TACLANE-Micro Inline Network Encryptor

MOA No. GDC4S-CCEP-061-04

(U) Interface & Operator's Guide

For
TACLANE-Micro

Release 3.3

ADRL PM09-04

10 July 2007

Prepared for:
NATIONAL SECURITY AGENCY
9800 SAVAGE ROAD
FT. GEORGE G. MEADE, MD 20755

Prepared by:
GENERAL DYNAMICS
C4 Systems

77 "A" STREET
NEEDHAM, MA 02494-2806

(U) THIS PAGE INTENTIONALLY LEFT BLANK

(U) Document Revision History

UNCLASSIFIED//FOUO		
Document Revision Number	**Dated**	**Description of Revision**
First release Version 1	26 February 2007	Release of TACLANE-Micro for HAIPE IS 1.3.5
Version 2	30 April 2007	Qual testing PTRs, Appendix C
Version 3	16 May 2007	Added Figure for Mounting Information, fixed typos
UNCLASSIFIED//FOUO		

(U) Table of Contents

(U) List of Figures

(U) THIS PAGE INTENTIONALLY LEFT BLANK

1.0 (U) INTRODUCTION

1.1 (U) About the Manual

Purpose

(U//FOUO) The purpose of this manual is to explain how to install, operate, and reconfigure the General Dynamics TACLANE-Micro (KG-175D) encryptor.

Audience

(U//FOUO) This manual is intended for operators with a basic understanding of IP networking, as well as data encryption.

Edition

(U//FOUO) This is the Operator's Manual for the TACLANE-Micro. It includes information specific to TACLANE-Micro Release 3.3. Release 3.3 is HAIPE IS v1.3.5 compliant and supports the BATON and MEDLEY traffic encryption algorithms.

Changes

(U//FOUO) The information presented in this manual is subject to change without notice. Any changes will be incorporated in subsequent editions, or change pages will be issued.

Contents

(U//FOUO) This manual covers the following topics:

Terminology: Operator vs. User

(U//FOUO) Throughout this manual, the term "operator" describes individuals who control the TACLANE. The term "user" describes individuals who control equipment on the PT-side of the TACLANE that is protected by the TACLANE.

Screen Snapshots

(U//FOUO) Screen snapshots for displaying information are shown in the SSO disabled mode. If the operator is SSO enabled, the screen will be slightly different.

1.2 (U) Reference Documents

Related TACLANE Documents

(U//FOUO) Additional information about TACLANE can be found in the following documents:

Document Number	Title	Rev	ADRL # or CDRL #	Date	Classif (U,C,S)
	TACLANE-Micro Interface Control Document				**U**
µTL-016-02	Key Management Plan for TACLANE-Micro		PM03	1/18/07	**S**
µTL-031-01	Security Features Users Guide for TACLANE-Micro		PM13	2/16/07	**S**

Other Referenced Documents

(U//FOUO) The following table lists information on other documents referenced in this manual.

Document Number	Title	Rev	ADRL or CDRL #	Date	Classif(U,C,S)
CNSSI No. 3029	Operational Systems Security Doctrine for TACLANE-Micro (KG-175D)	-	N/A	27-Mar-2003	U
0N477430	DTD User's Manual	latest rev	N/A	latest rev	U
Not available	Simple Key Loader (https://rdit.army.mil/commsc for AN/PYQ-10(C))				U

GEM X	GEM X Operator's Manual				U

Related IP Network Documents

(U//FOUO) Additional information about related network interfaces is provided in the IETF STDs and RFCs for IP networking.

1.3 (U) Acronyms and Abbreviations

Acronyms and Abbreviations

(U//FOUO) The following acronyms and abbreviations are used in this manual:

Acronym/ Abbr.	Definition
AC	Alternating Current
ACL	Access Control List
AH	Authentication Header
ARP	Address Resolution Protocol
AWG	American Wire Gauge
BGL	Bad Guy List
CC	Crypto Card
CCI	Controlled Cryptographic Item
CD	Compact Disc
CF	Central Facility
CIK	Crypto Ignition Key
COMSEC	Communications Security
CSESD	Communications Security Equipment System Document
CT	Ciphertext
D	Depth
DAC	Discretionary Access Control
dB	Decibel
dBm	Decibel (referenced to milliwatts)
DC	Direct Current
DF	Don't Fragment
DoD	Department of Defense
DoDAAC	Department of Defense Activity Address Code
DRAM	Dynamic Random Access Memory
DS	Differentiated Services

Acronym/ Abbr.	Definition
DSCP	Differentiated Services (DIFFSERV) Code Point
DTD	Data Transfer Device
ECN	Explicit Congestion Notification
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFF	Enhanced FIREFLY
EKMS	Electronic Key Management System
EMI	Electromagnetic Interference
ENET	Ethernet
ESP	Encapsulating Security Payload
F	Fahrenheit
FF	FIREFLY
FFVS	FIREFLY Vector Set
FPL	Fixed Packet Length
FSU	Field Software Upgrade
ft.	Feet
FTR	Field Tamper Recovery
GBSI	Global Broadcast Service Interface
GND	Ground
H	Height
HAIPE IS	High Assurance Internet Protocol Interoperability Specification
HEMP	High-altitude Electromagnetic Pulse
HHMMWV	Heavy High Mobility Multipurpose Wheeled Vehicle
HMI	Human-Machine Interface
Hz	Hertz
ICD	Interface Control Document
ICMP	Internet Control Message Protocol
ID	Identifier
ID	Inside Diameter
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
in.	Inches
INE	In-line Network Encryptor
IP	Internet Protocol
IPv4	IP version 4

Acronym/ Abbr.	Definition
KG	Key Generator
km.	Kilometers
KMID	Key Material ID
KSD	Key Storage Device
LAN	Local Area Network
lbs.	Pounds
LC	Lampert Connector
LCD	Liquid Crystal Display
LED	Light Emitting Diode
m.	Meters
MAC	Mandatory Access Control
MAC	Medium Access Control
MAX	Maximum
Mbps	Megabits per second
MDI	Media Dependent Interface
MIB	Management Information Base
MTBF	Mean Time Between Failures
MTEK	Main Traffic Encryption Key
MTU	Maximum Transmission Unit
µm.	Micrometers
NA	Numerical Aperture
NIC	Network Interface Card
nm.	Nanometers
NSA	National Security Agency
NSN	National Stock Number
PC	Personal Computer
PIN	Personal Identification Number
PMTU	Path Maximum Transmission Unit
PPK	PrePlaced Key
PSEQN	Payload Sequence Number
PT	Plaintext
RECIPe	Remote Encryptor Configuration Information Protocol
RFC	Request For Comment
SA	Security Association
SAMP	Security Association Management Protocol
SDD	Secure Dynamic Discovery

Acronym/ Abbr.	Definition
SDNS	Secure Data Network System
sec.	Seconds
SKL	Simple Key Loader
SNMP	Simple Network Management Protocol
SP	Security Processor
SSO	Site Security Officer
STD	Standard
STP	Shielded Twisted Pair
SW	Software
TEK	Traffic Encryption Key
TFS	Traffic Flow Security
TL	TACLANE
TOS	Type of Service
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
W	Watts
W	Width
WAN	Wide Area Network

1.4 (U) Safety Information

General (U//FOUO) The following general safety precautions must be observed during installation and operation of the TACLANE.

Liability (U//FOUO) General Dynamics assumes no liability for the customer's failure to comply with these requirements.

Grounding (U//FOUO) TACLANE ground: A ground wire is recommended for all installations. Verify that the ground wire is connected properly to an earth ground and connected properly to the TACLANE ground binding post.

Lightning (U//FOUO) Do not connect or disconnect cables during periods of lightning.

AC Power Safety

(U//FOUO) Make sure that the power rating and frequency of the power source match the requirements for the TACLANE.

AC power cord: The AC power cord ends in three-pole grounding plugs. Do not use three-pole to two-pole adapters with these plugs.

AC outlet: Verify that the AC outlet used is properly installed and grounded. The outlet must comply with applicable National Electric Codes.

Electrical Shock

(U//FOUO) There are no operator-serviceable parts inside the TACLANE chassis. There is a risk of electrical shock inside TACLANE. Any service should be performed only by depot personnel.

Lithium Battery

(U//FOUO) TACLANE may have a lithium battery installed. Do not incinerate lithium batteries because of the risk of explosion. Lithium batteries will last up to two years; scheduled replacement is recommended.

Alkaline Battery

(U//FOUO) TACLANE may use an alkaline battery as a backup or in places where a lithium battery is not available. Battery lifetime for alkaline batteries is approximately three months when the TACLANE-Micro is not connected to prime power.

1.5 (U) Hardware Versions

TACLANE-Micro

(U//FOUO) The following table identifies the base part number for the TACLANE-Micro product. Refer to section 2.0 of this document for a description of the capabilities of TACLANE-Micro.

Base Part Number	TACLANE Version
MC-10901-2	TACLANE-Micro (KG-175D)

Other TACLANE Versions

(U//FOUO) The following table identifies the base part numbers for other TACLANE versions.

Base Part Number	TACLANE Version & Description
0N649470-1 (AC) 0N649470-2 (DC)	TACLANE-Classic (KG-175) – supports 10Mbps IP/Ethernet and ATM DS3 (up to 45 Mbps rate) encryption; rear panel shows RJ-45, AUI, and BNC connectors.
0N649470-3 (AC) 0N649470-4 (DC)	TACLANE-GBSI (KG-175) – supports ATM OC3 encryption (up to 45 Mbps rate); rear panel shows MT-RJ connectors.
0N649470-7 (AC) 0N649470-8 (DC)	TACLANE AUS (KG-175) – Australian version of the TACLANE-Classic
0N649470-9 (AC) 0N649470-10 (DC)	TACLANE CAN (KG-175) – Canadian version of the TACLANE-Classic
0N649470-17 (AC) 0N649470-18 (DC)	TACLANE NZL (KG-175) – New Zealand version of the TACLANE-Classic
0N649470-5 (AC) 0N649470-6 (DC)	TACLANE-E100 (KG-175) – supports IP/Ethernet (10/100+ Mbps) encryption; rear panel shows MT-RJ and RJ-45 connectors.
0N649470-13 (AC) 0N649470-14 (DC)	TACLANE-E100 AUS (KG-175) – Australian version of the TACLANE-E100
0N649470-15 (AC) 0N649470-16 (DC)	TACLANE-E100 CAN (KG-175) – Canadian version of the TACLANE-E100
0N649470-19 (AC) 0N649470-20 (DC)	TACLANE-E100 NZL (KG-175) – New Zealand version of the TACLANE-E100
0N684240-1	TACLANE-GigE (KG-175A)
0N649755-1	TACLANE-Mini (KG-175B)

1.6 (U) Programmable Image Version

General

(U//FOUO) The TACLANE-Micro programmable image version is comprised of the software and FPGA images needed to perform the TACLANE-Micro feature set.

Software Versions

(U//FOUO) The TACLANE-Micro programmable image version 3.3 is the initial release of these products. The first TACLANE-Micro release supports HAIPE IS v1.3.5 compliant IP encryption.

1.7 (U) Customer Support and Contacts

TACLANE Help Desk

(U//FOUO) For technical support and installation questions, please contact the General Dynamics C4 Systems Help Desk at:

Phone: (877) 230-0236
E-mail: infosecsupport@gdc4s.com

TACLANE Product Registration

(U//FOUO) TACLANE product registration is recommended. Contact the TACLANE Help Desk to register a TACLANE unit. Registration information includes:

- TACLANE unit serial number
- Operational location
- User Representative POC.

TACLANE Sales Support

(U//FOUO) For TACLANE sales support inquiries, please contact the TACLANE Sales Support group at:

Phone: 888-TYPE1-4-U (888-897-3148)
E-mail: infosec@gdc4s.com.

TACLANE Training

(U//FOUO) General Dynamics offers a TACLANE Operator Training Course that teaches how to install, configure, and maintain TACLANE encryptors in an operational environment. This course is for network engineers, operators, and security and system administrators who will be installing, configuring, and operating TACLANE encryptors. Course attendance requires a U.S. Government Secret Clearance, COMSEC briefed. This interactive four-day course combines classroom presentations and hands-on exercises to give you practical operator experience. To register or to get more information on the course, contact:

Training Coordinator
General Dynamics C4 Systems
1190 Winterson Rd., Suite 300
Linthicum, MD 21090

Phone: (410) 487-0220
Fax: (410) 850-5005
E-mail: infosectraining@gdc4s.com
Web: www.gdc4s.com/

NSA Government Approval Office

(U//FOUO) Refer to the Operational Systems Security Doctrine for TACLANE-Micro (KG-175D).

2.0 (U) ABOUT THE TACLANE

2.1 (U) Introduction

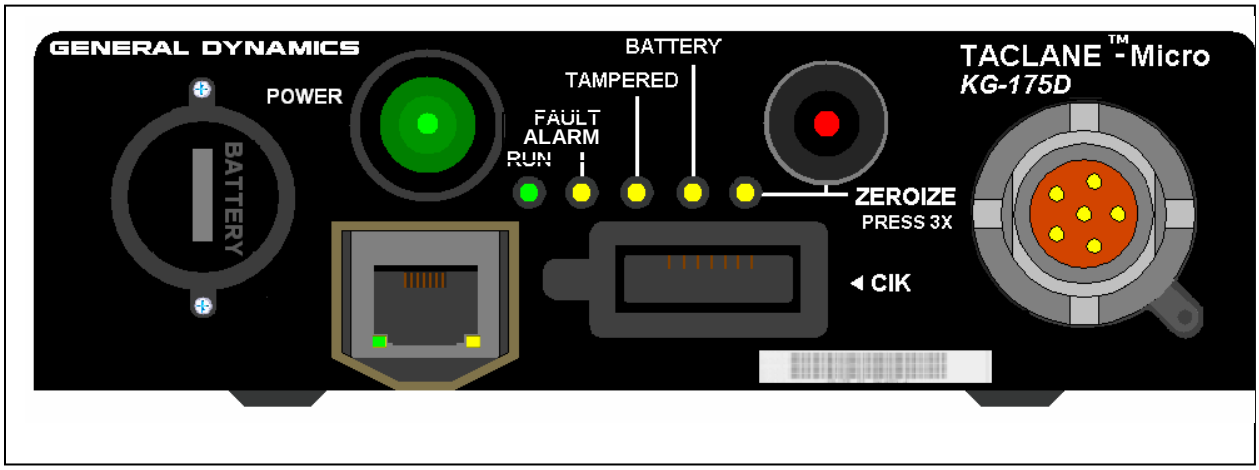
What is the TACLANE?

(U//FOUO) The TACLANE-Micro (KG-175D) is part of the TACLANE family of in-line network encryptor (INE) devices developed by General Dynamics C4 Systems (GDC4S) to secure the transfer of Internet Protocol (IP) datagram traffic for network applications. The TACLANE family of products provides low-cost, key-agile, in-line-network encryption for deployment in tactical and strategic networks.

(U//FOUO) The TACLANE-Micro provides 10/100 Mbps secure communication over fast IP networks. The TACLANE-Micro supports a 100 Mbps optical interface as well as an auto sensing 10/100 Mbps electrical interface.

(U//FOUO) The Type 1 encryption provided by the TACLANE is part of the Department of Defense *Defense in Depth* strategy and is only one portion of the overall defense in depth. A comprehensive network Information Assurance strategy involving *Defense in Depth* is required to ensure secure and reliable protection for sensitive and classified information.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure 2.1-1 (U) TACLANE-Micro (KG-175D)

2.2 (U) Concepts

IP Network Concepts

(U//FOUO) Below are some basic IP network concepts useful in understanding TACLANE:

Concept	Definition
IP Network	Interconnected fabric of routers and user equipment (hosts, etc.) supporting the connectionless transmission of data using IP datagrams. IP datagrams are variable-length, with a typical maximum size of 1500 bytes for IP/Ethernet. An IP address (IPv4) is 4 octets long, and is configured either manually or automatically. IP networks provide an unreliable data service, and upper-layer protocols are relied upon to provide reliable data transport. IP addresses are mapped to underlying network (physical) addresses for IP datagram transmission over the underlying network. (For example, in IP/Ethernet, IP addresses are mapped to Ethernet MAC addresses using ARP.)

Keying Concepts

(U//FOUO) Below are basic keying concepts useful in understanding TACLANE:

Concept	Definition
CIK	A CIK is a Crypto Ignition Key used to unlock wrapped key stored within the TACLANE. A valid CIK is needed to operate the TACLANE.
FIREFLY Vector Set	FIREFLY Vector Sets (FFVS) are used to dynamically generate pairwise FIREFLY Traffic Encryption Keys (TEKs) between communicating TACLANEs. FIREFLY Vector Sets are generated by the EKMS CF. Each FIREFLY vector set has a unique Key Material ID (KMID), Universal ID and Universal Edition assigned by the EKMS CF. In addition, a vector set may be ordered in a particular partition, which shows up as a partition code assigned to the vector set. TACLANE supports both the basic FIREFLY vector set and the enhanced FIREFLY (EFF) vector set.

Concept	Definition
TEK	Traffic Encryption Keys (TEKs) are used to encrypt and decrypt IP traffic. TEKs can be cooperatively generated FIREFLY TEKs or manually filled PPKs (traditional TEKs).
PPK	PPKs are manually filled traditional TEKs. PPKs are generated by the EKMS CF and are uniquely identified by the following information: 1. Short Title 2. Edition 3. Segment. When filled, each PPK is associated with an effective date.
DTD	DTDs are used to fill FIREFLY vector sets and PPKs.
SKL	SKLs are used to fill FIREFLY vector sets and PPKs.
PPK Changeover	PPK changeover replaces an old PPK with a new PPK. The new "changeover" PPKs are filled in advance and each changeover is accomplished based on the effective date of the new changeover PPK.
Zeroize	A panic zeroize deletes all keys.

TACLANE Security Concepts

(U//FOUO) Below are basic TACLANE security concepts:

Concept	Definition
Secure Virtual Network	TACLANE-protected enclaves at one security level communicating across a base network at a different security level.
Secure Communications	Device state in which TACLANE secures user traffic.
Security Association	An IP datagram tunnel secured by a TACLANE. There is at most one set of active security associations between a given pair of TACLANEs at any time. (The set includes 1 duplex SA and one multicast SA.). All user IP datagram traffic passed between a pair of TACLANEs is protected using the same security association.
Initiator	TACLANE at origin of security association.
Responder	TACLANE at destination of security association.

