Low PID number: 1 in this example
     - High PID number: 51 in this example
     - QAM TSID: 47 in this example

     Note: If not provided, the QAM TSID must be derivable based on the UDP port.
3. Click **File Upload** to set up mapping-table data. The File load Session Data window opens.
4. Click **Browse**. The File Upload window opens.
5. Select the .csv file that contains the mapping table for this TB-QAM modulator. The File name field in the bottom of the File Upload window displays the file you selected.

   Note: You may need to scroll through the list to find and select the file.
6. Click **Open**. The File Upload window closes and the file you selected appears in the Browse field.
7. Click **Load**. An Alert window prompts you to save the entries that have been uploaded.
8. Click **OK**. The Table-based Session Data now shows the data that has been uploaded.

   Note: Depending on the number of transport streams to be set up, it may take a moment for the Application Server to display all of the data for the mapping table.
9. Click **Save Changes**. An Alert window notifies you that sessions were saved.
10. Click **OK**, and go to step 13.
11. Click **Add**. A group of fields containing zeros appears in the window.
12. Obtain the following data from the QAM manufacturer or installer, and enter data in each of the fields on the Table-based Session Data window:
    - UDP Port
    - Output Port

- Program Number
- Low PID
- High PID
- QAM TSID (This number is assigned by the system.)

13 Click **Save**. An Alert message appears to let you know that this information was saved in the Application Server database.

14 Click **OK**. The Table-based Session Data now shows the data that you entered for this transport stream.

15 To map additional transport streams on this TB-QAM modulator, repeat steps 11 to 14 as many times as necessary.

Now that you have entered the TB-QAM information into the Application Server, create the GbE transport networks that connect Netcrypt Bulk Encryptors to QAM modulators. For assistance, see ***Create GbE Transport Network Elements*** (on page 58).

Create GbE Transport Network Elements

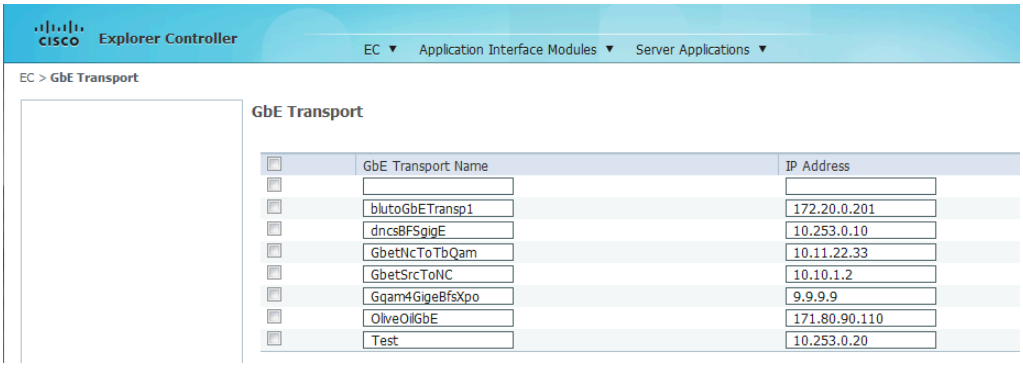
This section provides procedures for creating a GbE transport network on the Application Server. As discussed in Theory of Operation, a GbE transport network is a logical concept, not a physical device. Creating a GbE transport network allows you to specify and limit connectivity between Netcrypt Bulk Encryptors and QAM modulators. This is done by creating GbE transport networks with arbitrary numbers of connection "ports" and indicating the Netcrypt Bulk Encryptors, QAM modulators, and sources that are connected to those networks using the procedures in this section.

Creating a GbE Transport Network

Follow these instructions to create a GbE Transport network on the Application Server and connect it to a Netcrypt element and appropriate edge device, such as a TB-QAM modulator.

1 Click **EC** and then select **Gbe** under the Network Element Provisioning area. The GbE Transport List window opens and shows all GbE transport networks that have been created on the Application Server.

2 Click **Add**. A new line appears at the top of the GbE Transport Window.



3 Enter the following information in the fields of the Basic Parameters tab:

- **GbE Transport Name** – A name for the transport network.

  Note: You can use up to 20 alphanumeric characters. We recommend that you establish a naming scheme that allows you to easily identify this transport network and where it resides. For example, a name of **CFhub1GTN43** could represent a GbE transport network that connects to Hub 1 and is connected to a NOBE by a device whose IP address ends in 43.

- **IP Address** – The IP address of the transport device, such as a switch or router, that is physically connected to this Netcrypt Bulk Encryptor.

Note: This address is not used by the Application Server and simply provides a convenient place to save and retrieve this information should you wish to ping or telnet to the router or switch for monitoring or diagnostic purposes.

4. Click **Save**. The Application Server saves this data and makes the Connectivity tab available for you to select.
5. Click the Connectivity tab, and re-size the window to view all of the tab.
6. Click **Create Port**. The Port Number Prompt window opens.
7. Enter a number to identify the input port on the GbE transport network device that will receive data from a Netcrypt Bulk Encryptor or other source and click **OK**. The Port Number Prompt window closes, and a box representing the port appears in the Input Port column.
8. For each additional input port on the GbE transport network device, repeat steps 7 and 8 to create these input ports.
9. Click **Create Port**. The Port Number Prompt window opens.
10. Click **Output**. The Output port type option turns on.
11. Enter the number to identify the output port on the GbE transport network device that will be used to forward data to other devices in the transport network, and click **OK**. The Port Number Prompt window closes, and a box representing the port appears in the Output Port column.
12. For each additional output port on the GbE transport network device, repeat steps 10 through 12 to create these output ports.
13. Click an **Input Ports** box to enable it, then define how this input port on the GbE transport network device connects to the Netcrypt Bulk Encryptor or other source by entering the following information in each of the Connect To fields:
    - **Headend Name –** Select the headend that contains the Netcrypt Bulk Encryptor or other source that is physically connected to this input port on the GbE transport network device.
    - **Device Type –** Select the Netcrypt Bulk Encryptor, MPEG Source, or another GbE transport network as the type of device that sends data to this input port on the GbE transport network device.
    - **Device Name –** Select the name of the Netcrypt Bulk Encryptor or other source that sends data to this input port on the GbE transport network device.
    - **Port Number –** Select the port number on the NOBE or other source that is connected to this input port on the GbE transport network device.
14. Click **Apply**. The Application Server saves your changes.
15. If necessary, repeat steps 14 and 15 to define another input port.
16. Click an **Output Ports** box to enable it, then define how this output port on the GbE transport network device connects to the input port of the appropriate edge device, such as a TB-QAM modulator, by entering the following information in each of the Connect To fields:

- **Headend Name –** Select the headend that contains the device that is physically connected to this output port on the GbE transport network device.
- **Device Type –** Select the type of device that receives data from this output port on the GbE transport network device. This device may be, for example, a QAM modulator or another GbE transport network.
- **Device Name –** Select the name of the device that receives data from this output port on the GbE transport network device.
- **Port Number –** Select the port number on this device that is connected to this output port on the GbE transport network device.

17 Click **Apply**. The Application Server saves your changes and updates the Connectivity graphic to show a connection from this port on the GbE transport network device to the port on the appropriate edge device, such as a TB-QAM modulator, that receives data from the transport network.

18 If necessary, repeat steps 17 and 18 to define another output port.

19 Click **Save**. The Application Server saves your changes and closes the Set Up GbE Transport window.

20 Now that you have provisioned Netcrypt elements and elements for related devices, set up sessions on the Netcrypt elements. For assistance, go to ***Setting Up CF Sessions and Transport Stream Routes on a Netcrypt Bulk Encryptor*** (on page 65).

Provision a Netcrypt Bulk Encryptor for the SimulCrypt Support Option

This section contains instructions for provisioning the following two components that are required when a Netcrypt Bulk Encryptor uses the SimulCrypt support option:

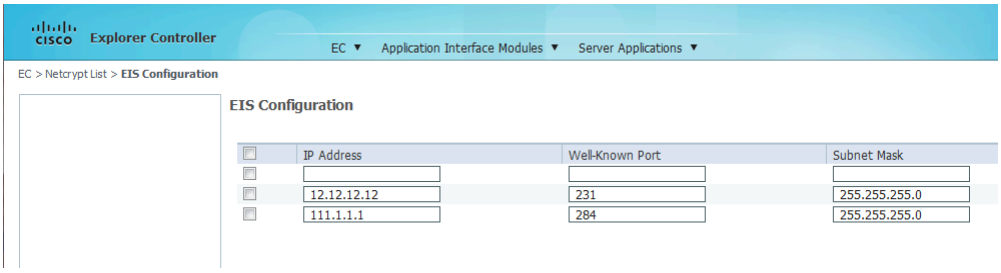
- **EIS and ECMG connections –** When using the SimulCrypt option, an ECMG is required to generate the ECM streams that are sent to the Netcrypt Bulk Encryptor. An EIS is required to provide the ECMG with information needed to generate ECM streams.
- **Third-Party Conditional Access Parameters –** When using the SimulCrypt option, the Netcrypt Bulk Encryptor supplements the standard PowerKEY CA system with up to two other CA systems. As a result, when using the SimulCrypt option, you need to configure the settings that the third-party CA systems use.