Concept	Definition
Access Control	Access controls are either mandatory (MAC) or discretionary (DAC). When a FIREFLY TEK is generated, TACLANE MAC checks include partition code and security level (both must be the same for the initiator and responder). MAC checks are always performed and cannot be disabled. TACLANE DAC is in the form of an operator-editable list of KMIDs. When the operator enables access control (see the chapter on "Configuring Access Control and the Network Manager"), the TACLANE only allows FIREFLY TEKs to be generated with remote FIREFLY vector sets having KMIDs on the operator's access control list. Security Administrator access is enforced using DAC. The SSO PIN must be provided to acquire access to Security Administration configurations. SNMPv3 uses shared secrets based on operator entered passwords to acquire access to any configuration or monitoring MIBs.
Bypass	PT data that is forwarded without encryption to the CT network, or CT data that is forwarded without decryption to the PT network.
Alarm	The result of an internal failure. Power can be cycled to attempt to recover from an alarm condition.
Tamper	The result of opening the TACLANE chassis, loss of battery power, or removal of the battery while TACLANE is powered off.

2.3 (U) Capabilities

TACLANE-Micro Capabilities

(U//FOUO) TACLANE-Micro supports IP datagram encryption over an Ethernet 10/100Base-TX or 100Base-FX physical interface:

- 200 Mbps aggregate throughput, full duplex
- HAIPE IS v1.3.5 compliant IP encryption
- 512 security associations supported for user traffic (one security association protects all user traffic between a given pair of TACLANEs)
- Automated peer TACLANE discovery for security associations using Secure Dynamic Discovery (SDD)
- PPK or dynamically generated FIREFLY TEK for each security association
- Enhanced FIREFLY (EFF) support
- Up to 16 PPK chains to be used for user traffic and SDD, with up to eleven changeover PPKs in each PPK chain
- IP TFS controls: Fixed Packet Length, PSEQN Checking, Type-of-Service (DSCP) Bypass, DF Bit bypass, IGMP Bypass, PMTU Bypass
- Auto-Negotiating 10Base-T vs. 100Base-TX Ethernet interface
- Static multicast with PPK
- Remote TACLANE static routes
- Over the Network Software Download and Field Software Upgrade
- Up to 9 simultaneous network managers.

Periods Processing at Multiple Levels

(U//FOUO) TACLANE can communicate at multiple security levels, one level at any given time. The SSO-privileged operator selects the security level. TACLANE products no longer support multilevel FIREFLY Vector Sets. The classification level of the vector set must match the operating level of the TACLANE to be activated.

Easy to Use

(U//FOUO) The TACLANE-Micro Human-Machine Interface (HMI) is web-browser based. It uses the menu structure of the simple menu interface common to all TACLANE models. The HMI is accessed by connecting a PC running browser software to the front-panel-mounted Ethernet Port provided for the Console, and entering the IP address of the Console Port into the browser address window. Refer to section 2.4 ("Web-based Human-Machine Interface (HMI)") for more details on the TACLANE-Micro HMI.

(U//FOUO) Multiple instances of the web-browser running on the operator's terminal can access a TACLANE-Micro HMI at the same time. This allows various multiple status screens to be displayed at the same time a command screen is being used to configure the TACLANE-Micro. This may be helpful, for example, in making configuration changes based on audit log entries or status displays. Status screens have to be manually refreshed to maintain currency. Managing a TACLANE-Micro through multiple instances of the web-browser in a time-interleaved fashion would cause command errors. These errors necessitate the operator reissuing a command if one or more commands are made from other instances between the loading of a command screen and execution of the command.

Local Key Management

(U//FOUO) The CIKs control access to the functionality of the TACLANE, and protect the encryption keys that have been filled into the TACLANE. An SSO-privileged operator can create up to two additional CIKs. These three CIKs can be used to allow multiple operators, independent, one-at-a-time access to a TACLANE-Micro. An SSO-privileged operator can delete any CIK except the active CIK, the CIK inserted when the TACLANE-Micro most recently started or restarted.

Access Control

(U//FOUO) The Mandatory Access Control function checks:

- Partition code of FIREFLY vector set
- Current security level of TACLANE-Micro.

Before initiating FIREFLY TEK generation. These must be the same for the initiator and the responder TACLANE.

(U//FOUO) The operator-selectable, Discretionary Access Control function checks the operator-editable Access Control List which contains a list of KMIDs (FIREFLY TEKs are only generated with remote FIREFLY vector sets having KMIDs on the ACL).

(U//FOUO) Functional access control is provided through the use of the CIK. When the CIK is removed, the TACLANE-Micro resets, causing all security associations (traffic and management connections) to be lost. The TACLANE-Micro then proceeds through a power-up sequence, pausing until a valid CIK is inserted. When a valid CIK is inserted, the TACLANE-Micro resumes the power-up sequence, returning to the device state in which it was operating immediately before the CIK was removed (Auto-Recovery).

NSA-Certified Type 1

(U//FOUO) TACLANE is NSA-certified to provide Type 1 encryption and decryption for information classified TOP SECRET codeword and below. When a valid CIK is inserted, the TACLANE is classified at the highest classification level of the key it contains. When the CIK is removed, the TACLANE is UNCLASSIFIED, but remains a Controlled Cryptographic Item (CCI), and the CIK is UNCLASSIFIED.

Field Software Upgrade and Field Tamper Recovery

(U//FOUO) The TACLANE software supports local and remote Field Software Upgrade (FSU) and local Field Tamper Recovery (FTR) capabilities. FSU allows a Site Security Officer (SSO) to upgrade the software in a TACLANE-Micro from an UNCLASSIFIED encrypted image on a CD. FTR enables a SSO to recover a TACLANE-Micro from a benign tamper using a classified SECRET Recovery CIK. Both features help reduce downtime since units no longer need to be sent to the depot for software upgrades or tamper recoveries. Please see the sections on "Performing a Field Software Upgrade" and "Performing a Field Tamper Recovery" for more information.

IP Traffic Flow Security

(U//FOUO) TACLANE software incorporates IP Traffic Flow Security features in accordance with version 1.3.5 of the HAIPE IS Traffic Flow Specification. These features prevent/reduce compromise of sensitive information due to certain types of attacks. Configuration of IP TFS parameters is restricted to the SSO; it is only possible to modify IP TFS parameters when the SSO privileges are enabled. The IP TFS features include:

- Fixed Packet Length (FPL) for outgoing CT encrypted traffic
- Payload Sequence Number (PSEQN) checking for incoming CT encrypted traffic
- Type-of-Service (including DSCP) bypass control
- Don't Fragment (DF) Bit bypass control
- IGMP bypass control
- PMTU bypass control.

(U//FOUO) Please see the chapter on "Configuring IP Traffic Flow Security Parameters" for more information.

Remote Management – Supported SNMP MIBs

(U//FOUO) The full functionality of the TACLANE-Micro can be remotely managed by GEM X, or an equivalent SNMPv3 Network Manager configured to use the GenDyn-EmbeddedProducts-Enterprise-MIB and portions of the HAIPE-MIB (Enterprise MIB) and standard MIBs listed below:

- GDC4S-ASSIGNMENTS-MIB (Enterprises # 1.3.6.1.4.1.576)
  - GDC4S-ENCRYPTION-PRODUCTS-MIB
    - TACLANE-MICRO-COMMON-MIB
    - TACLANE-MICRO-VERSION-ONE-MIB
    - GDC4S-ENCRYPTION-PRODUCTS-COMMON-MIB
    - NETWORKENCRYPTOR-ENTERPRISE-MIB
      - GDC4S-EXPERIMENTAL-TACLANE-MICRO-MIB
        - GDC4S-HAIPE-ASSIGNMENTS-MIB
          - GDC4S-HAIPE-FEATURE-HIERARCHY-MIB
            - GDC4S-HAIPE-MANAGEMENT-MIB
            - GDC4S-HAIPE-NETWORKING-MIB
              - GDC4S-HAIPE-NETWORKING-DISCOVERY-MIB
            - GDC4S-HAIPE-TRAFFIC-PROTECTION-MIB
- RFC 3418, System and SNMP Traps
- RFC 2863, Interfaces and IF
- RFC 2790, Host Resources MIB
- RFC 3014, Notification Log MIB
- RFC 3414, SNMP-USER-BASED-SM-MIB
- RFC 3415, SNMP-VIEW-BASED-ACM-MIB
- RFC 3413, SNMP-TARGET-MIB
- RFC 3411, SNMP-FRAMEWORK-MIB
- RFC 3412, SNMP-MPD-MIB
- RFC 3636, MAU-MIB.

Remote Management – Features

(U//FOUO) The TACLANE-Micro is designed such that up to nine remote security managers have the same management capabilities as are provided to the local manager. These capabilities include:

- PPK Assignment Table management
- Security Audit Log and Event Log management
- Static Routing Table management
- Device Date and Time management
- Device State management
- Trap management
- Device statistics management
- Firmware Download and Installation management
- TFS management
- Security Association/Host Table management
- Discretionary Access Control management
- Interface IP Address management.

Remote Management - Security

(U//FOUO) TACLANE-Micro can be managed from the Plaintext (PT) or Ciphertext (CT) side. Regardless of whether the Remote Manager is on the CT-side or the PT-side, SNMPv3 privacy and authentication protection is provided to all management traffic. In addition, CT-side management traffic is encrypted between the TACLANE fronting the Remote Management Workstation and the managed TACLANE.

(U//FOUO) Information on configuring TACLANE for remote management is in the section titled "Configuring the Network Manager". Please refer to the appropriate GEM X Operator's Manual for more information on configuring the HAIPE device fronting the GEM X and for more information on the GEM X Remote Management software.

2.4 (U) Web-based Human-Machine Interface (HMI)

Web-Browser-Based HMI

(U//FOUO) The Human-Machine Interface (HMI) in the TACLANE-Micro provides the local operator a web-browser-based replacement to the simple menu interface common to previous TACLANE models. This new HMI requires a PC running a web-browser application be connected to the TACLANE-Micro via the Console port on the front panel of the TACLANE-Micro. (The HMI is designed for Microsoft Corp's Internet Explorer® version 5.5 or later running with Windows 95, 98, Me, 2000, or XP operating system, although other browsers running under other operating systems may provide satisfactory performance.)

(U//FOUO) The IPv4 address for the TACLANE-Micro Console/HMI interface port is **172.16.0.1**. This address is entered in the address window of the web-browser to allow access to the TACLANE-Micro HMI by the local operator.

(U//FOUO) It is recommended that the controlling PC's Ethernet address should be on the 172.16 network to enable communication with the TACLANE-Micro 172.16.0.1 console interface.

(U//FOUO) The HMI console Ethernet is designed for full duplex operation, where the console is directly connected to the TACLANE-Micro.
Note: Use of a Hub on the console interface may result in receive buffer lockups caused by Ethernet errors. Recovery requires TACLANE-Micro to be restarted.

(U//FOUO) The operator interface flows were sustained to enable existing TACLANE (GigE/Mini/Classic/E100) operators to use TACLANE-Micro without retraining. The larger screen area of the VGA display allows the presentation of descriptive command names, status messages and data labels, in addition to on-screen help. This improved display provides an intuitive HMI for new operators.

Web-Browser-Based HMI Terminal Requirements

(U//FOUO) The TACLANE-Micro console interface is Unclassified. It is trusted to prohibit exposure of classified information to a connected PC. Therefore, a PC is not required to be dedicated to this activity unless local policy requires. However, the PC should not be connected to a network while connected to the TACLANE to ensure adequate security. Refer to the NSA Doctrine for specifics on connecting a PC to the KG-175D console interface.

(U//FOUO) The minimum hardware requirements for a PC connected to the console Ethernet interface to access the TACLANE-Micro HMI are:

- Unclassified PC (or notebook), or similar device with:
  - Network Adapter - 10BaseT Ethernet-capable
  - Display Adapter - supporting VGA (640 X 480) or higher resolution
  - Video Display - supporting VGA (640 X 480) or higher resolution
  - Keyboard
  - Pointing Device (Mouse, Trackball, Touchpad, etc.)
  - CD-ROM (for TACLANE-Micro Software Download only)

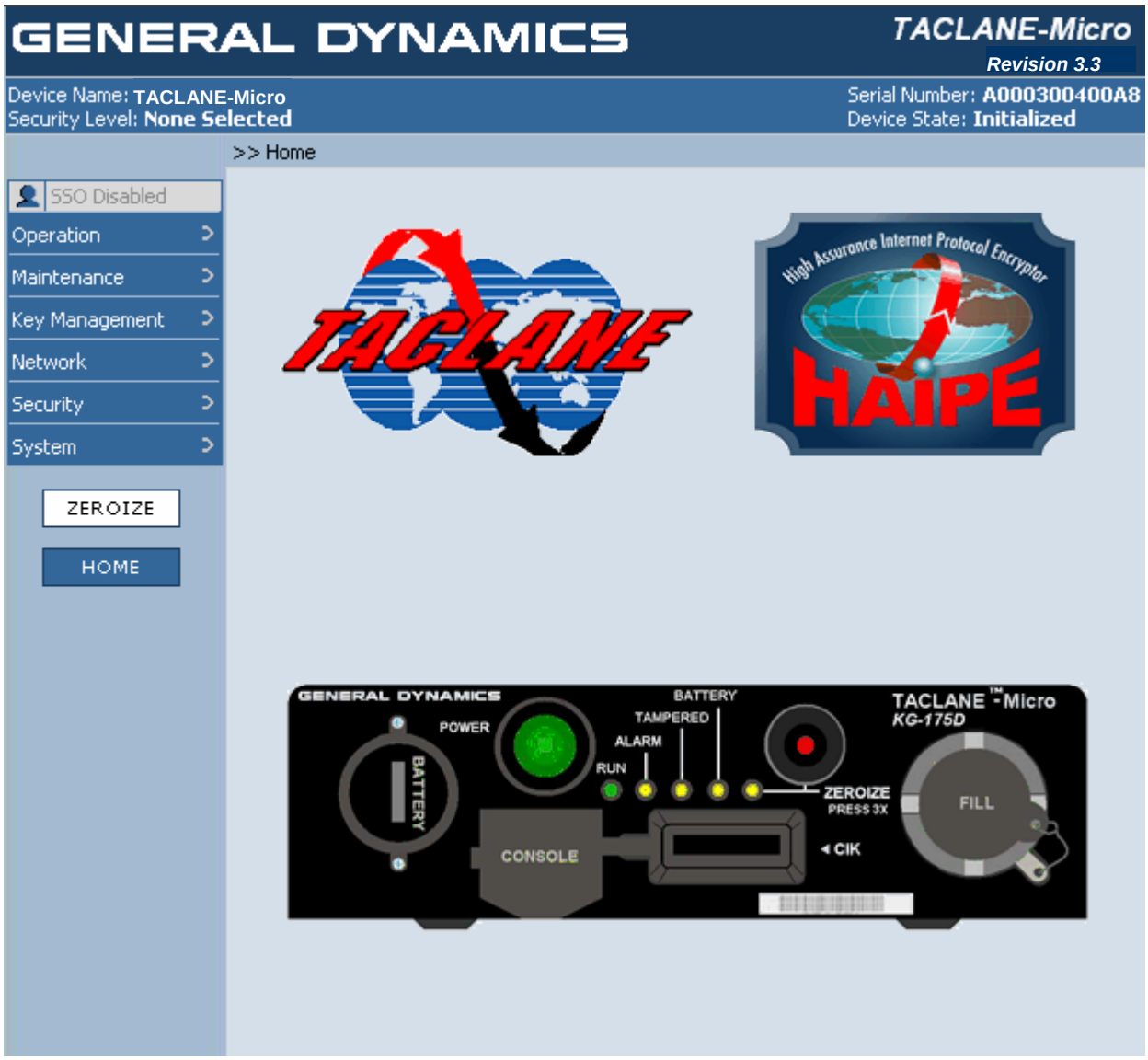
(U//FOUO) A keyboard-only mode of operation is provided, principally to maintain HMI functionality in the event of a pointing device failure.

(U//FOUO) The TACLANE-Micro HMI is compatible with Microsoft Internet Explorer®, version 5.5 or later, running with Windows 95, 98, Me, 2000, or XP operating system. Other compatible browsers and operating systems also work.

Enhanced HMI Display

(U//FOUO) Figure 2.4-1 below shows the TACLANE-Micro HMI screen format.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure 2.4-1 (U) TACLANE-Micro HMI Screen Format

Screen Area	Description
Header Area	(U//FOUO) Within the Header Area of the TACLANE-Micro HMI, the following information is displayed. • Programmed Image Version • System Name (operator entered) • Device Serial Number (same on unit, HMI, ESN and Station ID) • Device Security level • Device State.
Menu Area	(U//FOUO) The Menu Area contains button icons, which provide HTML links to the web pages used to manage the TACLANE-Micro. The root menu is always displayed, and contains the following menu items: • Operation • Maintenance • Key Management • Network • Security • System. When the operator moves the on-screen cursor over one of these root menu items, the next lower level set of menu items pops up, and in a similar fashion, each successive lower level in the menu tree is displayed with an additional pop-up. Menu items have been added when necessary to support the increased functionality of the TACLANE-Micro over earlier versions of the TACLANE. The Menu Area also includes button icons for instant access to the Zeroize command, and to command the display return to the Home screen.
Information Content Area	(U//FOUO) The Information Content Area is divided into four functional areas (as applicable to the active screen), each running the width of the screen. • Across the top is displayed the path through the menu tree used to access the currently displayed screen. This path is referred to as the breadcrumb. • The Screen Title, a RELOAD button icon, and a HELP button icon are displayed in the second area. The Screen Title identifies the current screen. The RELOAD button icon, when selected, causes the data fields on the screen to be refreshed/reloaded with the data held by the TACLANE-Micro. This is helpful when some of the displayed data items have been edited but not saved, and the operator wishes to return to the saved values. The HELP button icon launches another instance of the web-browser application, which displays the portion of the Help file relevant to the current screen. • The third functional area displays a status message relating to the current screen or TACLANE-Micro response to a previously issued command. The fourth area, depending on the particular screen displayed, contains fields for displaying TACLANE-Micro configuration, status or log data, or entering TACLANE-Micro configuration data. In addition, depending on the particular screen, button icons are also displayed to navigate to related screens, cancel the present screen, or initiate the command or enter the configuration data changes made on the displayed screen.