Provisioning Connections to an EIS and ECMGs for Optional SimulCrypt Support

Follow these instructions to provision the EIS and ECMG connections for a Netcrypt Bulk Encryptor that uses the SimulCrypt support option.

Note: Two ECMGs are used for redundancy: One is the primary ECMG; the other is a secondary ECMG, which is used as a backup.

1. From the Netcrypt List window, click **Define EIS elements**. The EIS Configuration window opens and lists any EIS connections that have been provisioned in the Application Server.
2. Click **Add**. A row of empty fields appears in the EIS Configuration window, similar to the following example.



3. Follow these instructions to enter data in the fields of the EIS Configuration window:
   - **IP Address –** Enter the IP address of the EIS connected to this Netcrypt Bulk Encryptor.
   - **Well-Known Port –** Enter the port number on the Netcrypt Bulk Encryptor to which this EIS connects.
   - **Subnet Mask –** Enter the subnet mask for the EIS.

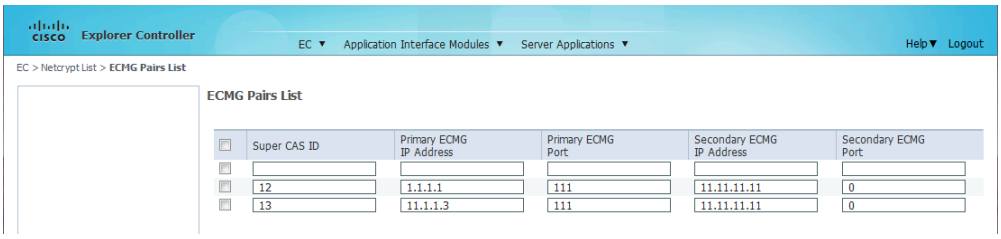
Note: When using the SimulCrypt support option, a Netcrypt Bulk Encryptor connects to the EIS through the ETHB (SCS interface) port on the back of the Netcrypt.

4 Click **Save**. The Application Server saves the information you entered and updates the window to display this connection.

5 In the path at the top of the window, click **Netcrypt List** as indicated in the following example. The EIS Configuration window closes and the Netcrypt List window opens.

6 Click **Define ECMG pairs**. The ECMG Pairs List window opens and shows any ECMG pairs that have already been configured in the Application Server.

7 Click **Add**. A row of empty fields appears in the ECMG Pairs List window.



8 Follow these instructions to enter data in the fields of the ECMG Pairs List window:

- **Super CAS ID** – Enter the SuperCAS (Conditional Access Software) identifier (ID). The SuperCAS ID is a unique identifier that associates a pair of ECMGs to an SCS port on the Netcrypt Bulk Encryptor.
- **Primary ECMG IP Address** – Enter the IP address of the primary ECMG.
- **Primary ECMG Port** – Enter the port number on the Netcrypt Bulk Encryptor to which the primary ECMG connects.
- **Secondary ECMG IP Address** – Enter the IP address of the backup ECMG.
- **Secondary ECMG Port** – Enter the port number on the Netcrypt Bulk Encryptor to which the backup ECMG connects.

Note: When using the SimulCrypt support option, a Netcrypt Bulk Encryptor connects to an ECMG pair through the ETHB (SCS interface) port on the back of the Netcrypt Bulk Encryptor. Two ECMGs are used for redundancy: one is the primary ECMG; the other is a secondary ECMG, which is used as a backup.

9 Click **Save**. The Application Server saves the information you entered and updates the window to display these connections.

10 Continue provisioning the Netcrypt Bulk Encryptor for the SimulCrypt support option. Go to ***Provisioning Third-Party Conditional Access Parameters for Optional SimulCrypt Support*** (on page 63).

Provisioning Third-Party Conditional Access Parameters for Optional SimulCrypt Support

When using the SimulCrypt option, a Netcrypt Bulk Encryptor supplements the standard PowerKEY CA system with up to two other CA systems. As a result, you need to provision the settings that the supplemental CA systems use.

Follow these instructions to provision third-party CA parameters for a Netcrypt Bulk Encryptor that uses the SimulCrypt support option.

1. From the Netcrypt List window, select the Netcrypt element whose CA parameters you want to configure, and click **Edit**. The Update Netcrypt Element window opens for this Netcrypt element.
2. Click **Third-Party CA Parameters**. The CA Parameters window opens for this Netcrypt element. The window is similar to the following example.
3. Follow these instructions to enter data in the fields of the Assignments area on the CA Parameters window:
   - **Open CAS ID –** Select the Open CAS IDs that this Netcrypt element uses. (The Open CAS ID pull-down menu contains all of the Open CAS IDs for ECMGs that have previously been provisioned on the system.)
   - **Selected EIS –** Select the IP address of the EIS this Netcrypt Bulk Encryptor uses. (The Selected EIS pull-down menu contains the EIS that was previously provisioned.)
   - **SCS Gateway IP (Default: 0.0.0.0) –** Enter the IP address of the SCS gateway.
4. Follow these instructions to enter data in the fields of the Constraints area on the CA Parameters window:
   - **ECM Response Timeout (Default: 30 seconds) –** Enter the amount of time, in seconds, that the Netcrypt Bulk Encryptor waits to receive confirmation that ECMGs are streaming ECMs to the SCS interface on the bulk encryptor.
   - **CW Provision Msg Repetition Rate (Default: 1) –** Do not modify the default value of 1 message per Crypto Period. This setting establishes the rate at which each CW_Provision (Control Word Provision) message is sent from the Netcrypt Bulk Encryptor SCS to the ECMG.
   - **Netcrypt to SCS Msg Timeout (Default: 30 seconds) –** Enter the maximum number of seconds allowed for messages to be sent from the Netcrypt Bulk Encryptor to the SCS interface. The SCS interface connects to the EIS and ECMGs.
   - **SCS Test Timeout (Default: 0 seconds) –** Enter the amount of time, in seconds, that the Netcrypt Bulk Encryptor waits to receive confirmation that the SCS channel between the Netcrypt Bulk Encryptor and the SCS interface is functioning as expected.
   - **Nominal CP Duration (Default: 1 second) –** Enter the amount of time, in seconds, each crypto period will last.

- **Min AC Delay Start (Default: 2 milliseconds)** – Enter the minimum delay, in milliseconds, to allow for access criteria (AC) changes beginning with the start of ECM broadcasting. (Access criteria contain specific information the ECMG uses to build an ECM.)

5. Click **Save**. The Application Server saves the information you entered and updates the window to display the ports you defined.
6. Now that you have provisioned this Netcrypt Bulk Encryptor to support the SimulCrypt option, place this Netcrypt online. Go to ***Placing a Netcrypt Bulk Encryptor Online*** (on page 51).

4

Setting Up CF Sessions and Transport Stream Routes on a Netcrypt Bulk Encryptor

This chapter describes the types of sessions that can be set up on a Netcrypt Bulk Encryptor and the new tools used to set up sessions on the Application Server. This information is followed with instructions for setting up sessions, including TSRs on a Netcrypt Bulk Encryptor.

Note: See ***Technical Specifications*** (on page 105) for the technical specifications of the Netcrypt Bulk Encryptor and consult your network wiring diagram when you provision the Netcrypt Bulk Encryptor to ensure a proper allocation of bandwidth.

For more information about the Application Server and operating the Application Server software, see the Application Server online help.

In This Chapter

Overview of Sessions Carried on a NOBE

This section summarizes the types of sessions that can be established using a Netcrypt Bulk Encryptor.

Note: For more information on sessions and stream types, see ***Theory of Operation*** (on page 4).

Types of Sessions

Sessions are temporary "pipes" or network paths that define a route for content through the various network elements responsible for content delivery, such as, a VOD server, a Netcrypt Bulk Encryptor, and session-based QAM modulators.

The Netcrypt Bulk Encryptor can carry traditional, continuous feed (CF) sessions as well as exclusive sessions (ES). In addition to these more familiar types of sessions, the Netcrypt Bulk Encryptor can be used to carry a new type of session called a TSR (Transport Stream Route).

The following paragraphs briefly describe the sessions that a Netcrypt Bulk Encryptor can carry:

- **Transport Stream Routes (TSRs) –** A TSR is used to pass content that does not require encryption through the Netcrypt Bulk Encryptor without altering the content. This approach can be used to pass pre-encrypted content streams through the Netcrypt Bulk Encryptor and on to simple edge devices, such as TB-QAM modulators, or to pass clear transport streams through the Netcrypt Bulk Encryptor without alteration.

  A TSR is useful in situations where operators need to pass an entire statistically multiplexed MPTS, while encrypting only some of the programs within the MPTS. Sessions would only be required for the programs that need to be encrypted. All others would be passed in the clear without alteration.

- **Continuous Feed (CF) Sessions –** CF sessions are relatively static connections between a video source and destination. Typically, the destination is a QAM modulator. CF sessions are primarily used for broadcasting and, as such, are relatively long-lived. CF sessions may be encrypted or in-the-clear. Each session may support one SPTS or one program within an MPTS.

  For more information, see the discussion of SPTS and MPTS in ***MPEG-2 Transport and Gigabit Ethernet*** (on page 4).

- **Exclusive Sessions (ES) –** Exclusive sessions are intended "exclusively" for one client. As a result, they are always unicast. Although they are used primarily for VOD, other applications are possible.

Note: For more information on sessions, see ***Theory of Operation*** (on page 4).

Session Setup Overview

This section provides an overview of how to set up different types of sessions on a Netcrypt Bulk Encryptor. Other sections in this chapter provide detailed instructions for setting up these sessions.

Before You Begin

Before you begin setting up sessions on a Netcrypt Bulk Encryptor, make certain that you have first provisioned the Netcrypt Bulk Encryptor and its associated devices, such as TB-QAMs. For assistance, see ***Provisioning the Netcrypt Bulk Encryptor and Associated Devices*** (on page 45).

Overview of Setting Up a Session Using a Netcrypt Bulk Encryptor

The steps you take to set up a session on a Netcrypt Bulk Encryptor differ according to the type of session you are setting up. The following instructions provide an overview of how to set up the following types of sessions using a Netcrypt Bulk Encryptor:

- TSR
- CF session

Process for Setting up a CF Session

Follow these steps to set up a CF session using a Netcrypt Bulk Encryptor and send it to a TB-QAM or GQAM.

1. If you have not already done so, provision the Netcrypt Bulk Encryptor and associated devices on the Application Server.

   Note: For assistance, see ***Provisioning the Netcrypt Bulk Encryptor and Associated Devices*** (on page 45).

2. Set up a CF session on this Netcrypt Bulk Encryptor.

   Note: For assistance, go to ***Set Up a CF Session on a Netcrypt Bulk Encryptor*** (on page 69).

3. Filter the Session List to verify that the session was created successfully.

   Note: For assistance, go to ***View CF Sessions Carried on Netcrypt Bulk Encryptors*** (on page 75).

Process for Setting Up a Transport Stream Route

Follow these steps to set up a TSR using a Netcrypt Bulk Encryptor.

Important: TSRs transport pre-encrypted content streams through the Netcrypt Bulk Encryptor without alteration and on to TB-QAMs. TSRs also transport clear streams through the Netcrypt Bulk Encryptor—again without alteration.

1. If you have not already done so, provision the Netcrypt Bulk Encryptor and its associated devices on the Application Server.

   Note: For assistance, see ***Provisioning the Netcrypt Bulk Encryptor and Associated Devices*** (on page 45).

2. Set up TSRs on Netcrypt Bulk Encryptors.

   Note: For assistance, go to ***Set Up a Transport Stream Route on a Netcrypt Bulk Encryptor*** (on page 73).

Set Up a CF Session on a Netcrypt Bulk Encryptor

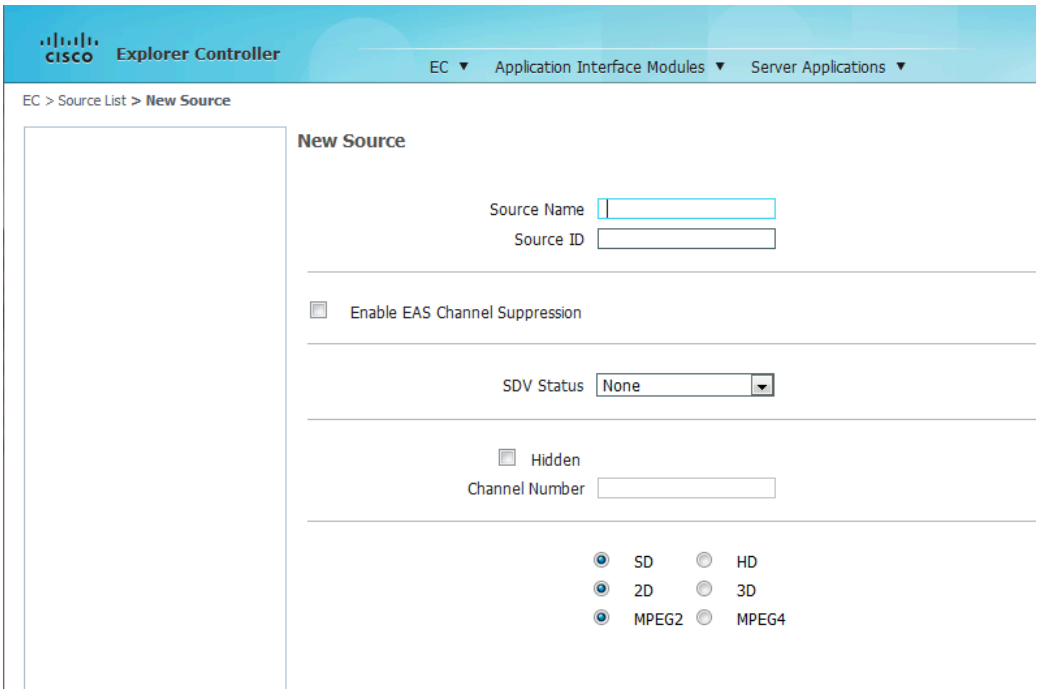
This section provides instructions for setting up a CF session using a Netcrypt Bulk Encryptor.

Setting Up a CF Session on a Netcrypt Bulk Encryptor

Follow these instructions to set up a CF session on a Netcrypt Bulk Encryptor.

1 Click **EC** and then select **Source** under the Service Provisioning section of the System Provision area. The Source List window appears.

2 Click **Add**. The New Source window appears.



3 Follow these instructions to enter data in the Set Up Source window:

- Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

  Note: We recommend that you use a naming scheme that indicates the source type (digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

- Click in the **Source ID** field and type the number you will use to identify this source. This can be any number (integer value) from 1 to 65535.

4 Click **Save**. The system saves the source information in the Application Server database and closes the Set Up Source window. The Source List window updates to include the new source.

5 Do you want to encrypt the service this session provides?
   - If **yes**, go to step 8.
   - If **no**, go to step 19.
6 Click once on the row containing the service you need to encrypt.
7 Click **Security Modes**. The Set Up Security Mode window opens.
8 In the Security Mode field, click the **Encrypted** option.
9 Do you want the content to be encrypted immediately?
   - If **yes**, in the **Date/Time** field, click the **Now** option and go to step 15.
   - If **no**, in the **Date/Time** field, click the **Custom** option and go to step 12.
10 Click in the **Effective Date** field and type the month, day, and year you want the system to start encrypting content from this source in a MM/DD/YYY format. For example, you would type April 22, 2006 as **04222006**.

   Note: The system inserts the slashes for you.
11 Click in the Effective Time field and type the hour, minute, and second you want the system to start encrypting this source.

   Important! Make certain that the time you enter is at least 15 minutes in the future.

   This field requires that you enter two digits for each value. For example, you would type 8:00 a.m. as 080000. The system inserts the colons for you and displays 08:00:00. You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.
12 Click **AM/PM** to establish which portion of the day you want the system to start encrypting all content from this source.
13 Click **Save**. The system saves the encryption information in the Application Server database and closes the Set Up Security Mode window. The Security Mode List window updates to include the new encryption information.
14 Click **Close** to close the Security Mode List window and return to the Source List window.
15 Create an unlimited segment for the source belonging to this session. For assistance, see the Application Server online help.
16 Add the segment you created in step 16 to a package so that authorized subscribers can view the content this source provides. For assistance, see the Application Server online help.
17 Click once on the row containing the content source that you created earlier in steps 4 through 6.

   Note: If you encrypted this source, you may have closed the Source List window. To open it, click **Source** on the **System Provisioning** tab.
18 Click **Source Definition**. The Source Definition List window opens for the source you selected.
19 Click **New Digital**. The Digital Source Set Up window opens.
20 Click in the first **Session ID** field and type 12 zeros.

21 Click in the second Session ID field and type the Service Source ID you used when you added the content source to the Source List.

22 Digital sources normally become effective as soon as they are saved. Do you want to delay the effective date and time of this digital service source?

- If **yes**, go to step 25.
- If no, go to step 29.

Note: Subscribers will see a blank channel until either the digital sources are saved or the time that you specify arrives.

23 Click the **Specify effective date and time** option, and then click **Next**. The Set Start Time/Date window opens.

24 Click in the **Effective Date** field and type the month, day, and year you want subscribers to be able to start viewing content from this source. You must type two digits for the month and day, and type four digits for the year.

Example: You would type July 4, 2003, as **07042003**. The system enters the slashes for you and displays 07/04/2003.

25 Click in the **Effective Time** field and type the hour, minute, and second you want subscribers to be able to start seeing content from this source. You must type two digits for each value.

Example: You would type eight o'clock as **080000**. The system enters the colons for you and displays 08:00:00.

You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.