Automatic Scrolling

(U//FOUO) In some cases, the amount of information displayed extends beyond the bottom of the Information Content Area. In those cases, the operator may use the elevator on the right-hand of the browser window to scroll down to see the remainder of the screen. Side-to-side scrolling is never required to view the TACLANE-Micro screen when using a display with VGA (640 x 480) resolution or greater.

Screen Area	Description
Screen Updates	(U//FOUO) The time-variable information displayed in the Header Area of the TACLANE-Micro HMI screens is updated periodically through a polling process under the control of the web-browser application. This ensures that the displayed Device Security Level and Device State are current. (U//FOUO) The fields in the fourth area of the Information Content Area, containing TACLANE-Micro configuration, status, or log data are not updated dynamically. Information is displayed as of the time a function is selected, i.e., the date/time screen does not change dynamically. These data fields can be updated by selecting the RELOAD button icon or selecting the screen from the menu. (U//FOUO) In the event another operator changes configuration data for a particular TACLANE-Micro between the time when the first operator last updated the screen, and when that first operator sends edits to the TACLANE-Micro, an error message and updated data will be returned to the first operator, and the first operator will have to reenter the edits.

'SSO Privileged' HMI Commands

(U//FOUO) These commands are noted in the HMI menu tree in section 3.8 ("HMI Menu Tree").

Access to 'SSO Privileged HMI Commands

(U//FOUO) Many HMI commands can be accessed by an operator but contain additional functionality for an SSO. This means that a user without SSO privileges 'enabled' can display the data for the command but a user that has SSO privileges 'enabled' has access to configure data via the command. SSO-privileges are enabled by entering the valid SSO PIN after obtaining functional access to the TACLANE-Micro. Refer to sections 9.16, 9.17, and 9.18 of this Operator's Manual for information on how to Enable SSO Privileges, Disable SSO Privileges, and Generate the SSO PIN, respectively.

3.0 (U) INSTALLING AND OPERATING THE TACLANE

3.1 (U) Unpacking

Unpacking

(U//FOUO) Before opening the package containing the TACLANE, inspect the package for shipping damage. Notify the carrier if the package shows signs of shipping damage.

Important

(U//FOUO) Keep all original packing material as it may be needed for storing or transporting the TACLANE. TACLANEs under warranty that are returned to General Dynamics must be in their original packing material.

3.2 (U) Equipment Checklist

System Components

(U//FOUO) The following table lists the TACLANE equipment part numbers including separately available equipment

Item	Qty	Description
1	1	TACLANE-Micro Part number: MC-10901-2
2	2	CIKs (1 initialized CIK, 1 blank spare and 2 CIK tags) shipped separately Part number: MC-101A (SST16Kb)
3	1	FTR CIK (Recovery CIK)
4	1	3.6V AA lithium battery (inside battery compartment) NSN: 6135-01-301-8776
5	1	External power supply with power cable Part number: MC-103A
6	3	CAT-5 cables (one for console, one for PT interface, and one for CT interface). Available separately. Part number: MC-102A (not included with unit)
7	2	Duplex Multimode (LC connector) Fiber pair cables (one for PT data interface and one for CT data interface). Available separately. Part number: MC-104A (not included with unit)
8	1	Operator's Manual for TACLANE-Micro included on CD-ROM

Recovery CIK

(U//FOUO) A Recovery CIK, needed to perform Field Tamper Recovery, is included when ordering a TACLANE. The Recovery CIK can be used to recover its associated TACLANE from a benign tamper (a maximum of five times) without returning it to the depot. The Recovery CIK is classified SECRET and must be shipped separately from the TACLANE. If the TACLANE is sent to a COMSEC account, then the Recovery CIK will be sent to that account's classified mailing address. If the TACLANE is sent to a DoDAAC, the Recovery CIK will be sent upon receipt of a valid classified mailing address for the receiving activity.

(U//FOUO) Recovery CIKs are TACLANE unit specific. Please make sure to note the serial number of the TACLANE associated with the Recovery CIK. Do not attempt to use Recovery CIKs in TACLANE units other than the one with which it is associated.

Rack Mount for TACLANE-Micro

(U//FOUO) The TACLANE-Micro can be placed on a shelf in a 19" rack and screwed in from the bottom. Three TACLANE-Micros will fit on a single shelf.

Additional Equipment Required

(U//FOUO) The following items not supplied with the TACLANE are required for configuring the unit:

- PC (or notebook)
- Web-Browser Software, Microsoft Internet Explorer® version 5.5 or higher, or equivalent
- Category 5, RJ45-to-RJ45 Ethernet Patch Cord.

(U//FOUO) The following items not supplied with the TACLANE are required for filling key:

- DTD (AN/CYZ-10(V3)) NSN: 5810-01-393-1973
- SKL (AN/PYQ-10©) NSN: 7010-01-517-3587
- Fill cable for DTD.

Important CIK Note

(U//FOUO) The Key Storage Devices are 16 Kbit storage devices.

3.3 (U) Handling and Environmental Conditions

TACLANE-Micro Handling and Environmental Specifications

(U//FOUO) Below are important TACLANE-Micro handling and environmental specifications:

Specification	Remarks
Size	1.61 in. H x 5.5 in. W x 10.85 in. D (without external power supply)
Weight	4.25 lbs.
Power	• Primary power input voltages to the external supply are auto-ranging with the following ranges: 90-246 VAC • TACLANE-Micro input frequency is 47-63 Hz • Output of the external power supply is 12 VDC • Dissipation: 30 watts max. within its operating temperature range
Temperature	• Non-operating: -40°C to +71 °C • Operating (no warm-up): -40°C to +60°C
Humidity	• Up to 95% non-condensing
Altitude	• Operating: 0' to 15,000' IAW MIL-STD-810F • Transport: 0' to 40,000' IAW MIL-STD-810F
TEMPEST	NSTISSAM TEMPEST/1-92 Level 1, NSTISSAM TEMPEST/1-93 and CNSSAM TEMPEST 01-02 (proper grounding and shielded twisted pair Ethernet cable (when using copper) are required.)
EMI	MIL-STD-461E for Army ground platforms (proper grounding and shielded twisted pair Ethernet cable (when using copper) are required.)
Vibration	• Operable in wheeled (XM1097 HHMMWV) vehicle. • Operable in tracked (XM1068) vehicle with external isolation system required.

Important Battery Removal Note

(U//FOUO) The battery may be changed while the device is powered on or while the device is powered off. It is recommended that the battery be changed while the device is powered on because when the device is NOT powered, there is a 30 second time limit to change the battery. In the unpowered situation, if the battery is not changed within 30 seconds, data will be lost. Therefore, it is important that the operator has the new battery ready before starting!

(U//FOUO) **It is very important that the new battery be placed in correctly for polarity. If the battery is inserted backwards, the device will be tampered if prime power is not present or removed.**

Failure Rate Summary Estimate

(U//FOUO) The Ground Benign prediction for the TACLANE-Micro is greater than 100,000 hours at 25°C ground benign environment.

3.4 (U) Mounting

TACLANE-Micro Rack Mount

(U//FOUO) From one to three TACLANE-Micros can be rack-mounted, side-by-side in a standard EIA 19 in. rack. In single or two unit mounting configuration, the mounting tray facilitates mounting of up to 2 TACLANE Micro power supplies.

Cooling

- (U//FOUO) TACLANE is passively cooled, i.e., there is no cooling fan. Placement or mounting must make sure that the TACLANE is operating within its temperature limits for minimum/maximum ambient temperature. The TACLANE-Micro should have clearance to permit air flow to facilitate conductive natural cooling or provide air flow to the heatsinks at the rear of the EIA mounting tray. The temperature at the root of the central heatsink area should not exceed 82°C.

(U//FOUO) For desk top usage, there is a mounting stand for holding the TACLANE-Micro on its side. This is included. (See "Handling and Environmental Conditions"). Use of the mounting stand is recommended, but not required.

(U//FOUO) Do not stack units because it will block airflow.

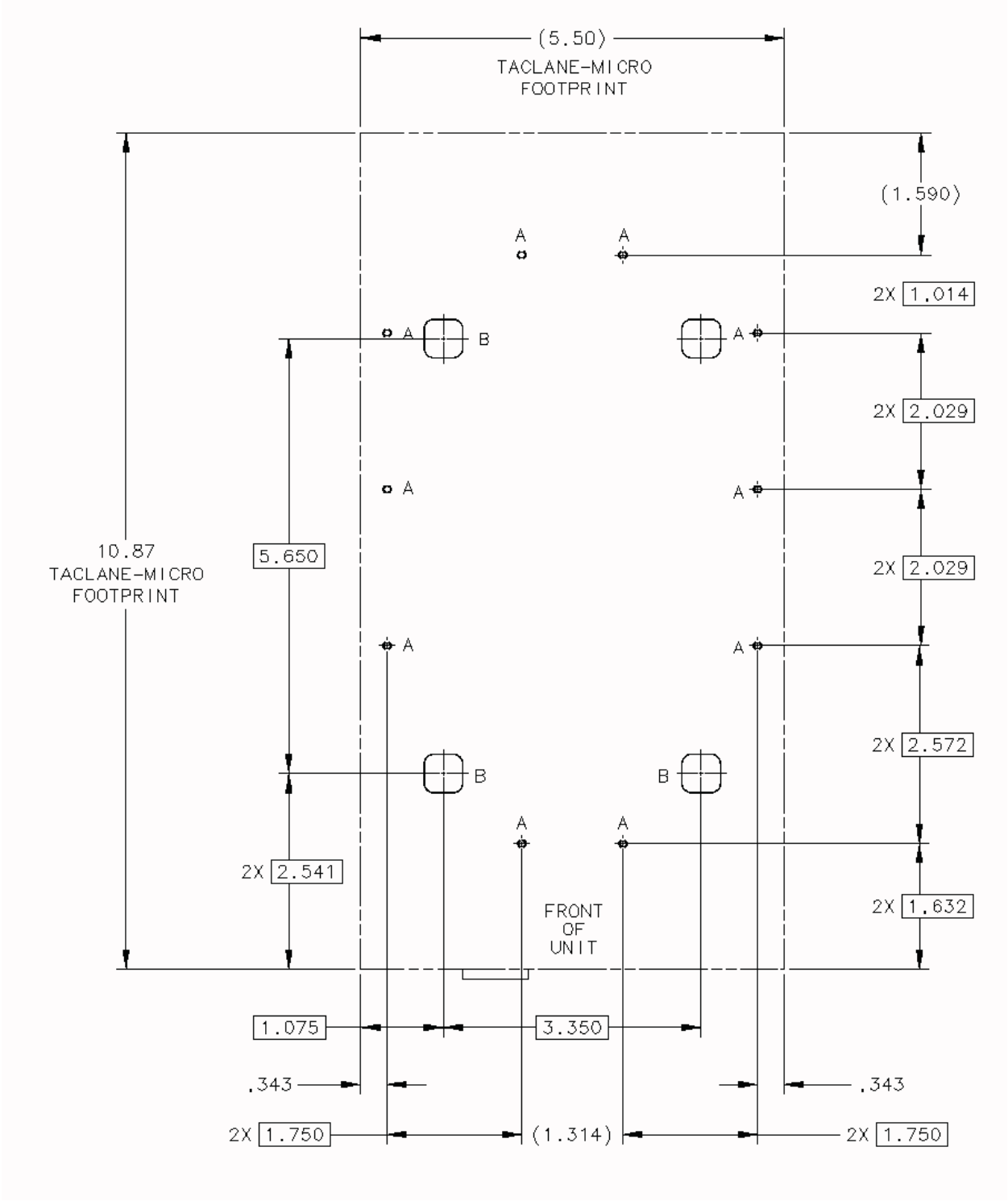
Cable Clearance

(U//FOUO) Make sure there is approximately a 4" clearance to the rear of the TACLANE so as not to excessively bend and damage the cables.

Rack Warning

(U//FOUO) When rack mounting, make sure that the rack is secure and not in danger of tipping over. Also, make sure that heavier equipment is mounted low on the rack to prevent a hazardous condition in which a rack could tip over.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure 3.4-1 (U) TACLANE-Micro Mounting Information

UNCLASSIFIED//FOUO

HOLE CHART			
HOLE CODE	COUNT	DESCRIPTION	NOTES
A	10	#4-40 UNC, .188 DEEP	1
B	4	.50-.53 SQ, R.12 MAX RADIUS CORNERS	2

NOTES:

1. EACH HOLE CODED "A" HAVE A STAINLESS STEEL HELICAL INSERT. GENERAL REQUIREMENT FOR HARDWARE SELECTION IS #4-40 UNC SCREW SUCH THAT THE REACH OF THE SCREW INTO THE HOLE DOES NOT EXCEED .157". THE THRU HOLE THROUGH THE PANEL IS SUGGESTED TO BE ø.140-.156

   REF: FOR GENERAL DYNAMICS TRAY PRODUCT (GENERAL DUTY), THE TRAY THICKNESS IS .093" MAX. 100° FLATHEAD SCREWS USABLE WITH THIS TRAY PRODUCT ARE MS24693-1 (3/16"L), MS24693-2 (1/4"L).

2. WHEN PUNCH METHOD IS USED FOR SUPPORTING SURFACE, THE HOLES CODED "B" MAY BE SHARP CORNER. THE FOUR SQUARE HOLE FEATURES ARE REQUIRED TO SEAT THE TACLANE-MICRO DEVICE.

3. FASTENING TACLANE-MICRO WITH DEVICE RESTING ON THE FOUR RAISED FEET, I.E. GAP BETWEEN MOUNTING SURFACE AND TACLANE-MICRO'S BOTTOM COVER IS NOT RECOMMENDED.

4. FOR TACTICAL ENVIRONMENT, PAN-HEAD SCREWS WITH LOCKING HARDWARE RECOMMENDED.

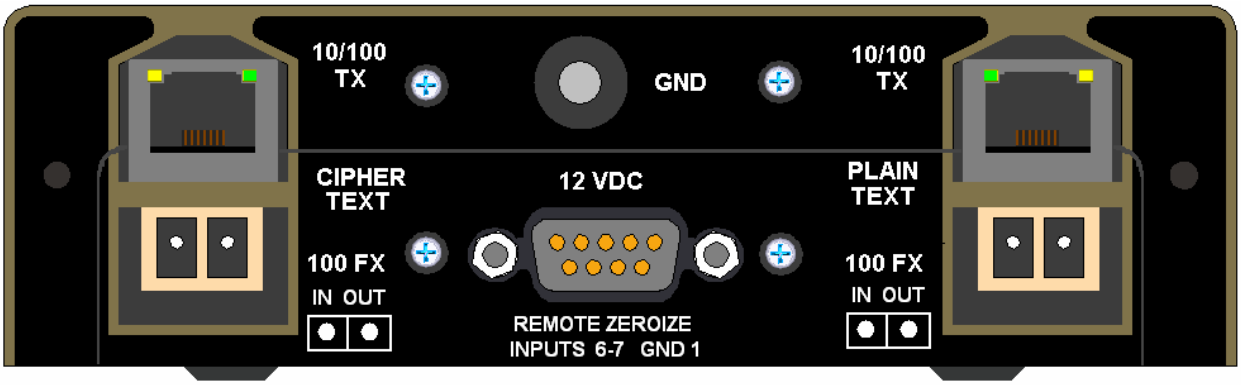
UNCLASSIFIED//FOUO

3.5 (U) Installing TACLANE Cables

Rear Panel

(U//FOUO) Refer to the diagram below when installing TACLANE cables.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure 3.5-1 (U) TACLANE-Micro (KG-175D) Rear Panel

Warning

(U//FOUO) A grounding stud is provided for additional grounding of the chassis.

- A short, low RF impedance ground strap is recommended when using the ground stud for chassis grounding. Grounding is required to ensure TEMPEST and EMI compliance.

Attaching the Ground Strap

(U//FOUO) The ground lug should have a 138 in. minimum ID to fit on the #6 ground binding post. (Example: MS25036-102 for #18 AWG ground wire.)

(U//FOUO) Follow these steps to install the TACLANE ground wire:

Step	Action
1.	Attach a ground wire to an earth ground.
2.	Loosen or remove the nut from the "GND" ground binding post on the TACLANE as needed.
3.	Attach the ground wire to the "GND" ground binding post on the TACLANE and tighten the nut.

Attaching the Power Supply Cable

(U//FOUO) Follow these steps to install the TACLANE power cable:

Step	Action
1.	Make sure that the TACLANE is powered off.
2.	Connect the power cable to the power connector on the TACLANE.
3.	Plug the power supply cable into a standard 110 VAC power outlet. Obtain an appropriate adapter for 220 VAC operation.

Attaching Fiber Cables

(U//FOUO) Follow these steps to attach the fiber cables. Note that General Dynamics cable assy 09-2802527-1 is equipped with rain and sand protection boot.

Step	Action
1.	Connect the fiber cable originating at the user PT port to the PT port on the TACLANE.
2.	Connect the fiber cable originating at the network CT port to the CT port on the TACLANE.

Attaching a Twisted Pair Copper Ethernet Cable

(U//FOUO) Follow these steps to attach a twisted pair copper Ethernet cable. Note that the IEEE recommended cable distance limit for Category 5 UTP, Category 5e UTP, and Category 6 UTP is 328 ft. (100 m.).

Step	Action
1.	Connect the Ethernet cable to the PT or CT RJ-45 jack on the TACLANE.

Ethernet Cable Installation for TEMPEST/EMI Compliance

(U//FOUO) TEMPEST and EMI compliance requires use of double shielded signal cables. The Plaintext (PT) and Ciphertext (CT) cables must be separated by a minimum of two (2) inches. For long cable lengths (greater than 10 feet), SFTP (foil and braid shield) is preferred and the PT cable shall be routed such that it is separated by a minimum of six inches from the AC power cable. In addition, it is required that a ground strap shall be connected between the binding post on the rear of the chassis labeled "GND" and earth ground. Optional cables 09-2792090-1 have been tested to comply with TEMPEST AND EMI requirements and equipped with rain and sand protection boot.