26 Click **AM/PM** to establish which portion of the day you want subscribers to be able to start viewing content from this source.

27 Click **Next**. The Define Session window opens.

28 Because this source will be providing broadcast (audio/video) programming rather than system information, click the Broadcast programming option.

29 Click **Next**. The Session Setup window opens.

30 Click the **Input Device** arrow and select the MPEG Source that provides the Netcrypt Bulk Encryptor with content for this CF session.

31 Click **Next**. The Select Outputs window opens and displays the list of devices that can receive this content. In this example, only one device (a TB-QAM) is available to select.

32 Click to select the output TSID on the TB-QAM that will receive content for this transport stream, and then click **Next**. The Wrap-Up window opens.

33 Click in the **MPEG Program Number** field and type the program number of the desired program in the transport stream. This number must match the program number of the MPEG source as defined by your content provider.

34 Click in the **Bandwidth** field and type the bit rate (in Mbps) that the system should reserve for this service. This value is usually defined by your content service provider, or it can be set using a re-rating or re-coding device.

35 If this session will be multicast, click the **Netcrypt Multicast Input** button to enable it. Then enter the multicast (class D) IP address of the stream.

Note: The IP address must be unique and within the range of IP addresses reserved for multicasting (224.0.0.0 to 239.255.255.255).

36 Click in the **Netcrypt Input** field of the **Ethernet UDP Ports** settings and enter the destination UDP port number of the incoming stream.

37 Click in the **Netcrypt Output** field of the **Ethernet UDP Ports** settings, and enter the destination UDP port number that you would like on the outgoing stream. Note that for a TB-QAM, this number determines the input to output mapping through the QAM per its mapping table. For more information, see ***Theory of Operation*** (on page 4).

Note: If this Netcrypt Bulk Encryptor uses the SimulCrypt support option, enter the transport stream identifier of the SCG that the third-party CA system uses.

38 You can obtain this number from the vendor of the third-party CA system.

39 Click **Next**. The Save Source Definition window opens.

40 Click **Save**. The system closes the Save Source Definition window, saves the source definition in the Application Server database, and updates the Source Definition List window to include the new source information.

41 Now that you have created a CF session from this content source, define how you want to offer this session as a service to subscribers. The process for defining a service from a Netcrypt session is no different than defining a service from a QAM session. However, the process is summarized below for easy reference:

a For a clear or encrypted service, register the service with the Service Application Manager (SAM) to define how the service operates when a DHCT receives it. For assistance, see **Register a Service** in the online help.

b For a clear or encrypted service, place the service in the IPG Service List so that information about this service appears in the on-screen IPG that is presented to subscribers. For assistance, see **Setting Up IPG Services** in the SARA Application Server User's Guide appropriate to your system release.

c For a clear or encrypted service, place the service on a Channel Map so subscribers can access the service by tuning to a particular channel. For assistance, see **Add a Service to a Channel Map** in the online help.

42 Now that you have set up CF sessions on the Netcrypt elements that require them, use the Session Filter to view the sessions and ensure they were built. Go to ***View CF Sessions Carried on Netcrypt Bulk Encryptors*** (on page 75).

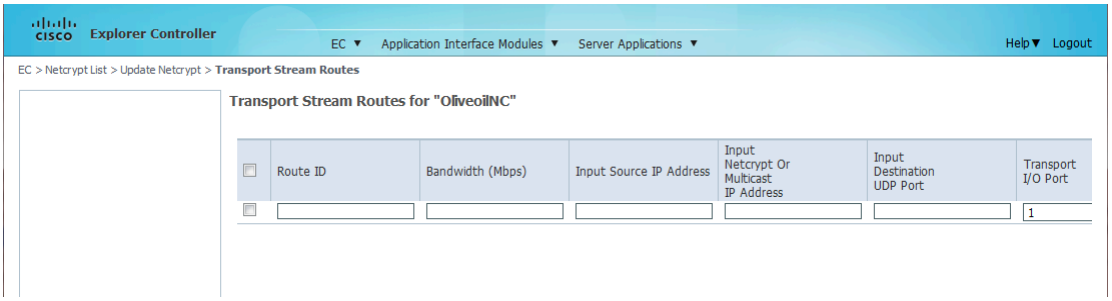
Set Up a Transport Stream Route on a Netcrypt Bulk Encryptor

This section describes how to set up a TSR on a Netcrypt Bulk Encryptor.

Setting Up a Transport Stream Route on a Netcrypt Bulk Encryptor

Follow these steps to set up a TSR on a Netcrypt Bulk Encryptor.

1. Click **EC** and then select **Netcrypt** under the Network Element Provisioning area. The Netcrypt List window opens and shows all the Netcrypt elements that have been provisioned on the Application Server.
2. Select the Netcrypt element that will carry the TSR and click **Edit**. The Update Netcrypt Element window opens for the Netcrypt element you selected.
3. Click **Transport Stream Routes**. The Transport Stream Route window opens and displays any TSRs that have been set up on this Netcrypt element.
4. Click **Add**. Empty fields appear so that you can set up a new TSR, similar to the following example.



5. Follow these instructions to enter data in the empty fields of the Transport Stream Route window:
   - **Route ID** – Enter a unique number to identify this TSR. This number must be a 2-byte integer in the range of 1 to 65535.
   - **Bandwidth** - Enter the amount of bandwidth (in Mbps) that the system should allow for the service this session provides. This value is usually defined by your content service provider, or it can be set using a re-rating or re-coding device.
   - **Input Source IP Address** – Enter the IP address of the source device, such as a GbE multiplexer or re-rater.
   - **Input Netcrypt Or Multicast IP Address** – The value for this field varies according to your system configuration:
     - For unicasts, enter the IP address of the selected GbE port on the Netcrypt Bulk Encryptor.
     - For multicasts, enter the IP address assigned to that content.

Note: If you are unsure of these values, confirm them with your system administrator or consult your network map.

- **Input Destination UDP Port –** The value for this field varies according to your system configuration:
  - For unicasts, enter the UDP port number that uniquely identifies this stream.
  - For multicasts, this number is not required; however, the system may choose to assign a well-known UDP port number to multicasts.
- **Transport I/O Port –** Enter the number of the physical GbE port that will be used for this stream, as labeled on the back panel.
- **Output Destination IP Address –** The value for this field varies according to your system configuration:
  - For output unicasts, enter the GbE IP address of the destination device, such as a TB-QAM or GQAM, to which you want the content to flow.
  - For output multicasts, enter the multicast group destination address (GDA) that has been assigned to that content.
- **Output Destination UDP Port –** The value for this field varies according to your system configuration:
  - For output unicasts to SB-QAMs, enter a number to uniquely identify the stream.
  - For output unicasts to TB-QAMs, this number is derived from the QAM's table in order for the QAM to properly route streams. Note that some TB-QAMs do not support MPTSs.
  - For output multicasts, this number is not required; however, the system may choose to assign a well-known UDP port number to multicasts.

6 Click **Save**. The system saves this TSR and updates the Transport Stream Route window.

7 Do you need to set up another TSR on this Netcrypt element?

- If **yes**, repeat steps 6 to 8 to set up another TSR on this Netcrypt Bulk Encryptor.
- If **no**, go to step 10.

8 Do you need to set up a TSR on another Netcrypt Bulk Encryptor?

- If **yes**, click **Netcrypt List** in the path at the top of the window to display the Netcrypt List window. Repeat steps 4 to 9 to set up a TSR on another Netcrypt element.
- If **no**, you have successfully set up TSRs on the Netcrypt elements that require them. To close the Transport Stream Route window, click **Exit**.

View CF Sessions Carried on Netcrypt Bulk Encryptors

This section describes how to use the Session List to view CF sessions that are carried on Netcrypt Bulk Encryptors.

Viewing CF Sessions Carried on All Netcrypt Bulk Encryptors

Follow this procedure to view CF sessions that have been set up on all the Netcrypt Bulk Encryptors in your system.

1. Click **EC** and then select **Session List** under the Utilities area. The Session List Filter window opens and shows session-carrying devices listed by type.
2. Select a QAM or server and click **Display**. The Session Summary window opens and shows all active Netcrypt CF sessions.
3. Do the CF sessions you created appear in the list?
   - If **yes**, click **Exit All Session screens** to close the Session Filter window.
   - If **no**, contact Cisco Services for assistance.

Viewing CF Sessions Carried on Specific Netcrypt Bulk Encryptors

Follow this procedure to view CF sessions that have been set up on specific Netcrypt Bulk Encryptors in your system.

1. Click **EC** and then select **Session List** under the Utilities area. The Session List Filter window opens and shows session-carrying devices listed by type.
2. In the Netcrypts list, select the Netcrypt Bulk Encryptor whose CF sessions you want to view.
3. Click **Display**. The Session Summary window f opens and displays the CF sessions carried on the Netcrypt Bulk Encryptor that you selected.
4. Do the CF sessions you created appear in the list?
   - If **yes**, click **Exit All Session screens** to close the Session Filter window.
   - If **no**, contact Cisco Services for assistance.

5

Maintaining and Repairing the Netcrypt Bulk Encryptor

This chapter contains procedures for maintaining a Netcrypt Bulk Encryptor that has been installed in a DBDS. It also provides basic repair instructions and recommendations for spare parts to keep on-hand.

Note: Once installed as described, the Netcrypt Bulk Encryptor is designed to run unattended for extended periods. However, proper maintenance is required to keep it functioning properly.

In This Chapter

Maintenance Overview

Performing routine maintenance extends the life of the Netcrypt Bulk Encryptor and helps to reduce the need for troubleshooting.

Note: For instructions on how to diagnose alarm conditions, see ***Troubleshooting the Netcrypt Bulk Encryptor*** (on page 89).

Recommended Spare Parts

We recommend that you stock the following spare parts. Keeping these spare parts on hand enables you to quickly return the Netcrypt Bulk Encryptor to operating order in the unusual event that the Netcrypt Bulk Encryptor malfunctions:

- Two 4.0 A, SLO BLO 250 V fuses (part number 188106)
- One fan kit, which includes the replacement fan and instruction sheet (part number 4010291-40)

Quarterly Inspection

The Netcrypt Bulk Encryptor can operate unattended for extended periods. However, perform a visual inspection once every three months to ensure that the unit is in good operating order.

Important: Only qualified personnel should attempt maintenance and service of the Netcrypt Bulk Encryptor.

Check the following items during a visual inspection:

- **Cables and connectors -** Verify that all cables are mated properly and all retaining screws are tight. Inspect cables for stress and chafing.
- **Cover and rear panel -** If necessary, clean the cover and rear panel with a soft cloth dampened with a mild detergent solution.
- **Fan intakes on side panel -** Check the fan intakes on the side panel for excessive lint or dust buildup. Remove the lint and dust from the intakes using a damp cloth or a small hand vacuum.
- **Front and back panel indicators -** Check the indicators on the front and back panel of the unit to verify that they show the Netcrypt Bulk Encryptor is operating as expected. For assistance, go to ***Front Panel Status Indicators During Normal Operation*** (on page 79) and ***Back Panel Status Indicators During Normal Operation*** (on page 79).

Front Panel Status Indicators During Normal Operation

The following table lists the status of front panel indicators when the unit is operating as expected.

Indicator	Status
POWER (green)	On
RUN/LOAD (green)	On
RESET (yellow)	Off
MINOR ALARM (yellow)	Off
MAJOR ALARM (red)	Off

Note: If the indicators show that the unit is not operating as expected, see ***Troubleshooting the Netcrypt Bulk Encryptor*** (on page 89) for assistance.

Back Panel Status Indicators During Normal Operation

The following tables list the status of back panel indicators when the unit is operating as expected.

Indicator	Status
DUP (green)	■ On when in full duplex mode ■ Off when in half duplex mode
L1000 (green)	On when a 1000 Mbps (gigabit Ethernet) link is established
L100 (green)	On when a 100 Mbps (fast Ethernet) link is established
L10 (green)	On when a 10 Mbps (Ethernet) link is established
TX (green)	On when transmitting data
RX (green)	On when receiving data

Note: If these indicators show that the unit is not operating as expected, see ***Troubleshooting the Netcrypt Bulk Encryptor*** (on page 89) for assistance.

Indicators for Ethernet Connections During Normal Operation

Indicator	Status
TX (green)	On
L/RX (green)	On or blinking
ERROR (yellow)	Off

Note: If these indicators show that the unit is not operating as expected, see ***Troubleshooting the Netcrypt Bulk Encryptor*** (on page 89) for assistance.

Replace the Fuses

Each Netcrypt Bulk Encryptor contains two power fuses. This section describes how to replace the fuses with spares that you should have on hand.

Before You Begin

CAUTION:

To minimize the disruption of services, we recommend keeping two spare fuses for each Netcrypt Bulk Encryptor in your system.

To replace the fuses, you must have the following:

- Two 4.0 A, SLO BLO 250 V fuses (part number 188106)
- A small, flat-blade screwdriver or similar tool to pry the fuse holder from the back panel of the Netcrypt Bulk Encryptor

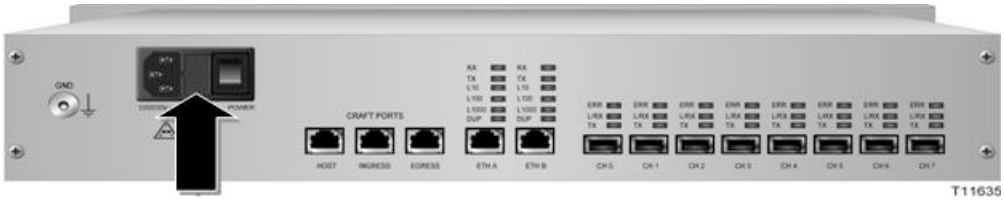
Replacing the Fuses

WARNING:

Avoid electric shock. Disconnect the power cord on this product before you remove the fuses and only use fuses that have the correct type and rating.

To replace the SLO BLO 250 V fuses, follow these steps.

1. Power down the Netcrypt Bulk Encryptor and unplug the power cord from the back panel.
2. Locate the fuse holder on the left side of the back panel of your Netcrypt Bulk Encryptor.



3. Use a small, flat-blade screwdriver to pry the fuse holder from the back panel of the Netcrypt Bulk Encryptor.
4. Remove and discard both blown fuses, and replace them with new fuses.
5. Insert the fuse holder into the back panel and press firmly until it snaps in place.
6. Replace the power cord and power on the Netcrypt Bulk Encryptor.
7. If necessary, order additional fuses to ensure that you have spares readily available. See ***Customer Information*** (on page 103) for the telephone number of a customer service center in your area.

Replace a Fan

This section provides instructions for replacing a fan unit on the Netcrypt Bulk Encryptor by either hot swapping the fan unit or powering off, disconnecting, and removing the bulk encryptor completely from the rack. When hot swapping a fan, you do not need to power down the Netcrypt Bulk Encryptor. As a result, you can replace a fan without disrupting service to subscribers.

Important: Do not wait for a maintenance window to replace a failed fan. Replace failed fans as soon as possible; otherwise, damage can result to the Netcrypt Bulk Encryptor.

How to Identify a Fan Failure

Indicator lights on the front panel of the Netcrypt Bulk Encryptor helps you identify a fan failure. If a fan fails, the **MAJOR** LED on the front panel will light. In addition, if you are using Cisco's optional DBDS Alarm Management System to monitor network elements, the message **Fan <fan number> failure** is displayed for operators. The Alarm Management System numbers fans 1 to 5 from front to back.

CAUTION:

Replace a failed fan as soon as you identify it has failed; otherwise, damage can result to the Netcrypt Bulk Encryptor. Do not wait for a maintenance window to replace a fan.

Before You Begin

WARNING:

Avoid electric shock and damage to this product. Replace a fan only with a genuine replacement fan from Cisco. Contact the representative who handles your account to order replacement fans.

In order to hot swap a fan unit, you must have the following:

- Sufficient length in all cords and cables so you can slide the bulk encryptor forward in the rack far enough to fully access the fan units on the side panel
- The ability to externally support the Netcrypt Bulk Encryptor with a cart or table or with the assistance of another person
- A #10 Torx bit
- Either of the following replacement parts:
  - A replacement fan unit (part number 4007846)
  - A replacement fan kit, which includes the replacement fan and instruction sheet (part number 4010291-40)

Replacing a Fan

The Netcrypt Bulk Encryptor has five fans on the side panel. The fans are designed to be hot swappable, meaning you do not need to power down the Netcrypt Bulk Encryptor to replace a failed fan. If you allowed for sufficient cable lengths during installation, you are able to slide the Netcrypt Bulk Encryptor forward in the rack to fully access fans and allow the unit to operate uninterrupted.

> **CAUTION:**
>
> **Avoid damage to this product. Replace a fan unit only with a genuine replacement fan unit from Cisco. Contact your Cisco Customer Service Representative to order replacement fan units.**

To replace a fan on the Netcrypt Bulk Encryptor, complete these steps.

1. Identify the fan that failed on the Netcrypt Bulk Encryptor.

   If you are using Cisco's optional DBDS Alarm Management System to monitor network elements, the message **Fan <fan number> failure** is displayed for operators. For example, if fan 1 has failed, the message **Fan 1 failure** is displayed. The Alarm Management System numbers fans 1 to 5 from front to back.

2. Are the cables connected to the back panel of the bulk encryptor long enough to allow you to slide the unit forward in the rack so that you can access the fan units?

   - If **yes**, remove the four screws that secure the Netcrypt Bulk Encryptor in the rack and carefully slide the bulk encryptor forward until you can access the fan units. Go to step 5.

     > **CAUTION:**
     >
     > **To avoid damaging the unit, you must be able to externally support the Netcrypt Bulk Encryptor with a cart or table or with assistance when you slide the chassis forward in the rack.**

   - If **no**, power off the bulk encryptor and disconnect all cables.