STP vs. UTP Ethernet Cable

(U//FOUO) TACLANE can be used with shielded twisted pair (STP) or unshielded twisted pair (UTP) Ethernet cable. However, STP Ethernet cable is required in order to meet EMI/TEMPEST specifications.

Straight vs. Crossover Ethernet Cable

(U//FOUO) Each TACLANE Ethernet interface auto-senses the Ethernet cable type, so crossover or straight through cables can be used interchangeably.

Fiber Interface Characteristics

(U//FOUO) The following characteristics apply to the TACLANE-Micro 100Base-FX fiber interfaces:

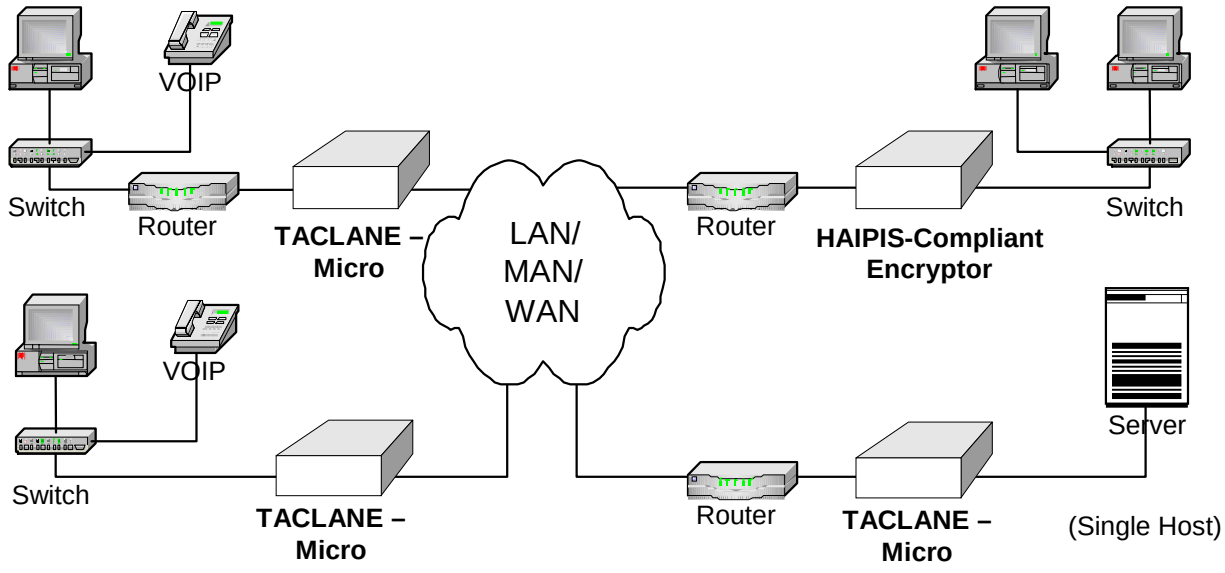
- 1300 nm short reach optics
- Duplex LC fiber connectors.

3.6 (U) Configuring the IP Network

Typical Secure IP Network

(U//FOUO) Figure 3.6-1 below depicts a typical IP network secured with TACLANE-Micros.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure 3.6-1 (U) TACLANE-Secured IP/Ethernet Network

Firewalls Must Pass IKE and ESP

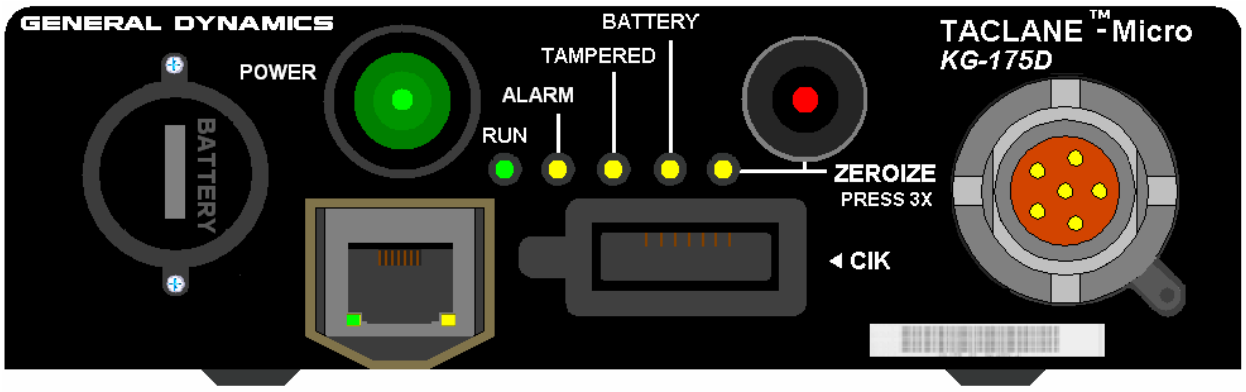
(U//FOUO) Any firewalls in the path between communicating TACLANEs must be configured to pass SDD, IKE, and ESP. See Appendix A ("Factory Default Settings") for the port numbers for these protocols.

3.7 (U) Operating the TACLANE

TACLANE Front Panels

(U//FOUO) The TACLANE-Micro contains the following Front Panel components:

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure 3.7-1 (U) TACLANE-Micro (KG-175D) Front Panel

Component	Description
CONSOLE Port	The HMI port is an RJ-45 Ethernet interface that connects to a PC, providing the HMI interface for the TACLANE- Micro. This interface also supports field software upgrades.
POWER Button	Power switch for the TACLANE.
ZEROIZE Button	Invokes zeroize function when ZEROIZE button is pressed three (3) times in less than 10 seconds, whether TACLANE is ON or OFF.

Component	Description
Status LEDs	• POWER (green): Illuminates when unit is powered on. • RUN (green): Illuminates continuously when in Offline state (not secure user traffic; management SA can operate). Flashes on/off once per second when in Secure Communications state (processing secure traffic). (Prime power must be applied and the device must be powered on.) • ALARM (yellow): Illuminates continuously when an alarm condition is detected in the INE. (Prime power must be applied and the device must be powered on.) • TAMPERED (yellow): Indicates if unit is tampered. (Prime power must be applied and the device must be powered on.) • BATTERY (yellow): Illuminates continuously when the battery power drops below the acceptable threshold. (Prime power must be applied and the device must be powered on.) • ZEROIZE (yellow): Illuminates continuously when unit is zeroized and powered on, illuminates for five seconds when unit is zeroized and powered off.
FILL Port	The DS-101 Fill port provides the ability to load key information using a Data Transfer Device (DTD) or Simple Key Loader (SKL).
CIK Port	DataKey Electronics Slimline SR4210 serial memory CIK port.
Battery	For the TACLANE-Micro, the battery is located on the front panel of the device. Battery power is provided by a 3.6 volt size AA lithium battery or a 1.5 volt size AA alkaline battery.

Important CIK Notes

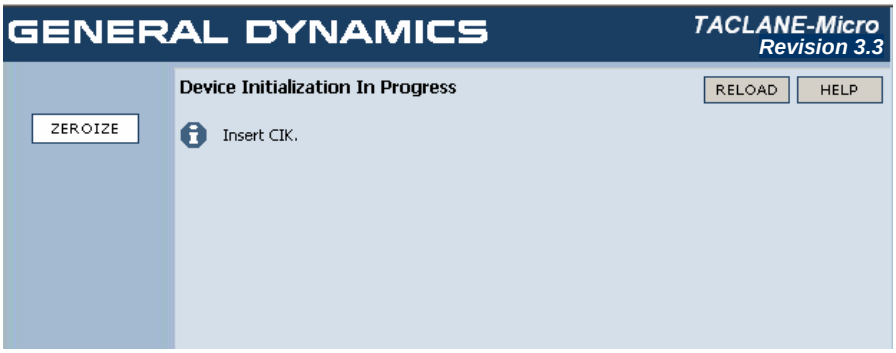
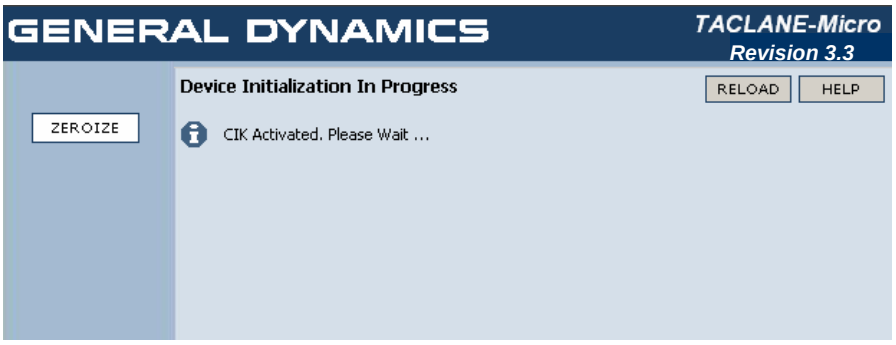
(U//FOUO) Use care when inserting and removing, especially the first few times a CIK is inserted and removed.

(U//FOUO) If a CIK is inserted, do not remove the CIK during TACLANE startup (or restart) to avoid write errors on the CIK.

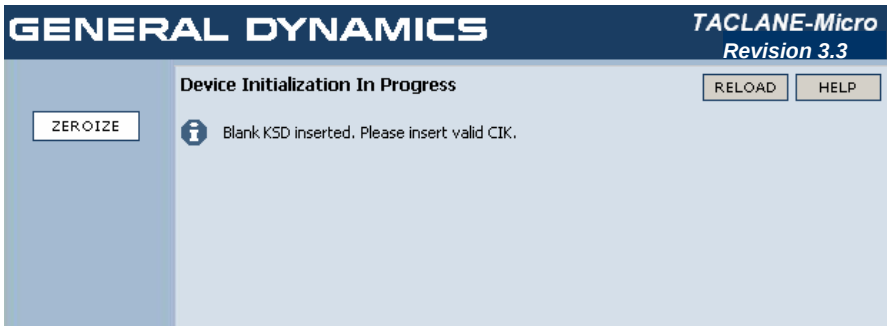
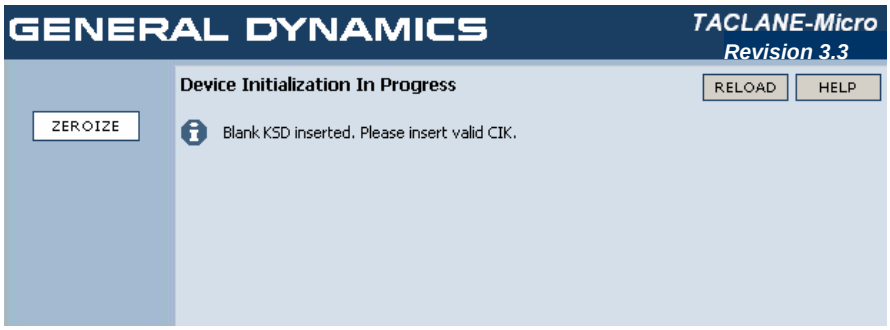
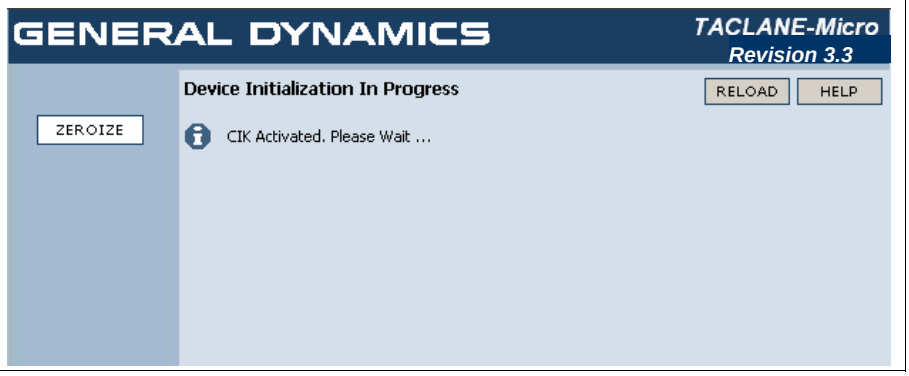
(U//FOUO) One CIK is provided when a TACLANE-Micro arrives from the factory. A Key Storage Device (a blank CIK) is also included with the TACLANE. General Dynamics recommends that the operator use this KSD to create a second CIK for the unit. One of the two CIKs should then be tagged and kept in a safe place while the other CIK is used for normal TACLANE operation.

Starting Up the TACLANE

(U//FOUO) Follow these steps to startup the TACLANE: *[Note: These steps assume that the operator PC has been configured, as described in section 2.4, with the web-browser application running with the address of the TACLANE-Micro Console port entered in the address window of the web-browser.]*

Step	Action
1.	Turn on the TACLANE. Note: It is recommended that the CIK be inserted before turning on the TACLANE-Micro. If it is not, when the CIK is required to continue the startup sequence will pause, prompt the operator to insert the CIK, and continue after the CIK has been inserted. (see step 2) Note: Do not remove the CIK during startup or restart. Doing so may invalidate the CIK because of a CIK write error. Note: Do not power down the TACLANE during the power-up sequence. Doing so may invalidate the CIK.
2.	CIK not inserted in the TACLANE, Result: The following screen is displayed: 
3.	CIK is detected during startup, Result: The following screen is displayed: 

Continued on next page

Step	Action
4.	Detected KSD is blank or KSD is not a valid CIK for this TACLANE-Micro. Result: The following screen is displayed: 
5.	TACLANE-Micro is unable to read or write to the detected KSD. Result: The following screen is displayed:  A valid CIK is detected and activated, Result: The following screen is displayed: 

Step	Action
6.	The Home page is displayed after successful startup:  Note: If a different screen is displayed, see "Other Startup Screens."

Other Startup Screens

(U//FOUO) The table below describes other startup screens that may appear.

Screen	Description
TACLANE zeroized	Alerts the operator that a panic zeroize previously occurred. After the operator presses OK to continue, the message does not appear again until the next panic zeroize occurs.
Tamper detected or Depot tamper recovery in progress	See the chapter on "Maintaining TACLANE."

Shutting Down the TACLANE

(U//FOUO) The TACLANE-Micro is shutdown by turning off the power. Please refer to the chapter on "Maintaining TACLANE."

Auto-recovery

(U//FOUO) If the TACLANE is turned off or prime power fails while processing user traffic, the TACLANE performs auto-recovery when power is restored, and automatically returns to the operational state it was in immediately preceding the shutdown:

- Security associations reestablish automatically without operator intervention.

Clock Drift

(U//FOUO) The TACLANE-Micro Real-Time-Clock is accurate to better than ±27.5 minutes per year under operating environmental conditions. TACLANE date and time should be checked for accuracy at least once every six months and adjusted if needed. See the chapter on "Maintaining TACLANE."

3.8 (U) HMI Menu Tree

HMI Menu Tree for TACLANE-Micro

(U//FOUO) Below is the TACLANE Menu Tree for the version 1.3.5 TACLANE-Micro. The Main Menu choices are centered and in bold. Lower level menu items appear left-justified below the Main Menu choices with increasing levels of indenture corresponding to lower levels in the Menu Tree. Menu items available only in a specific mode (or modes) are noted by letters in parentheses.

Operation	Maintenance	Key Management	Network	Security	System
Restart (I, O, S, R)	**Security Administration**	FIREFLY Vector Set (I, O, S, P)	Dynamic Discovery (I, O, S, P)	Access Mode (I, O, S, SSO)	Audit Log Threshold (I, O, S, P)
Security Level (I, O, S, SSO) (R if in sec level)	Enable SSO Privileges (I, O, S)	PrePlaced Key (I, O, S, P)	Ethernet Comm (I, O, S)	Access Control List (I, O, S, P)	Info (I, O, S)
Initialize (O, S, R)	Disable SSO Privileges (I, O, S, SSO)		**IP Comm**	CIK Management (I, O, S, P)	Network Managers (I, O, S, P)
Offline (I, S)	Generate SSO PIN (I, O, S, SSO)		IPv4 Addresses (I, O, S)	PPK Assignment (I, O, S, P)	
Secure Comm (O, L)	Battery (I, O, S)		MTU (I, O, S)	SA Configuration (I, O, S, P)	
SA Info	Date/Time (I, O, S, SSO, R)		PING Configuration (I, O, S)	**Static Routes**	
SA Table (O, S)	**Field Software Upgrade**			Route Management (I, O, S)	
	Servers (I, O, S, SSO)			Delete All Routes (I, O, S)	
	TFTP Settings (I, O, S, SSO)			**Traffic Flow Security**	**Legend**
	Upgrade Management (I, O, S, SSO)			Fixed Packet Length (I, O, S, P)	S – Secure Comm (Cryptography Active Mode)
	Logs			Bypass (I, O, S, P)	O – Offline Mode
	Event Log (I, O, S)			PSEQN Check (I, O, S, P)	I – Initialized Mode
	Audit Log (I, O, S)				L – In Security Level
	Delete Audit Log (I, O, S, SSO)				P – Contains Additional Functionality for SSO-Privileged Operator
					R – Restart Occurs
					SSO – SSO-Privileges Required to Access this Page.

4.0 (U) FILLING AND MANAGING KEYS

4.1 (U) Obtaining DTDs, SKLs, and Keys

DTD/SKL

(U//FOUO) The Data Transfer Device (DTD) (AN/CYZ-10(V3)) and the Simple Key Loader (SKL) can be used to fill TACLANEs with FIREFLY vector sets and PPKs. Operation of the SKL is similar to the DTD. This manual describes key fill operation using a DTD. Refer to the SKL manual for specific directions for the SKL operation.

Obtaining DTDs and SKLs Through Military Supply

(U//FOUO) Obtaining DTDs through military supply:

- Only available to DoD
- National Stock Number (NSN) 5810-01-393-1973.

(U//FOUO) Obtaining SKLs through military supply:

- Only available to DoD
- National Stock Number (NSN) 7010-01-517-3587.

Note: U.S. Army personnel must order the AN/CYZ-10(V3) (and AN/PVQ-10(C)) through the Army Item Manager only. Call DSN 879-8176 or commercial (520) 538-8176 for additional information.

Obtaining DTDs Through COMSEC Utility Program (CUP)

(U//FOUO) Obtaining DTDs through CUP:

- Available to DoD, civil agencies, and foreign allies
- POC: Rose Bechtold or Susan Carter, NSA
- POC Phone Number: (410) 854-6154.

Obtaining DTDs and SKLs from Manufacturer

(U//FOUO) Obtaining DTD from Sypris Electronics LLC (formerly GroupTech), Tampa, FL:

- Available to all, including contractors
- POC: Melissa Pruss
- POC Phone Number: (813) 972-6234.

(U//FOUO) Obtaining SKL from Sierra Nevada Corporation:

- Available to all, including contractors
- POC: Nicholas Balestrino
- POC Phone Number: (732) 427-4469.

Obtaining FIREFLY Vector Sets

(U//FOUO) Obtaining FIREFLY vector sets:

- Coordinate with Controlling Authority for closed partitions (if needed).
- Coordinate with COMSEC count(s) to order and receive FIREFLY vector sets (SDNS communications key) via EKMS and indicate:
  - Order is for TACLANE device
  - Open or closed partition
  - Key Type of operational
  - Key Application of test or operational
  - Classifications.

Obtaining PPKs

(U//FOUO) Obtaining PPKs:

- Coordinate with Controlling Authority for Short Title.
- Coordinate with COMSEC Account(s) to order and receive traditional keys via EKMS and indicate:
  - Order is for TACLANE/FASTLANE-type traditional keys
  - Classification of traditional keys/cryptonet
  - Whether traditional keys are test or operational
  - Number of editions (crypto-period is one month)
  - In place and implementation date
  - Regular re-supply or as-needed
  - Short Title if reordering.

4.2 (U) Attaching a Fill Cable

Introduction

(U//FOUO) A DTD, connected using a fill cable, is used to fill the TACLANE with a FIREFLY vector set and/or PPKs. See the DTD User's Manual for more information on DTD operation.

Note

(U//FOUO) The fill cable is only needed when filling a key. The same procedure applies whether attaching the fill cable to the TACLANE or the DTD – the cable connectors at each end are the same.

Procedure (U//FOUO) Follow these steps to attach the fill cable:

Step	Action
1.	Line up the fill cable connector with the fill port on the TACLANE front panel so that the flat side of the connector is on top and centered on the red dot on the top of the fill port.
2.	Apply firm pressure to the cable connector, then slightly rotate the cable connector clockwise until it stops. Note: If the cable connector is difficult to attach, apply a small amount of silicone lubricant to the rubber O-ring inside the cable connector.
3.	Remove pressure so the cable can set into locked position. Result: The fill cable is locked onto the fill port.

Procedure (U//FOUO) Follow these steps to remove the fill cable:

Step	Action
1.	Apply firm pressure to the cable connector, then slightly rotate the cable connector counter-clockwise until the flat side of the connector is on top.
2.	Pull to remove the fill cable connector. Result: The fill cable is released from the fill port.

4.3 (U) Filling the FIREFLY Vector Set

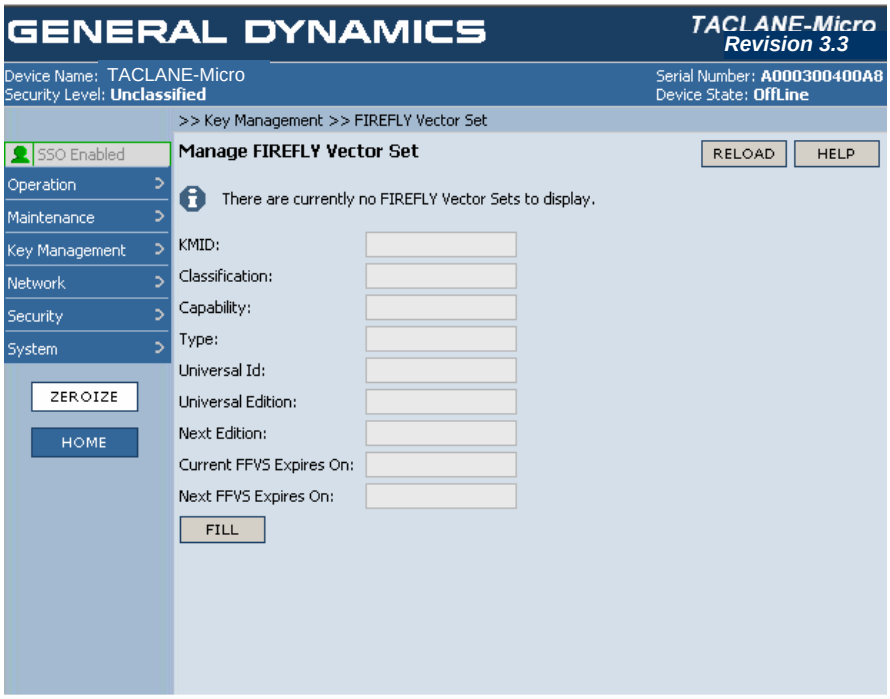
Introduction (U//FOUO) The SSO operator can fill TACLANE, using a DTD, with one operational (current or current and next) FIREFLY vector set. The FIREFLY vector set allows pairwise FIREFLY TEKs to be dynamically set up between an initiator and responder TACLANE.

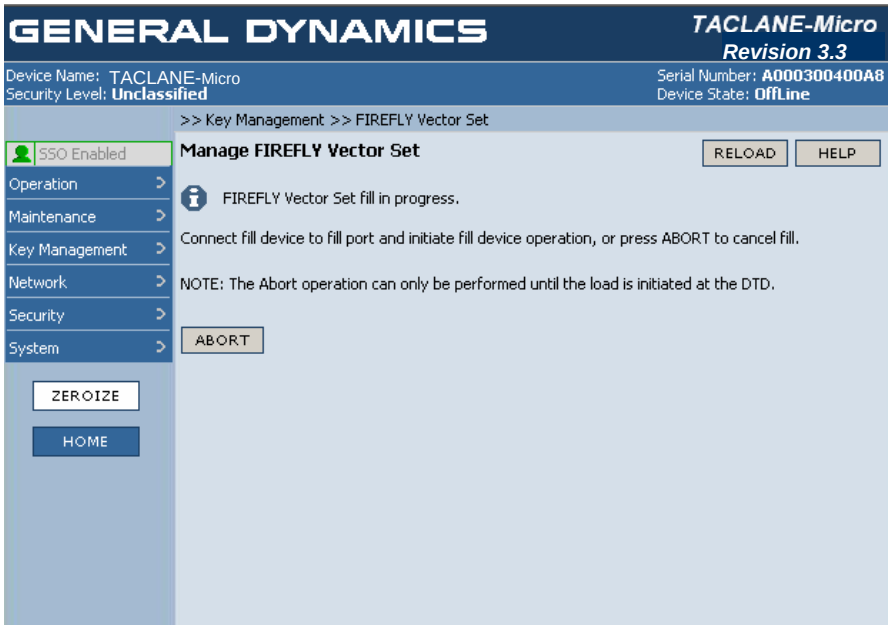
Enhanced FIREFLY and Basic FIREFLY (U//FOUO) The TACLANE supports both the Enhanced FIREFLY (EFF) as well as the Basic FIREFLY.

Notes (U//FOUO) The following notes apply to filling the FIREFLY vector set:

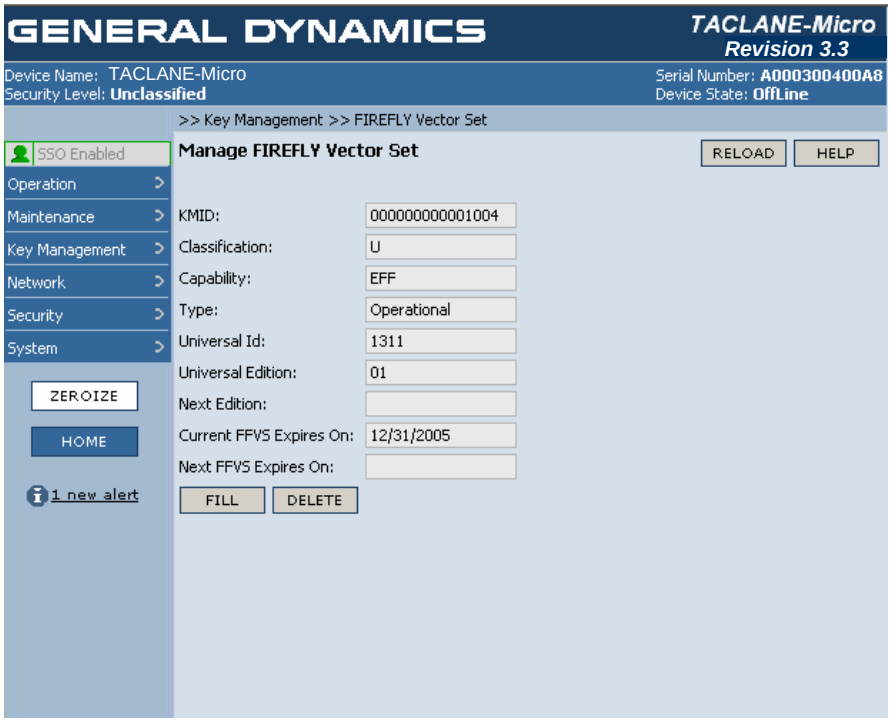
- Only the SSO can fill a FIREFLY vector set.
- The operator must delete any existing FIREFLY vector set before filling a new FIREFLY vector set (See Section 4. 7, "Deleting the FIREFLY Vector Set") or must allow a new FIREFLY vector set to supersede an existing FIREFLY vector set.

Procedure (U//FOUO) Follow these steps to fill the FIREFLY vector set:

Step	Action
1.	From the MAIN MENU, select Key Management => FIREFLY Vector Set. Result: The following screen is displayed:  Note: If there is an existing FFVS, the current values are displayed on the screen.

2.	Select FILL to begin fill. Result: The following screen is displayed:  Note: If the fill is not completed within 5 minutes, the fill operation is aborted. Note: ABORT cancels a fill operation in progress if the abort is issued before the DTD indicates start-of-fill. Otherwise, the ABORT is ignored.

Procedure (continued)

Step	Action
3.	Using a fill cable, connect a DTD to the TACLANE fill port.
4.	Configure the DTD to transmit the operational FIREFLY vector set. Note: The DTD must be configured to "fill" the FIREFLY vector set rather than "issue" it.
5.	Transmit the operational FIREFLY vector set from the DTD. Result: The following screen appears if the fill operation was successful:  Note: Specific values depend on the particular FIREFLY vector set. Note: If the fill operation was unsuccessful due to a PrePlaced Key being loaded instead of a FFVS, an FFVS Fill Failed entry is placed in the audit log with reason = Invalid Key Material.
6.	Disconnect the fill cable from the TACLANE fill port.

4.4 (U) Deleting the FIREFLY Vector Set

Introduction

(U//FOUO) The SSO operator can delete the operational FIREFLY vector set.

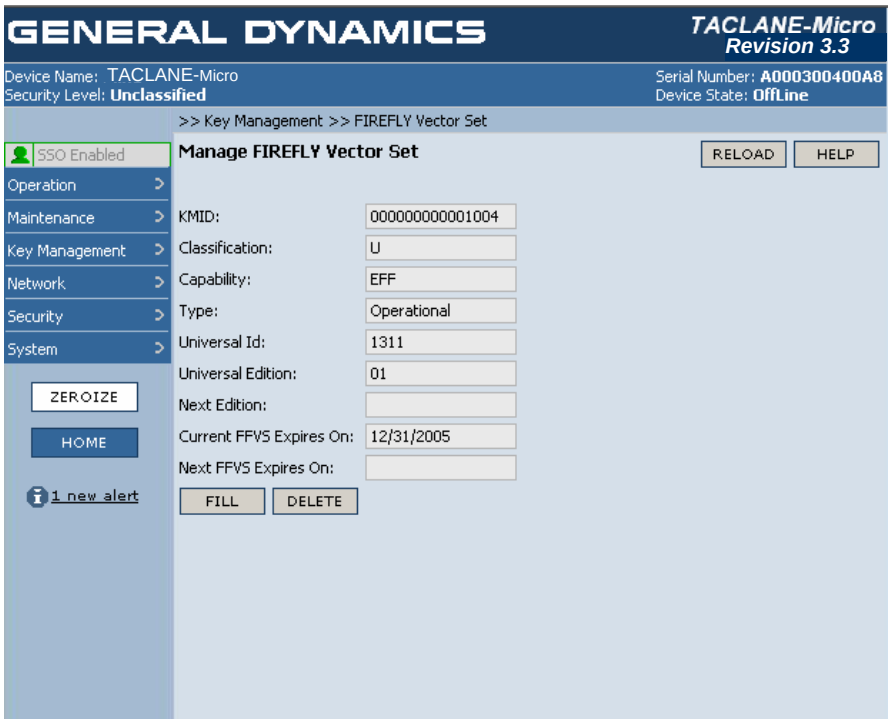
Note

(U//FOUO) The following notes apply to deleting the FIREFLY vector set:

- Only the SSO can delete a FIREFLY vector set.

Procedure

(U//FOUO) Follow these steps to delete the FIREFLY vector set:

Step	Action
1.	From the MAIN MENU, select Key Management => FIREFLY Vector Set. Result: The following screen is displayed: 
2.	Select DELETE to delete the FIREFLY vector set.

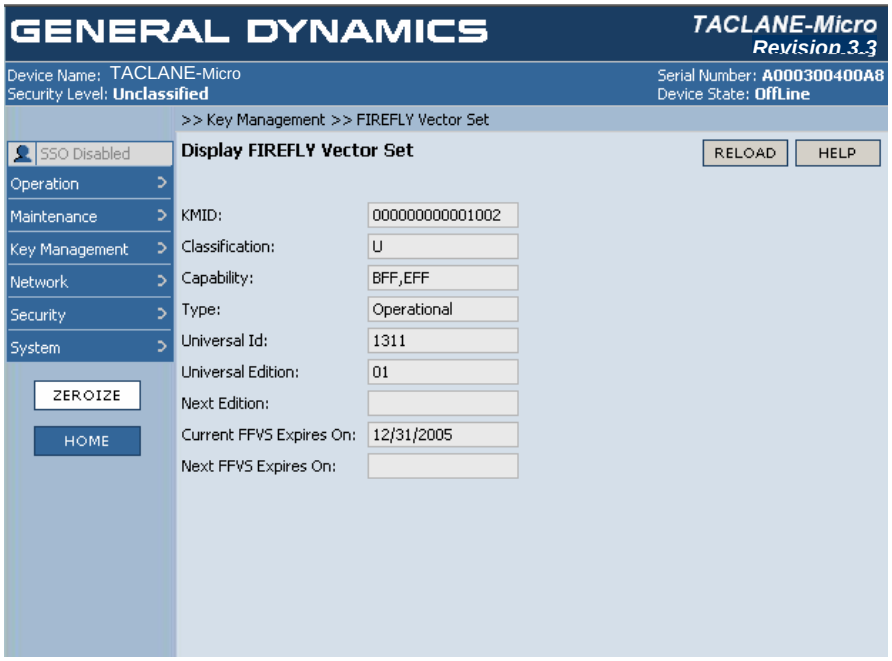
4.5 (U) Displaying the FIREFLY Vector Set Information

Introduction

(U//FOUO) The operator can display the information associated with the operational FIREFLY vector set.

Procedure

(U//FOUO) Follow these steps to display the FIREFLY vector set information:

Step	Action
1.	From the MAIN MENU, select Key Management => FIREFLY Vector Set. Result: The following screen is displayed:  Note: The current FFVS is displayed. Note: Specific values depend on the particular FIREFLY vector set.

4.6 (U) Filling a PrePlaced Key

Introduction

(U//FOUO) The SSO operator can fill a TACLANE, using a DTD, with up to 16 active PPKs or PPK Chains. PPKs are used to create security associations between an initiator and responder TACLANE.

Notes

(U//FOUO) The following notes apply to filling PPKs:

- Only the SSO can fill a PPK.
- A total of 16 PPK chains may be filled in a TACLANE. A PPK chain consists of the one active PPK and up to 11 changeover PPKs. During normal operation each PPK has a 1-month crypto-period, the 11 changeover PPKs allow an operator to only have to fill the PPKs once per year.
- Each PPK chain is assigned to a PPK ID or slot number. The PPK IDs (slot numbers) range from 1 – 16, and are available at any security level. All 16 PPK chains may be filled at one security level or several PPK chains may be filled at different security levels (up to a total of 16 PPK chains). As an example, one PPK chain may be filled under PPK ID 01 at the UNCLASSIFIED level, and another PPK chain may be filled under PPK ID 02 at the SECRET level.
- There are two uses of PPKs: User PPKs and Secure Dynamic Discovery (SDD) PPKs. The User PPKs secure user traffic while the SDD PPKs are used to encrypt the SDD messages.
- When filling a PPK, the operator is prompted to enter the Effective Date of the PPK, the Use of PPK (User vs. SDD), and the cryptography Algorithm (BATON or MEDLEY).
- When the operator fills a PPK into a slot that already contains an active PPK (i.e., it is not an empty slot), then this filled PPK is saved as a changeover PPK. In this case, the use and algorithm are not prompted for in filling the changeover PPK since these parameters are inherited from the slot's active PPK.
- Note that for proper operation within a cryptonet using PPKs, all TACLANEs in the cryptonet must have the PPK configured with the same effective date, use, and algorithm.

PPK Format Supported

(U//FOUO) The TACLANE-Micro supports the DS-100-1 PPK format.

Continued on next page

PPK Changeover

(U//FOUO) TACLANE PPK changeover (occurs on the same day every month as defined by the effective date) is centered around 12:00 AM with a plus or minus 55 minute window (to allow for clock drift) that starts at 11:05 PM and ends at 12:56 AM.

(U//FOUO) For a security association, a TACLANE starts using the changeover PPK to encrypt user traffic at 12:00 AM. A TACLANE is able to decrypt user traffic using either the current or changeover PPK within the window (11:05 PM – 12:56 AM). At the end of the window, the current PPK is deleted.