   Important: When the unit is powered off, service to customers is disrupted.

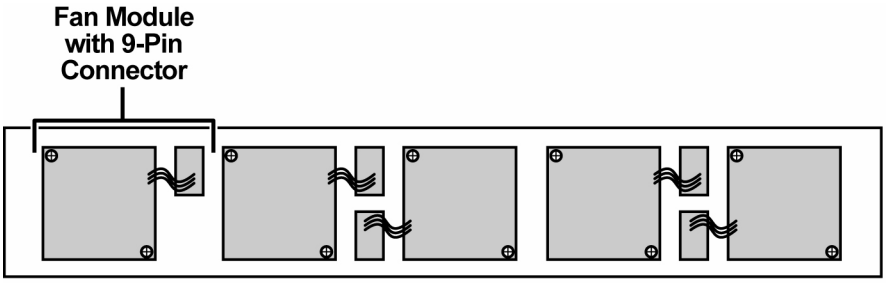
3. If you cannot slide the unit forward in the rack because any of the cables in the rack are not long enough to allow access to the fan, you must power off the unit and disconnect all cables.

4. Remove the four screws that secure the Netcrypt Bulk Encryptor in the rack.

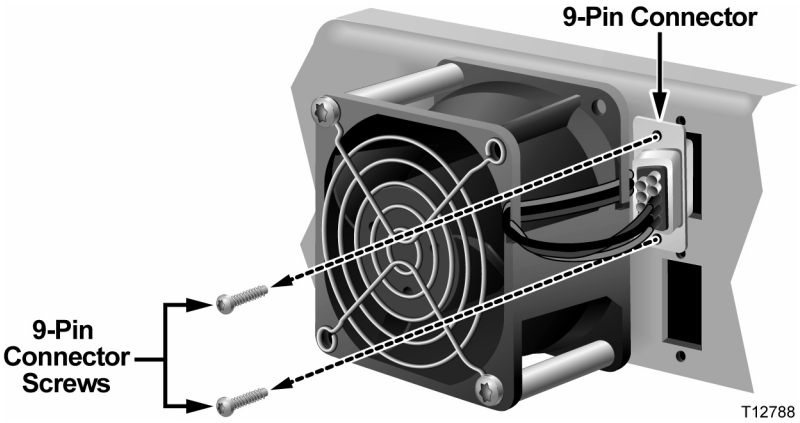
5. Carefully remove the Netcrypt Bulk Encryptor completely from the rack and place it on a sturdy, level work surface, such as a work cart.

6. Identify the fan that failed on the bulk encryptor (the one that is not spinning). If you removed power from the bulk encryptor, apply power from a temporary source to identify the fan that failed. Then, power off again before continuing.

7 Locate the 9-pin connector for the fan you want to replace. The following diagram shows the location of the 9-pin connectors on the bulk encryptor.



8 Remove the two screws that secure the 9-pin connector to the side panel and place them in a safe location nearby.

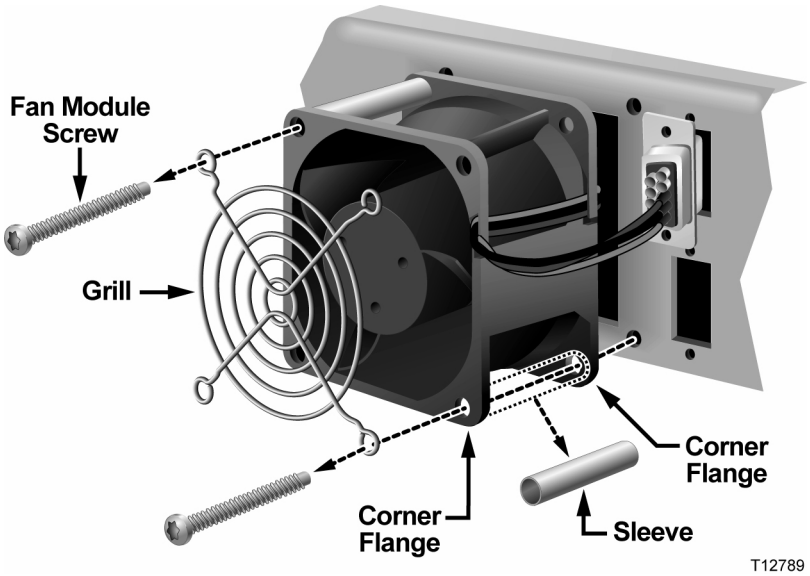


9 Disconnect the 9-pin connector.

10 Remove the following components from the unit and place them in a safe location nearby:

- Two torx screws
- Two sleeves
- The grill that protects the fan from debris

Important: The sleeves are loosely positioned between the flanges and are not connected to the fan. Be careful not to drop them as you remove them from the unit.



11 Remove the non-functioning fan unit. Set this fan unit aside for safe disposal later.

> **WARNING:**
>
> **Avoid electric shock hazard. Hazardous voltage can be accessed inside the unit when a fan is removed.**

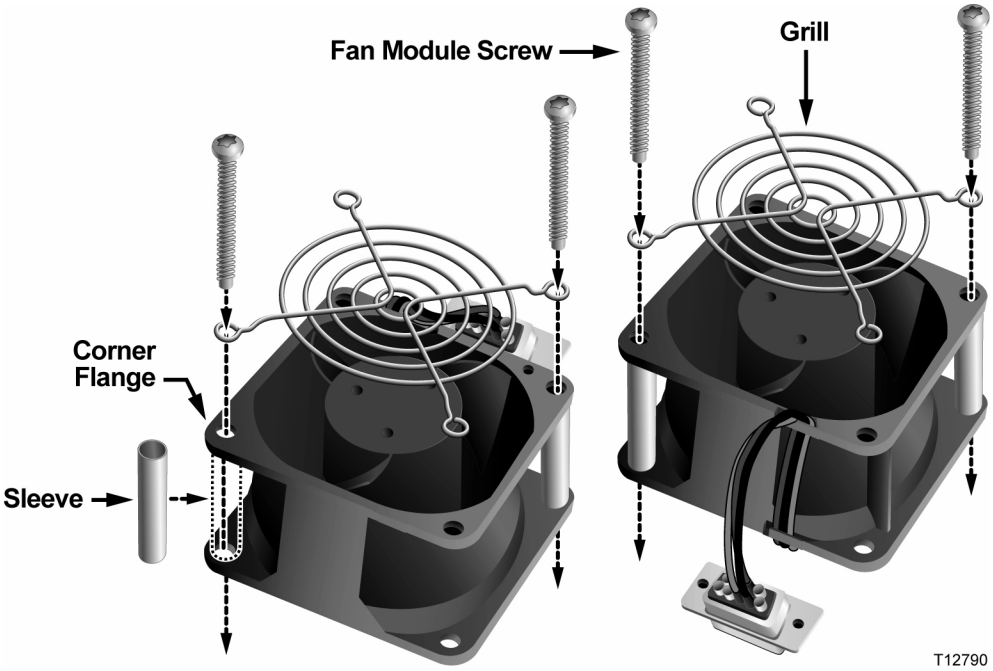
12 Place the new fan unit on a flat work surface or on top of the Netcrypt Bulk Encryptor.

13 Place the grill in the proper location on the fan.

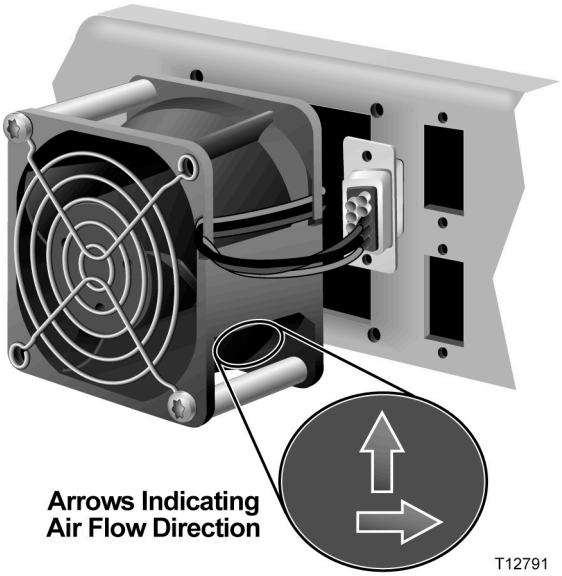
14 Insert the sleeves between the corner flanges.

15 Hold each sleeve in place while you insert the screw through the grill, sleeve, and the back of the fan unit. Repeat this step for all four screws.

Note: You may find an alternate method for reassembling the fan pieces that is more comfortable for you. Whatever method you use, be careful that you do not drop one of the fan components.



16 Hold the new fan unit in place on the side panel of the bulk encryptor so that the 9-pin connector aligns with its socket. Verify that the arrows indicating air flow direction are pointing up and into the unit (see the following diagram). Make sure the arrows are not pointing toward you. Tighten both screws to secure the fan in place.



17 Insert the 9-pin connectors into the 9-pin socket, and then replace and carefully tighten both screws that secure the 9-pin connector to the side panel. Do not over tighten or cross thread any of the screws.