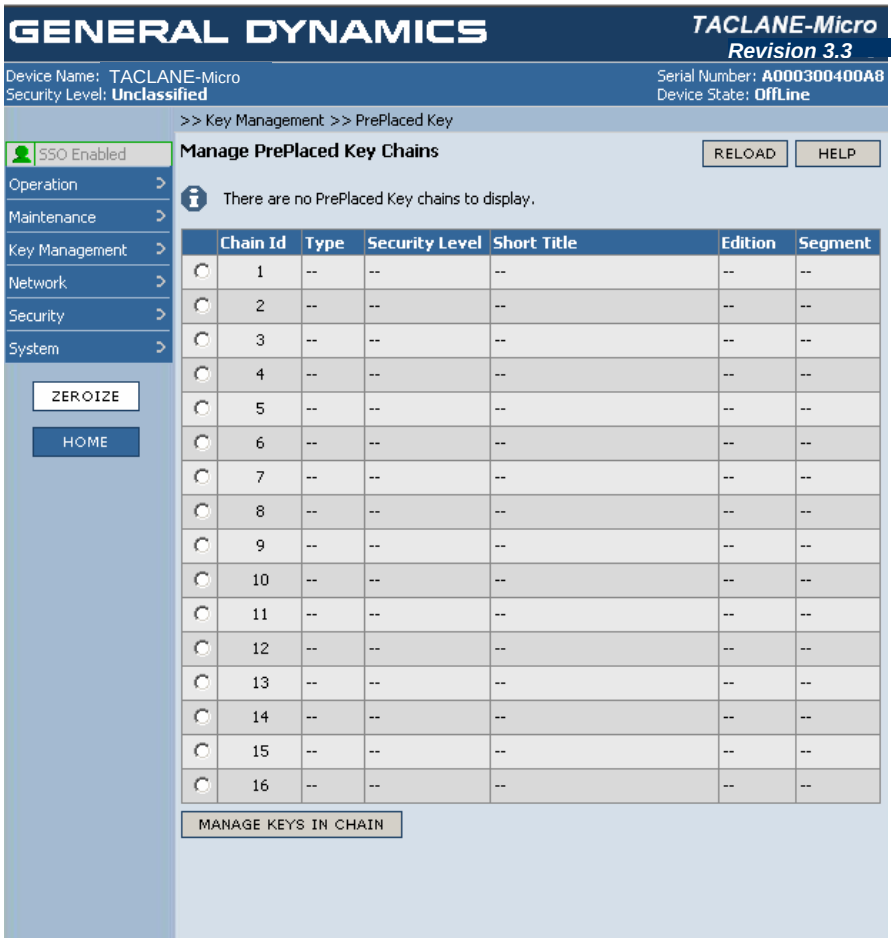
PPK Update

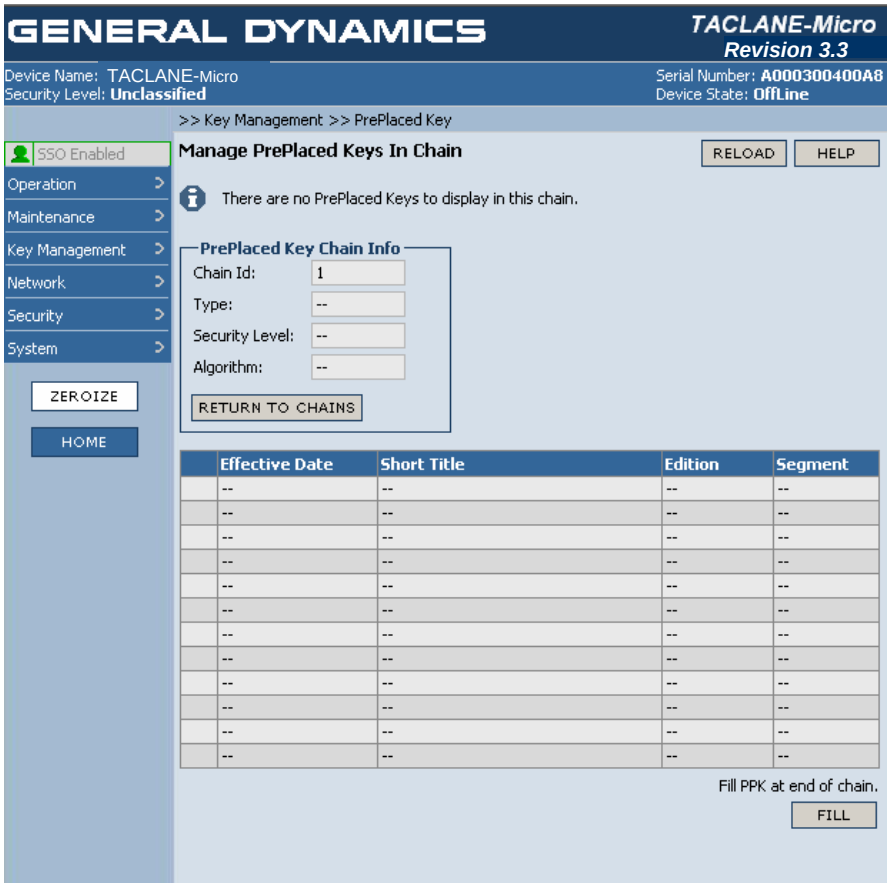
(U//FOUO) TACLANE PPK update (performed each day) is centered around 2:00 AM with a plus or minus 55 minute window (to allow for clock drift) that starts at 1:05 AM and ends at 2:56 AM:

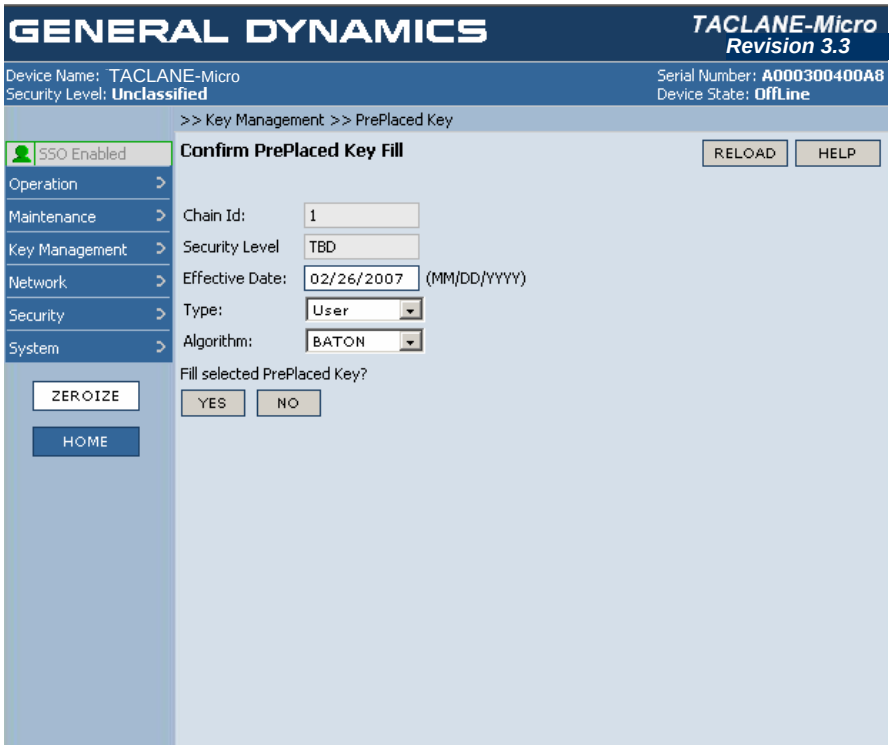
- For a security association, a TACLANE starts using the updated PPK to encrypt user traffic at 2:00 AM. A TACLANE is able to decrypt user traffic using either the pre-update or post-update PPK within the window (1:05 AM – 2:56 AM). At the end of the window, the pre-update PPK is deleted.

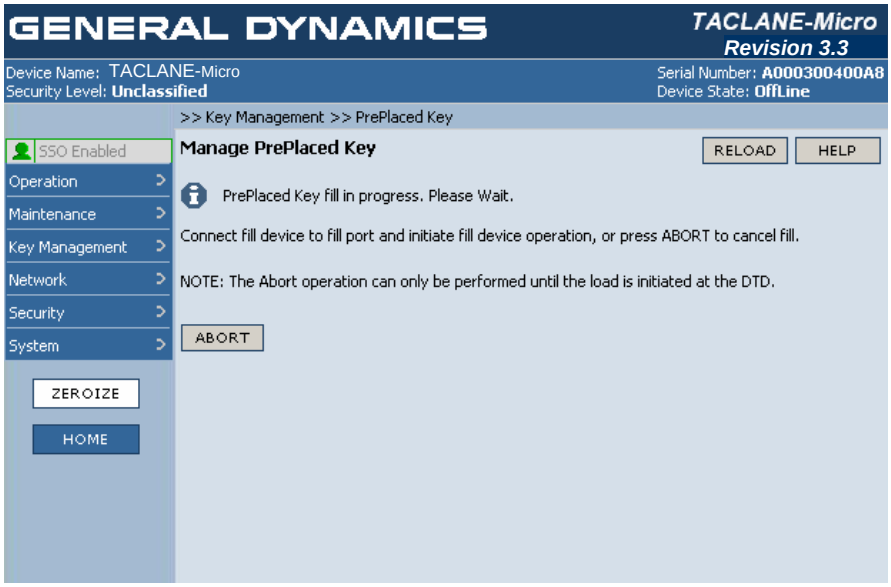
Procedure (U//FOUO) Follow these steps to fill a PPK:

Step	Action
1.	From the MAIN MENU, select Key Management => PrePlaced Key. Result: The following screen is displayed:



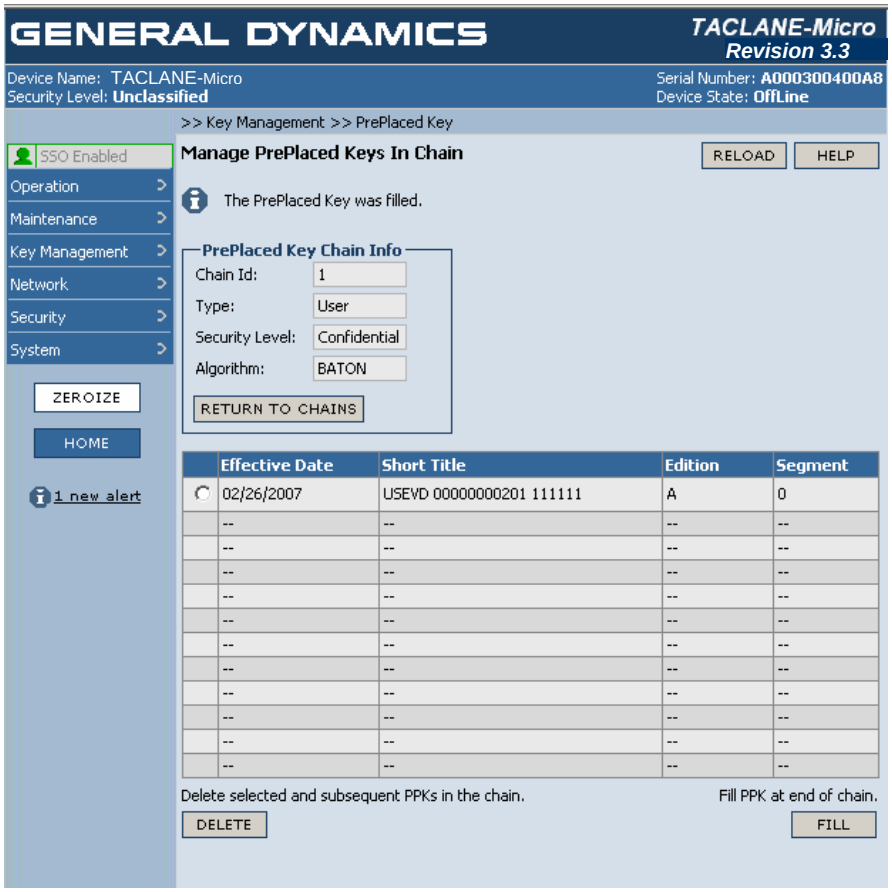
2.	Select the radio button next to an active or empty PPK Chain Id to which the new PPK will be associated and MANAGE KEYS IN CHAIN. Result: The following screen is displayed:  **Note: Selecting a PPK Chain Id is necessary to access Key Processing Commands to Manage the Keys associated with a chain.**

3.	Select FILL to continue the fill operation. Result: The following screen is displayed:  Note: If the PPK ID is empty (slot does not have a Current PPK assigned) additional data entry boxes are displayed for Effective Date, Use and Algorithm. If it is an active PPK ID (Current PPK is already assigned), the security Level, Use and Algorithm are displayed with the configuration values of the active PPK ID.

4.	Enter the Effective Date, Type, and Algorithm if this is the first key in slot. Select YES to fill the PrePlaced key. Result: The following screen is displayed:  Note: If the fill is not completed within 5 minutes, the fill operation is aborted. Note: ABORT cancels a fill operation in progress if the abort is issued before the DTD indicates start-of-fill. Otherwise, the ABORT is ignored.

Continued on next page

Procedure

Step	Action
5.	Using a fill cable, connect a DTD to the TACLANE fill port.
6.	Configure the DTD to transmit the PPK. Note: The DTD must be configured to "fill" the PPK rather than "issue" it.
7.	Transmit the PPK from the DTD. Result: The following screen appears if the fill operation was successful:  Note: Specific values depend on the particular PPK. Note: If the fill operation was unsuccessful due to a FIREFLY Vector Set being loaded instead of a PPK, a PPK Fill Failed entry is placed in the audit log with reason = DS-101 Parity Error.
8.	Disconnect the fill cable from the TACLANE fill port.

4.7 (U) Displaying PrePlaced Key Information

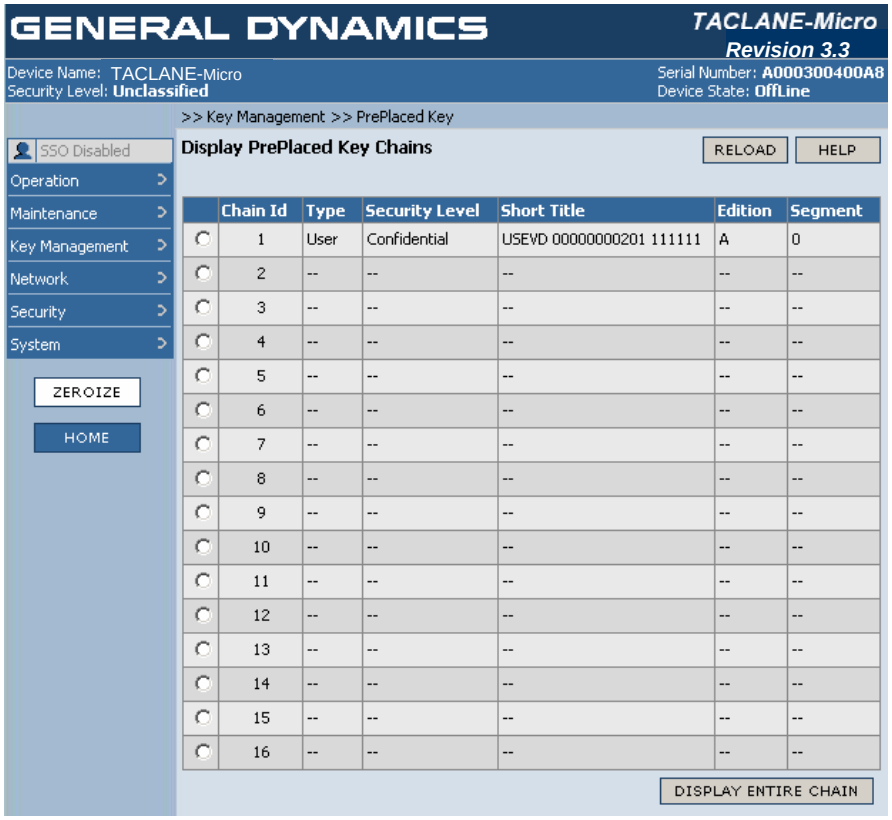
Introduction

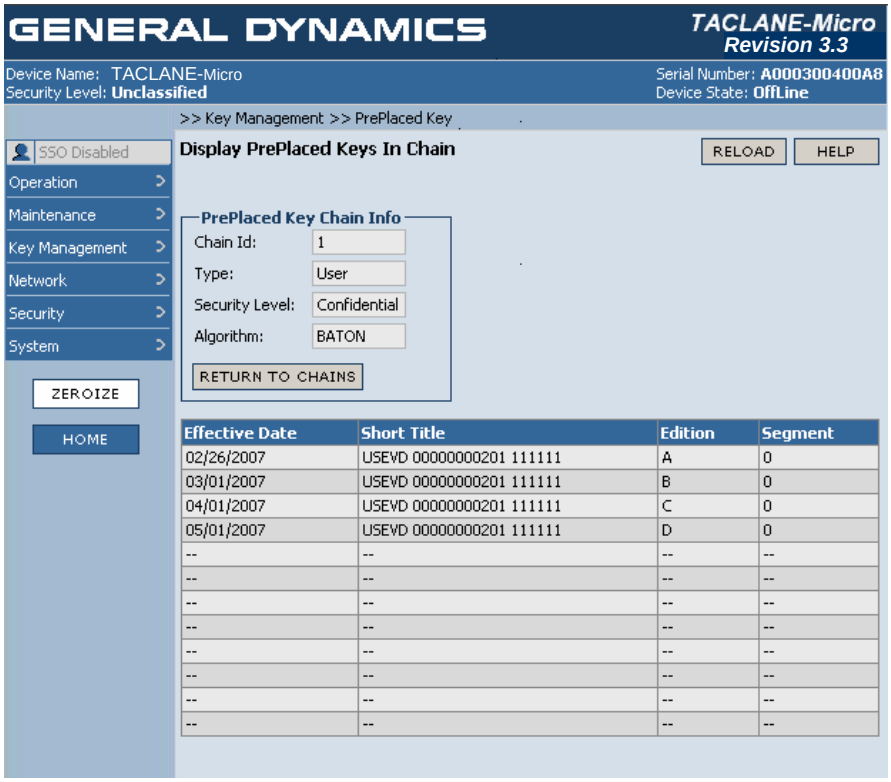
(U//FOUO) The operator can display the information associated with a PrePlaced Key (PPK).