18 Did you have to remove the Netcrypt Bulk Encryptor completely from the rack?

- If **yes**, go to step 19.
- If **no**, go to step 20.

19 Replace the Netcrypt Bulk Encryptor into its original position in the rack and secure it in the rack using the original screws. Then, go to step 20.

20 Reconnect the power cord and power on the NOBE.

21 Does the new fan unit operate properly and did the alarm(s) clear?

- If **yes**, you have completed this procedure.
- If **no**, contact Cisco Services for assistance.

6

Troubleshooting the Netcrypt Bulk Encryptor

This chapter provides explanations of major, minor, and status alarm conditions and instructions for checking alarms.

In This Chapter

Alarm Conditions

This section describes major, minor, and status alarms. See ***Troubleshooting With Alarm Manager*** (on page 92) for a list of alarms and possible solutions.

Purpose and Severity Levels of Alarm Indicators

Alarms provide system operators with an indication of an abnormal condition. Alarm indicators turn on when hardware or software conditions occur that might cause the Netcrypt Bulk Encryptor to operate incorrectly or fail. Examples of such conditions include temperature fluctuations, power supply failure, communication problems, or the detection of bad data. All alarms are automatically enabled after powering up the Netcrypt Bulk Encryptor.

The following table describes each of the status and alarm indicators on the front panel of the Netcrypt Bulk Encryptor.

Status Indicators

Indicator	Description
POWER	When the POWER indicator lights, the Netcrypt Bulk Encryptor is receiving power.
RUN/LOAD	When the RUN/LOAD indicator lights, the Netcrypt Bulk Encryptor is running under normal conditions. When the RUN/LOAD indicator blinks, the Netcrypt Bulk Encryptor is downloading a new version of code.

Alarm Indicators

Title	Title
MINOR ALARM	When the MINOR ALARM indicator lights, a non-fatal error condition is pending. Under this condition, the Netcrypt Bulk Encryptor may continue to operate with some loss of functionality.
MAJOR ALARM	When the MAJOR ALARM indicator lights, a fatal error condition is pending. A fatal error indicates a complete loss of functionality. Major alarms occur for hardware or software conditions that indicate a serious disruption of service or the malfunctioning or failure of important circuits. These situations require the immediate response of the technician to restore or maintain system operability.

Front Panel Alarm Indicators

The following table lists the conditions that cause MAJOR ALARM and MINOR ALARM indicators to turn on.

Note: For additional information on each of the alarm descriptions listed here, see ***Troubleshooting With Alarm Manager*** (on page 92).

Alarm Level	Alarm Description
MINOR ALARM	■ Temperature Exceeded ■ Input (1-8) MPEG continuity error ■ Input (1-8) MPEG Transport error ■ Input (1-8) errored MPEG packets ■ Input (1-8) FIFO overflow ■ Output (1-8) FIFO overflow ■ Output (1-8) packets were dumped ■ Input (1-8) ECM PID conflict ■ Power supply failure
MAJOR ALARM	■ Input (1-8) loss of input signal ■ Ethernet loss of signal ■ Hardware error ■ Runtime error (operating system) ■ Input (1-8) auto negotiate failure ■ Fan (1 - 5) failure ■ Session xxx data error, where xxx is a number from 0 to 991

Troubleshooting With Alarm Manager

If you are using our optional DBDS Alarm Management System to monitor network elements, Netcrypt alarms are monitored on the Application Server. Refer to the table in this section to find and correct the cause of these alarms. Some alarms may require you to contact Cisco. Refer to ***Customer Information*** (on page 103) for contact information.

Alarm Manager Alarms

Refer to the following table to diagnose and correct the following alarm conditions.

Note: For more details on troubleshooting alarms, refer to *DBDS Alarm Manager 1.0 Online Help* (part number 78-745259-01) .

- Threshold Exceeded alarm
- Session Capacity Exceeded alarm
- Total Outstanding Sessions alarm (This alarm will alert the operator of the need for an additional Netcrypt Bulk Encryptor).