Procedure

(U//FOUO) Follow these steps to display PPK information:

Step	Action
1.	From the MAIN MENU, select Key Management => PrePlaced Key. Result: The following screen is displayed:



2.	Select the radio button next to the PPK Chain Id and DISPLAY ENTIRE CHAIN to display a list of all the PPKs in a particular chain. Result: The following screen is displayed:  Note: Specific values depend on the particular PPK.

4.8 (U) Deleting a PrePlaced Key

Introduction

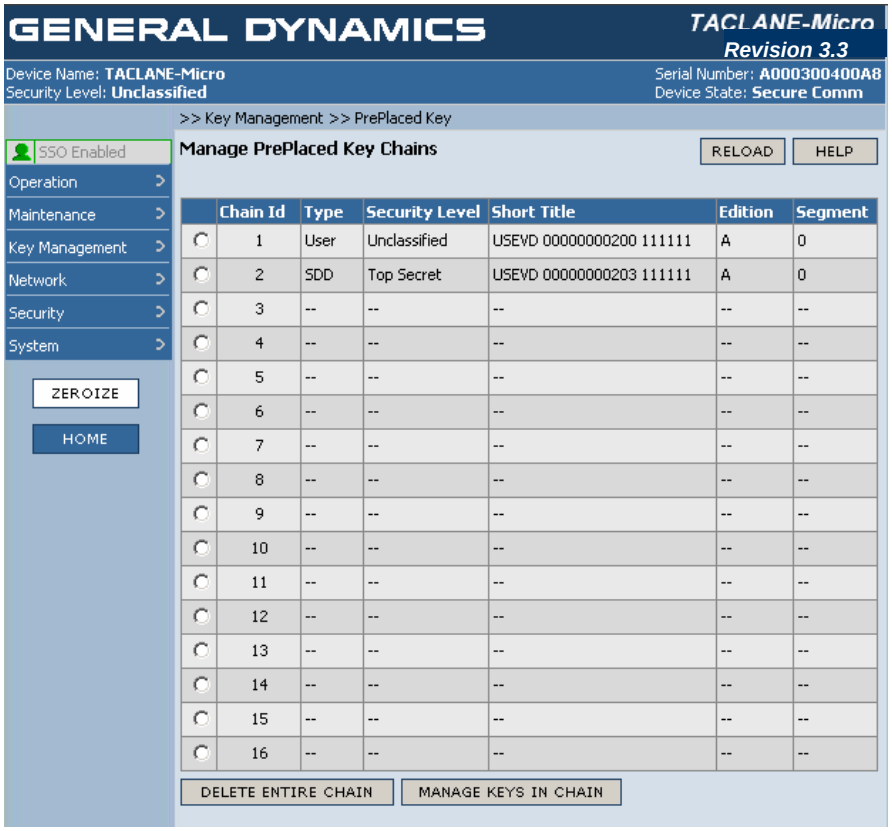
(U//FOUO) The SSO operator can delete a PrePlaced Key (PPK).

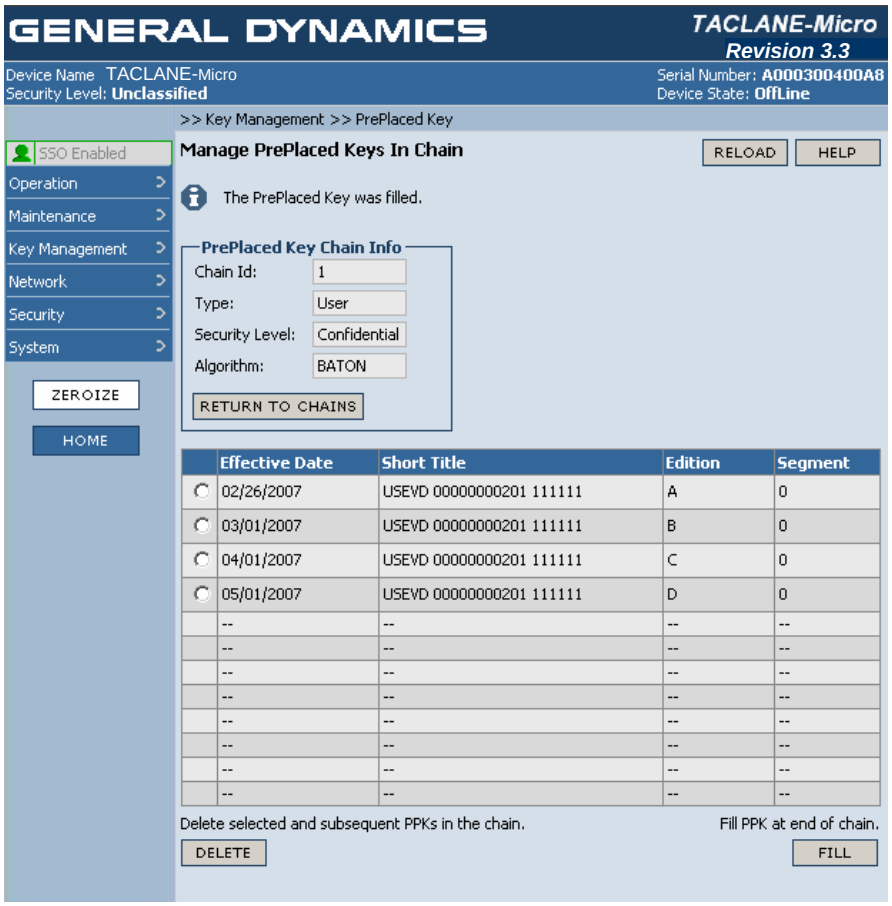
Note

(U//FOUO) The following notes apply to deleting a PPK:

- Only the SSO can delete a PPK
- Deleting a PPK deletes that PPK and all PPKs following it in the chain along with associated assignments.

Procedure (U//FOUO) Follow these steps to delete a PPK:

Step	Action
1.	From the MAIN MENU, select Key Management => PrePlaced Key. Result: The following screen is displayed: 
2.	To delete a PrePlaced Key chain, select the radio button next to the Chain Id and DELETE ENTIRE CHAIN.

3.	To delete specific changeover PPKs, select the radio button next to the Chain Id and MANAGE KEYS IN CHAIN. This displays a list of all the PPKs in a particular chain. Result: The following screen is displayed: 
4.	Select the radio button next to the PPK and DELETE to delete a PPK and all PPKs that follow it in the chain (or select RETURN TO CHAINS to return to the previous screen).

4.9 (U) Selecting a Security Level

Introduction

(U//FOUO) The SSO operator must select a security level for the TACLANE to fully operate. Certain menu choices, such as selecting secure communications mode, are only available when a security level is selected.

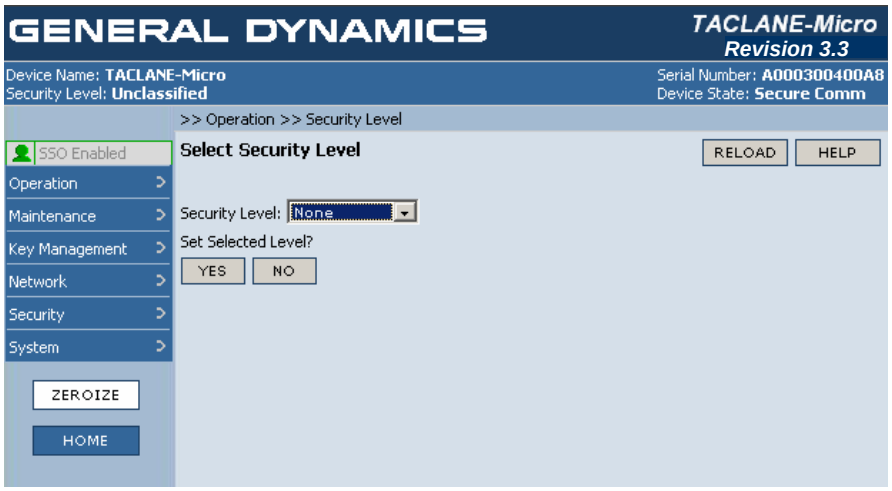
Notes

(U//FOUO) The following notes apply to selecting a security level:

- Only the SSO can access this command.
- The FIREFLY vector set may only be used to generate FIREFLY TEKs if the selected security level matches one of the classification levels supported by the FIREFLY vector set.
- PPKs may only be used at the security level matching the PPK classification.

Procedure

(U//FOUO) Follow these steps to select a security level:

Step	Action
1.	From the MAIN MENU, select Operation => Security Level. Result: The following screen is displayed: 
2.	Select the desired security level from the pull-down list.
3.	Select YES to set the selected security level.
4.	Select OK to confirm the action and restart the TACLANE (if currently in a security level).

4.10 (U) Exiting a Security Level

Introduction

(U//FOUO) The SSO operator can exit the current security level, returning to "no security level." Certain menu choices are only available when the TACLANE is not in a security level.

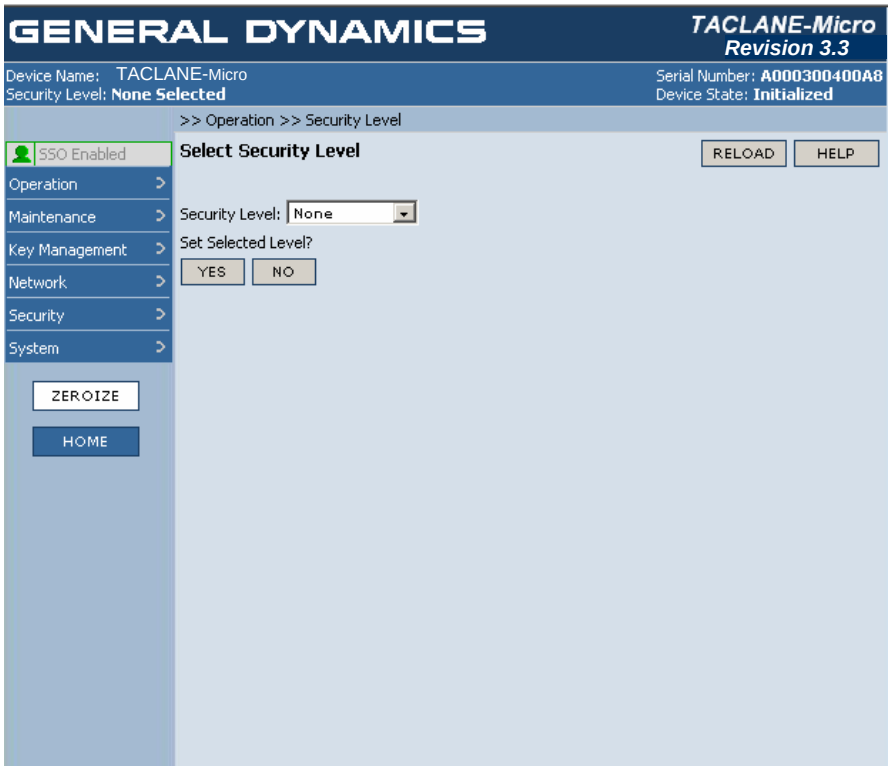
Note

(U//FOUO) The following notes apply to exiting a security level:

- Only the SSO can access this command.

Procedure

(U//FOUO) Follow these steps to exit a security level:

Step	Action
1.	From the MAIN MENU, select Operation => Security Level. Result: The following screen is displayed: 
2.	Select None from the pull-down list.
3.	Select YES to exit the current security level.
4.	Select OK to confirm the action, which will restart the TACLANE. Note: This confirmation is displayed to alert the operator that existing communications include communication with a Network Manager will be lost if this change is made.

5.0 (U) CONFIGURING IP/ETHERNET

5.1 (U) Configuring the Ethernet Media and Physical Parameters

Introduction

(U//FOUO) The TACLANE's PT and CT physical interface parameters are configurable by the operator. Specifically, the Ethernet interface speed, duplex mode, and media can all be configured to accommodate the characteristics of the networks to which a TACLANE is connected.

(U//FOUO) The TACLANE supports both an auto-negotiation interface as well as manual configuration settings (i.e., speed/duplex combinations). The auto-negotiation option automatically chooses the highest bandwidth that is compatible with the devices (link partners) on the respective network interface.

Supported TACLANE-Micro Physical Settings

(U//FOUO) The TACLANE-Micro supports the following user-configurable Ethernet physical settings.

copper interfaces:

- Auto-Negotiate
- 100/F
- 100/H
- 10/F
- 10/H

fiber interfaces:

- 100/F

(U//FOUO) The default medium for both the PT and CT interfaces is: copper.

(U//FOUO) The default setting for a TACLANE-Micro copper interface is: Auto-Negotiate.

(U//FOUO) The default, and only possible, setting for a TACLANE-Micro with a fiber interface is: 100/F.

Continued on next page

Auto-Negotiate Notes

(U//FOUO) The following notes apply when the Ethernet physical parameter is set to Auto-Negotiate:

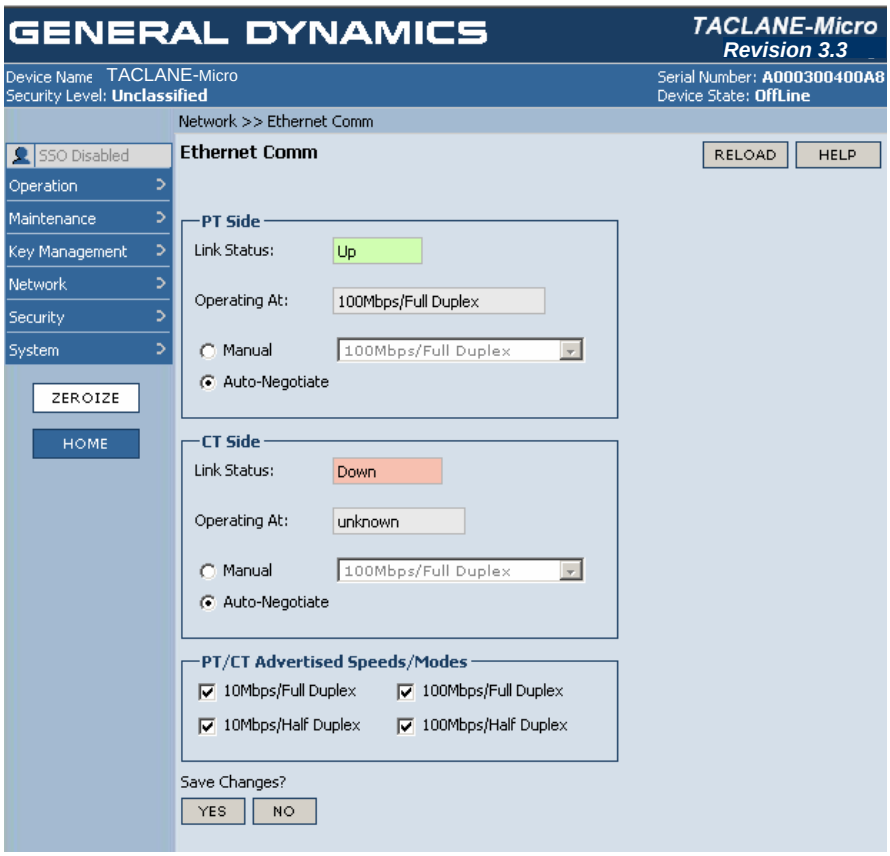
- If the physical parameter is set to Auto-Negotiate, a two-stage negotiation process is carried out. First, each interface auto-negotiates with its link partner, offering all the advertised bandwidths. Then, the Micro selects the highest bandwidth that is within the capabilities of both link partners, and auto-negotiates with both devices again, offering only the selected bandwidth.
- Auto-negotiation should take between 2 – 6 seconds, depending on the network speed capabilities
- If the auto-negotiation fails, the TACLANE will continue to try auto-negotiation until a response is received.
- The TACLANE's network interface will automatically re-negotiate (assuming it was configured to auto-negotiate) when it detects network changes (e.g., link, speed, duplex, clocking).
- If the negotiation fails because a link partner is set to a constant bandwidth or does not support auto-negotiation, then the speed is sensed using Parallel Detection . Since Parallel Detection does not determine full or half duplex, the interface will automatically use half duplex. (This is the correct behavior according to the standard, although it sometimes produces unsatisfactory results, since Parallel Detection cannot sense the remote device's duplex setting.) Parallel detection is only used for 10/100BASE-T equipment.

Other Notes

(U//FOUO) The following additional notes apply to configuring the Ethernet physical parameters:

- The PT and CT physical interface settings are independent. For example, it's possible to have a Micro configured with its CT interface at 100/F and its PT interface set to Auto-Negotiate.
- A manual interface speed setting should be used if the TACLANE interfaces with network equipment that doesn't support auto-negotiation.
- If the Ethernet Configuration is changed from Fiber and Copper or vice-versa in the Off-Line or Secure Comms state, then there will be a period, up to about 5 seconds, where all packets will be dropped.

Procedure (U//FOUO) Follow these steps to configure the Ethernet physical parameters:

Step	Action
1.	From the MAIN MENU, select Network => Ethernet Comm. Result: The following screen is displayed: 
2.	For both of the PT and CT sides, the current link status, speed and mode that the interfaces are operating at is displayed.
3.	For the PT side, select the radio button next to manual and select the speed and mode from the pull down menu or select the radio button next to auto-negotiate.
4.	For the CT side, select the radio button next to manual and select the speed and mode from the pull down menu or select the radio button next to auto-negotiate.
5.	Select the desired PT/CT advertised speed/mode by selecting the checkboxes next to the appropriate choices.
6.	Select YES to save the changes.

5.2 (U) Entering/Modifying the TACLANE IP Addresses

Introduction

(U//FOUO) TACLANE requires an IP address for IP communication with the PT side of the TACLANE and a CT IP Address for IP communication with the CT side of the TACLANE. TACLANE supports a PT default gateway for routing packets exiting the PT interface that are not on the local PT network (also known as off-network). Likewise, TACLANE supports a CT default gateway for routing packets exiting the CT interface that are not on the local CT network.