Alarm Description	Alarm Level	Probable Cause	Check and Correct
Temperature Exceeded	Minor	The internal temperature of the Netcrypt Bulk Encryptor is approaching 120ºC (248ºF) for the network processors and 120ºC (248ºF) for the FPGA (field-programmable gate array).	Remove vent obstructions. Provide more cooling and ventilation. Check power connections for the exhaust fans. Contact Cisco Services. **Important:** You should check the temperature on the Netcrypt Bulk Encryptor daily or more frequently if possible.
Input (1-8) MPEG continuity error	Minor	MPEG continuity error counter. One or more of the MPEG packets are being dropped.	Check one or more upstream devices connected to the GbE ports. Contact Cisco Services.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
Input (1-8) MPEG Transport error	Minor	MPEG transport error indicator counter. An error occurred in the header of the MPEG packet.	Check one or more upstream devices connected to the GbE ports. Run the Doctor Report to troubleshoot network connectivity issues. Contact Cisco Services.
Input (1-8) loss of input signal	Major	No signal. This indicates one or more of the following conditions: ■ An upstream device that provides input to the Netcrypt Bulk Encryptor has failed or is offline. ■ A cable has been disconnected.	Check for loose or broken GbE cable connections to the Netcrypt Bulk Encryptor. Check that the GbE outputs of upstream devices are active. Run the Doctor Report to troubleshoot any network connectivity issues. Contact Cisco Services.
Input (1-8) errored MPEG packets	Minor	An MPEG sync byte error occurred in the header of MPEG packets as they arrived at the indicated Input port.	Contact Cisco Services. Check one or more upstream devices connected to the GbE ports.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
Input (1-8) FIFO overflow on the GigE media access controller (GMAC)	Minor	A first-in first-out (FIFO) overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the Application Server for the Netcrypt Bulk Encryptor. ■ The data rate as defined from the Application Server for the Netcrypt session is too low, which also means that the data rate of the GbE input to the Netcrypt Bulk Encryptor is too high. ■ Excessive amount of IP (non-MPEG) network traffic. ■ Hardware problem exists.	Reduce the data rate of input to the Netcrypt Bulk Encryptor by doing the following: ■ Reducing the amount of incoming data ■ Reducing the amount of data added to the stream Verify and correct session rate targets and threshold values. Reduce flow of general IP (non-MPEG) traffic to the Netcrypt Bulk Encryptor. Contact Cisco Services.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
Input (1-8) packets were dumped See also Input (1-8) FIFO overflow	Minor	A FIFO overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the Application Server for the Netcrypt Bulk Encryptor. ■ The data rate as defined from the Application Server for the Netcrypt session is too low, which also means that the data rate of the GbE to the Netcrypt Bulk Encryptor is too high. ■ Hardware problem exists. ■ Excessive IP (non-MPEG) network traffic being sent to the Netcrypt Bulk Encryptor.	Reduce the data rate of input to the Netcrypt Bulk Encryptor by doing the following: ■ Reducing the amount of incoming data ■ Reducing the amount of data added to the stream Run the Doctor Report to troubleshoot network connectivity issues. Reduce flow of general IP (non-MPEG) traffic to the NOBE. Contact Cisco Services.
Ethernet loss of signal	Major	This indicates one or more of the following conditions: ■ An upstream device that provides input to the Netcrypt Bulk Encryptor has failed or is offline. ■ A cable has been disconnected.	Check for loose or broken Ethernet cable connections to the Netcrypt Bulk Encryptor Check that the Ethernet outputs of upstream devices are active. Run the Doctor Report to troubleshoot any network connectivity issues. Contact Cisco Services.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
Output (1-8) FIFO overflow See also Output (1-8) packets were dumped	Minor	A first-in first-out (FIFO) overflow occurred and packet data has been lost. This indicates one or more of the following conditions: Too many sessions defined from the Application Server for the Netcrypt Bulk Encryptor. ■ The data rate as defined from the Application Server for the Netcrypt session is too low, which also means that the data rate of the GbE input to the Netcrypt Bulk Encryptor is too high. ■ Hardware problem exists.	Reduce the data rate of input to the Netcrypt Bulk Encryptor by doing the following: ■ Reducing the amount of incoming data ■ Reducing the amount of data added to the stream ■ Verify and correct session rate targets and threshold values. Contact Cisco Services.
Output (1-8) packets were dumped See also Output (1-8) FIFO overflow	Minor	A FIFO overflow occurred and packet data has been lost. This indicates one or more of the following conditions: ■ Too many sessions defined from the Application Server for the indicated port on the Netcrypt Bulk Encryptor. ■ The data rate as defined from the Application Server for one or more Netcrypt sessions is too low for the indicated port, which also means that the data rate of the GbE to the Netcrypt Bulk Encryptor is too high ■ Hardware problem exists.	Reduce the data rate of input to the Netcrypt Bulk Encryptor by doing the following: ■ Reducing the amount of incoming data ■ Reducing the amount of data added to the stream Run the Doctor Report to troubleshoot network connectivity issues. Contact Cisco Services.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
Reset detected	Status	The Netcrypt Bulk Encryptor has been reset by either a power loss or a manual reset.	Session and alarm provisioning are sent to the Netcrypt Bulk Encryptor again automatically from the Application Server. However, you should also check the following: ■ Verify that there are still broadcast services on this Netcrypt Bulk Encryptor. ■ Verify that the reset did not adversely affect broadcast services. ■ Run the Doctor Report to troubleshoot any network connectivity issues. ■ Contact Cisco Services.
Hardware error	Major	General-purpose hardware error or hardware failure occurred.	Contact Cisco Services.
Runtime error	Major	General-purpose software error occurred.	Reset the Netcrypt Bulk Encryptor by the power switch or, if possible, by Application Server control. Contact Cisco Services.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
Craft event change	Status	The Netcrypt Bulk Encryptor did not receive the third-party CA provisioning message. The Netcrypt Bulk Encryptor will not attempt to connect to external devices such as the Event Information Scheduler (EIS) and the Entitlement Control Message Generator (ECMG) devices while this alarm is active.	Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables. Check the EIS Configuration and ECMG List windows on the Application Server for this Netcrypt Bulk Encryptor and enter data in the fields on these windows if necessary. Display the Application Server Control window and verify that the pkeManager process on the Application Server is running. If it is not running, restart the pkeManager process.
SCS CA not provisioned	Status	The Netcrypt Bulk Encryptor did not receive the third-party CA provisioning message. The Netcrypt Bulk Encryptor will not attempt to connect to external devices such as the Event Information Scheduler (EIS) and the Entitlement Control Message Generator (ECMG) devices while this alarm is active.	Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables. Check the EIS Configuration and ECMG List windows on the Application Server for this Netcrypt Bulk Encryptor and enter data in the fields on these windows if necessary. Display the Application Server Control window and verify that the pkeManager process on the Application Server is running. If it is not running, restart the pkeManager process.
SCS CA EIS link lost.	Status	This alarm is sent when the Netcrypt Bulk Encryptor has not established a TCP/IP link with the primary EIS.	Verify that the setting for the EIS Well Known Port field in the EIS Configuration window on the Application Server is correct.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
SCS CA no connect EIS.	Status	This alarm is sent if the TCP/IP link is established with the EIS and then subsequently fails.	Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables. Verify network connectivity by pinging the EIS or using a network analyzer. Contact your third-party CA provider for assistance in determining if their firewall is preventing you from accessing the EIS.
SCS CA ECMG (1-4) link lost	Status	This alarm is sent when the Netcrypt Bulk Encryptor has not established a TCP/IP link with an Entitlement Control Message Generator (ECMG).	Verify that the settings for ECMGs on the ECMG List are correct.
SCS CA ECMG (1-4) no connect	Status	This alarm is sent if the TCP/IP link is established with an ECMG and then subsequently fails.	Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
SCS CA no SA session	Minor	This alarm is sent when the Netcrypt Bulk Encryptor receives Scrambling Control Group (SCG) information for a session that has not been set up on the Application Server. The Netcrypt Bulk Encryptor clears the alarm immediately. **Note:** The SCG message is sent from the EIS to the Netcrypt Bulk Encryptor to control the encryption of a session.	Verify that the sessions this SCS MQAM modulator carries have been set up correctly by first checking the Application Server and then, if necessary, checking the EIS. ■ If your check of the Application Server determines that an existing session does not match current SCG message parameters, correct the session. Or, if necessary, set up a new session on the Application Server. Then, use the EIS disconnect to force the EIS to resend SCG messages. ■ If your check of the Application Server determines that the sessions are set up correctly on the Application Server, contact your third-party CA system administrator to correct the parameters in the SCG message. ■ If you verify that the parameters in the SCG do match the existing sessions, contact Cisco Services for assistance. **Note:** To determine which SCG parameters the modulator is receiving, manually disconnect the EIS and then turn on logging for the EIS/ECMG connection and EIS process.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
SCS CA SCG refused PID conflict	Minor	An attempt to create a session failed because the PIDs in the input PMT do not agree with those specified in the session setup message and they conflict with PIDs of existing sessions.	Tear down and rebuild the session using PID values that agree with the PMT and that do not create conflicts.
Input (1-8) ECM PID conflict	Minor	Program Specific Information (PSI) table data changed in the input stream.	Check the upstream MPEG input sources connected to the Netcrypt Bulk Encryptor. If the alarm does not automatically clear, contact Cisco Services.
Input (1-8) auto negotiate failure	Major	The Ethernet auto-negotiation algorithm has failed on the indicated (1-8) GbE port. **Note:** The GMAC device attempts to auto-negotiate again and clear the alarm on its own.	If the alarm does not clear, try connecting the Ethernet cable for that port to another port on the GbE hub/switch. Contact Cisco Services.
Input (1-8) PAT update	Status	The PAT seen at one of the inputs (1-8) on the Netcrypt Bulk Encryptor yields a version number change indicating that the input stream has changed.	No action required.
Input (1-8) PMT update	Status	The PMT for an MPEG program on input 1-8 has changed.	No action required.
Fan (1 - 5) failure	Major	One of the ventilation fans failed. **Note:** Fans are numbered 1 to 5 from front to back.	Verify that the fan power cable is connected. Contact Cisco Services
Power supply failure	Minor	At least one internal power	Contact Cisco Services.

Alarm Description	Alarm Level	Probable Cause	Check and Correct
Session xxxx data error where xxxx is a number from 0 to 3999	Minor	A **data_overflow** error indicates that the data rate for this session exceeds the threshold value. There is a potential for loss of programming content, black screens, freeze frames, and other degradations to services sent from this Netcrypt Bulk Encryptor.	Verify and correct any session setup problems including the session rate target and threshold values. Verify the sources feeding this Netcrypt Bulk Encryptor.
		A **data_underflow** error indicates that the data rate for this session drops to 0 (zero) or is a predefined percentage less than the threshold value.	Verify and correct any session setup problems including the session rate target and threshold values. If the session setup is correct, data is becoming corrupted. Verify the sources feeding this modulator. If loss of input signal is the cause, restore the input signal.
		A **data_pid_enable**_error indicates that a PID that should be enabled on the Netcrypt Bulk Encryptor is not enabled. (A PID is contained in the MPEG header to link MPEG packets together.)	If this alarm occurs with this Cause Code and then quickly clears, it is not a cause for concern. **Note:** If the alarm does not quickly clear, tear down the session, verify the session parameters, and restart the session. If the alarm reoccurs, the PID is missing from the input stream. Verify the missing PID with an MPEG analyzer.

7

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

Technical Specifications

Introduction

This appendix lists the power, rack, and environmental requirements for installing the Netcrypt Bulk Encryptor and provides technical specifications for the unit.

In This Appendix

Installation Requirements

This section lists the power, rack, and environmental conditions necessary for installing and operating the Netcrypt Bulk Encryptor.

Power Requirements Table

The following table describes the power specifications for the Netcrypt Bulk Encryptor.

Item	Specification
Supply Voltage	100–240 VAC 50/60 Hz 2.5 A
Fuse	Two 4.0 A SLO BLO 250 V fuses (Cisco part numbers 188106)
Line Frequency	47 to 63 Hz
Power Required	300 VA (maximum)
Power Dissipated	275 Watts (maximum)
In Current	■ 35 amps maximum, Vin = 100 VAC ■ 75 amps maximum, Vin = 240 VAC

Rack Requirements Table

The following table lists the rack requirements for the Netcrypt Bulk Encryptor.

Item	Specification
Rack Mount Type	EIA RS-310
Height	3.5 in./88.9 mm
Width	19 in./482.6 mm
Depth	22.5 in./571.5 mm
Weight	24.5 lb./11.10 kg

Environmental Requirements Table

The following table lists the environmental for the Netcrypt Bulk Encryptor.

Item	Specification
Operating Temperature	0°C (32°F) to 50°C (122°F) **CAUTION:** **Avoid damage to this product. Your warranty is void if you operate this product above the maximum specified operating temperature.** **Do not obstruct the air vents or fan vents on the sides of the unit. Otherwise, damage can occur to the unit.** **Important:** You must use the supplied notched rack mounts (part numbers 734845 and 734846) to mount the Netcrypt Bulk Encryptor in the rack. These rack mounts allow correct air circulation through the unit.
Storage Temperature	-10°C (14°F) to 70°C (158°F)
Operating Humidity	5% to 95%, non-condensing
Electrostatic Shock Susceptibility	No damage sustained from five discharges of 15 KV IEC electrostatic discharge model (150pF + 150 ohm) to all exposed connections

Connector Type Table

The following table lists the various types of connectors for the Netcrypt Bulk Encryptor.

Item	Specification
Gigabit Ethernet	SFP Module. Modules are available for duplex multimode fiber and copper interface
10/100 BASE-T Ethernet (2)	RJ-45
AC Power	IEC three wire (with integrated or close proximity power switch)
Craft (serial port) I/O	RS-232 serial port using an RJ-45 jack

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

March 2014 Part Number OL-28808-01