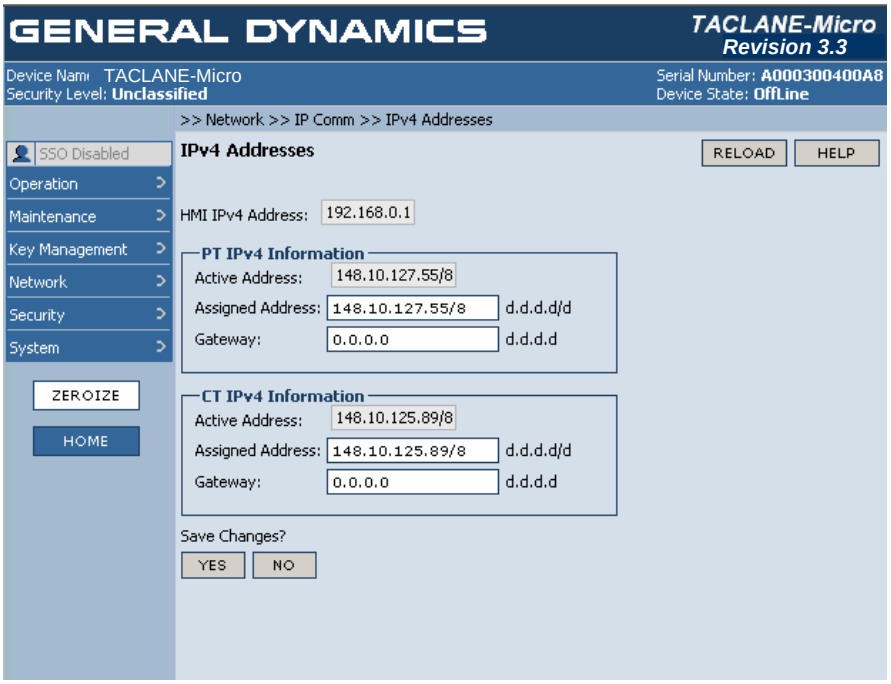
Notes

(U//FOUO) The following notes apply to entering/modifying the TACLANE IP addresses:

- The CT and PT IP addresses must include the prefix length.
- The Active Address values displayed are the current values used on the interfaces. The Assigned Address values will take effect after the next restart.
- The Gateway address becomes active upon saving changes to IP addresses – without a need to restart.
- The Gateway address must be consistent with the corresponding Active Address (e.g., PT Gateway must be consistent with the PT Active Address)
- The TACLANE can be configured with its CT and PT IP addresses in the same or in different subnets.
- The CT and PT IP addresses must be unique such that no host or remote device (e.g., another TACLANE) uses these IP addresses.

Procedure

(U//FOUO) Follow these steps to enter or modify the TACLANE IP addresses:

Step	Action
1.	From the MAIN MENU, select Network => IP Comm => IPv4 Addresses. Result: The following screen is displayed:  **Note**: The HMI IPv4 Address is for display only.
2.	Type in the desired IP addresses. For the PT and CT IP Addresses, include a "/" followed by the prefix length. Note: All IP addresses must be unique. Note: The CT and PT IP addresses may be in the same or in separate networks (or subnetworks).
3.	Select YES to save changes.

5.3 (U) Modifying the TACLANE MTU Size

Introduction

(U//FOUO) The operator may modify the TACLANE Maximum Transfer Unit (MTU) size. The MTU size is the length, in bytes, of the largest IP datagram the TACLANE sends without fragmenting the IP datagram.

MTU and FPL

(U//FOUO) For optimum performance when FPL is enabled, PT-side hosts and routers may require modifications to their MTU settings. See section B.3 of Appendix B for more information.

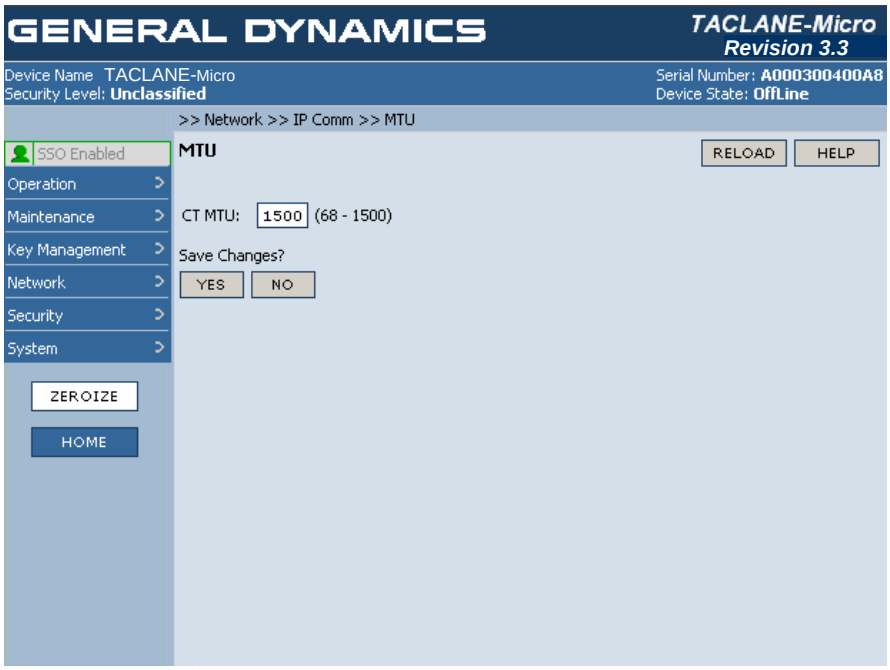
Notes

(U//FOUO) The following notes apply to modifying the MTU size:

- TACLANE defaults the MTU size to 1500 bytes. The maximum possible MTU size is 1500 bytes. The minimum possible MTU size is 68 bytes.
- TACLANE disregards the Don't Fragment (DF) bit in the IP header because ESP increases the packet size, which can create packets that require fragmentation to comply with MTU.

Procedure

(U//FOUO) Follow these steps to modify the TACLANE MTU size:

Step	Action
1.	From the MAIN MENU, select Network => IP Comm => MTU. Result: The following screen is displayed: 
2.	Type in the desired MTU size.
3.	Select YES to save changes.

5.4 (U) PING Configuration

Introduction

(U//FOUO) The operator may configure PING processing on the PT side and the CT side.

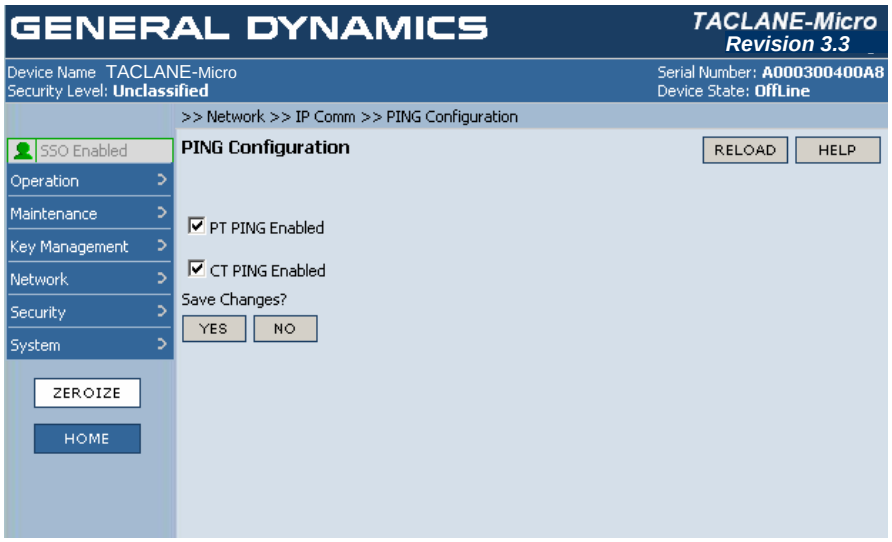
Notes

(U//FOUO) The following notes apply to PING configuration:

- TACLANE defaults the PT PING and CT PING to enabled.
- TACLANE ignores PINGs for its PT IP Address Received on the CT Interface.
- TACLANE ignores PINGs for its CT IP Address Received on the PT Interface.

Procedure

(U//FOUO) Follow these steps to modify the PING configuration:

Step	Action
1.	From the MAIN MENU, select Network => IP Comm => PING Configuration. Result: The following screen is displayed: 
2.	To enable PT interface PING responses, select the checkbox next to PT PING Enabled. If the box is checked, (a checkmark is present in the box) then PT PING processing is enabled. If the box is empty (no checkmark present in the box) then PT PING processing is disabled.
3.	To enable CT interface PING responses, select the checkbox next to CT PING Enabled. If the box is checked, (a checkmark is present in the box) then CT PING processing is enabled. If the box is empty (no checkmark present in the box) then CT PING processing is disabled.
4.	Select YES to save changes.

6.0 (U) CONFIGURING/MANAGING SECURITY ASSOCIATIONS

6.1 (U) Enable/Disable Secure Dynamic Discovery

Introduction

(U//FOUO) The operator can enable or disable Secure Dynamic Discovery (SDD) processing.

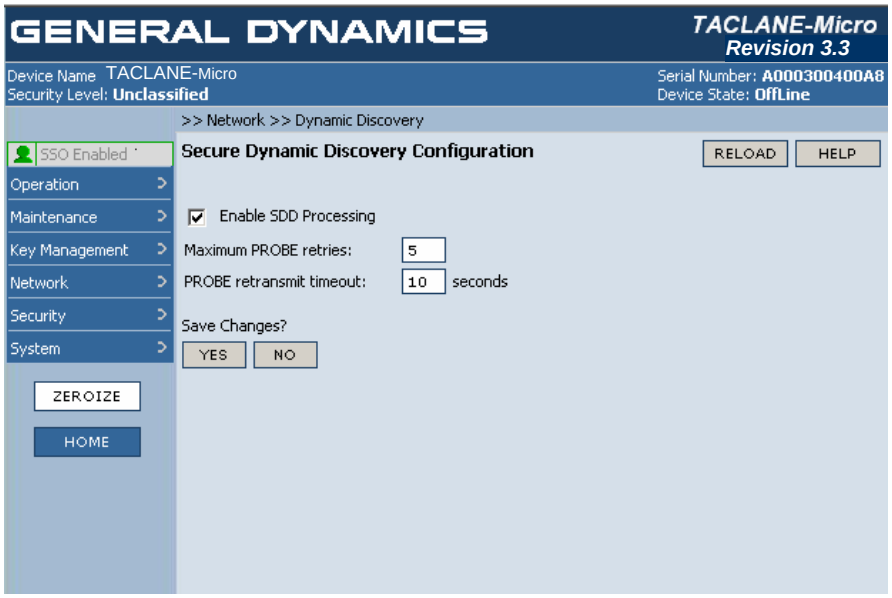
Notes

(U//FOUO) The following notes apply to enabling or disabling SDD processing:

- Only the SSO can edit parameters using this command.

Procedure

(U//FOUO) Follow these steps to enable or disable SDD processing:

Step	Action
1.	From the MAIN MENU, select Network => Dynamic Discovery. Result: The following screen is displayed: 
2.	To enable SDD, select the checkbox next to Enable SDD Processing. If the box is checked (a checkmark is present in the box), then Enable SDD Processing is enabled. If the box is empty (no checkmark present in the box), then Enable SDD Processing is disabled.
3.	If SDD Processing is enabled, enter the Maximum PROBE retries (1-5).
4.	If SDD Processing is enabled, enter the PROBE retransmit timeout (1-30) in seconds.
5.	Select YES to save changes.

6.2 (U) Assigning a PPK to an IP Address

Introduction

(U//FOUO) PPKs can be used to secure Security Associations (SA). The operator must assign a PPK to a remote TACLANE IP address to apply the PPK to that SA.

(U//FOUO) When a remote TACLANE IP address is assigned to a PPK, all secure IP traffic destined to that remote TACLANE uses the assigned PPK.

Determining the Remote TACLANE IP Address

(U//FOUO) In order to determine the applicable remote TACLANE IP address, the TACLANE can be configured to use static routing and/or automated peer TACLANE discovery via Secure Dynamic Discovery (SDD). The static routing table is searched first. If no match is found in the routing table, the TACLANE will try SDD.

(U//FOUO) Once the remote TACLANE is identified, PPK assignments are checked for a match based on the remote TACLANE IP address. If a match is found, the corresponding PPK is used in the security association.

Multicast PPK Assignment

(U//FOUO) A multicast (Class D) address may be entered instead of the remote TACLANE address.

(U//FOUO) When a multicast assignment is made, both the CT and PT IP addresses must be assigned to the same multicast address.

Continued on next page

(U) Assigning a PPK to an IP Address, continued

Notes

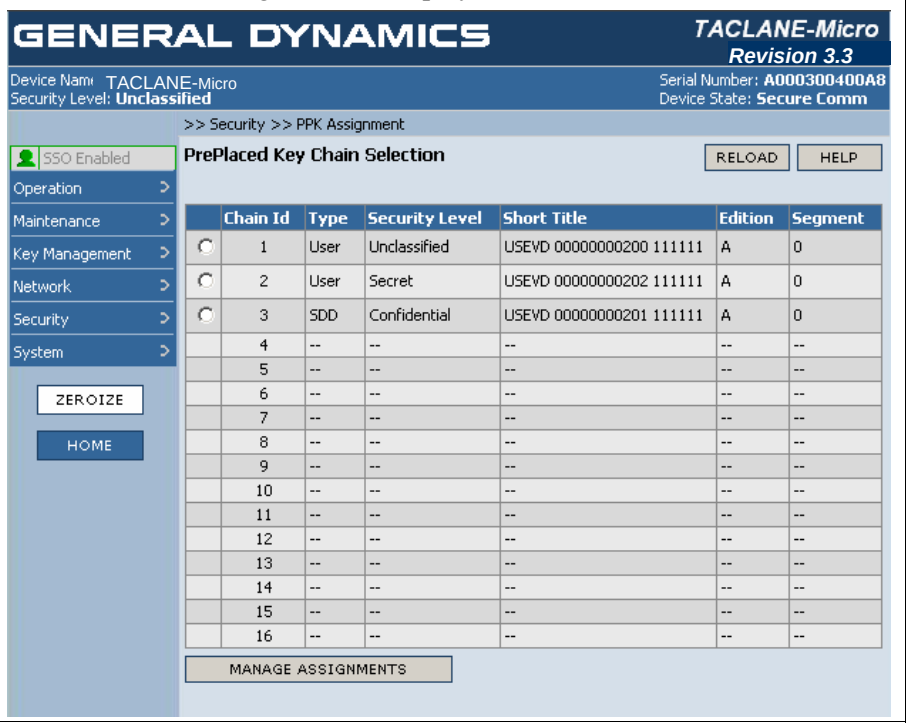
(U//FOUO) The following notes apply to assigning a PPK to an IP address:

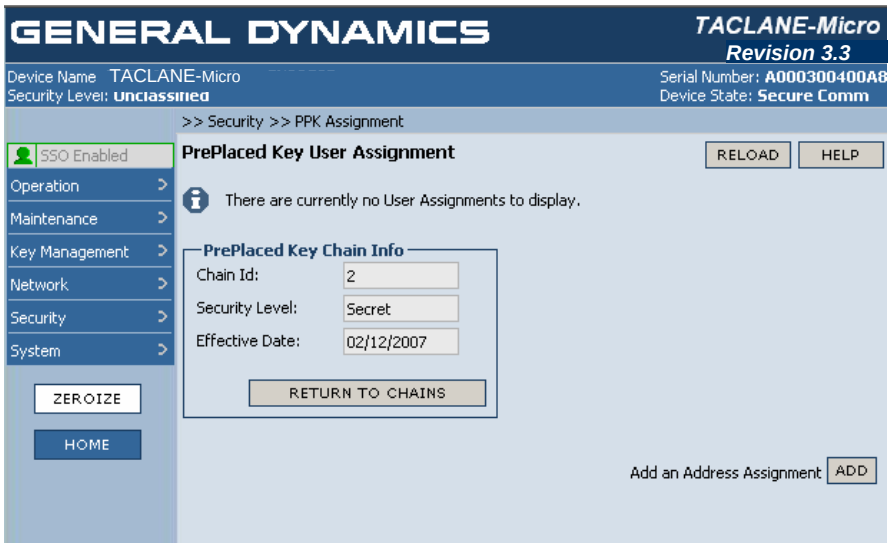
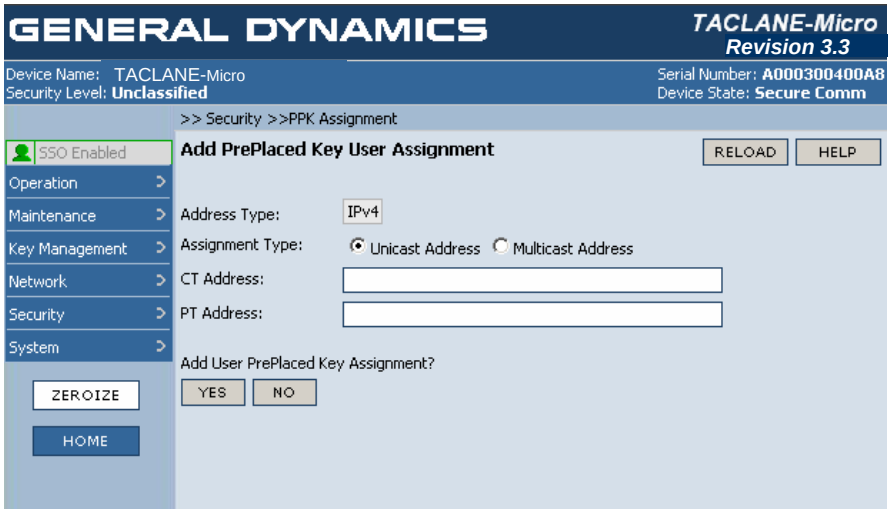
- Only the SSO can assign a PPK to an IP Address.
- TACLANE-Micro supports 1024 PPK assignments. Assignments are pooled for use by any PPK or at any security level
- For SAs using PPKs, all communicating TACLANEs must have the same PPK, at the same security level, with the same effective date, under the same PPK ID.
- All communicating TACLANEs must have their respective TACLANE IP addresses assigned (as the remote TACLANE IP address) to the same PPK ID at each respective TACLANE. (Both TACLANEs must point to each other.)
- Both the CT and PT remote TACLANE IP addresses must be entered.
- If one of the remote TACLANE IP addresses is unicast, then both IP addresses must be unicast.
- When a PPK address is assigned it is enabled, by default.
- For PPK configuration tips, see Appendix B, "IP/Ethernet Configuration Tips."

Procedure

(U//FOUO) Follow these steps to assign a PPK for establishing Security Associations with a specified remote INE:

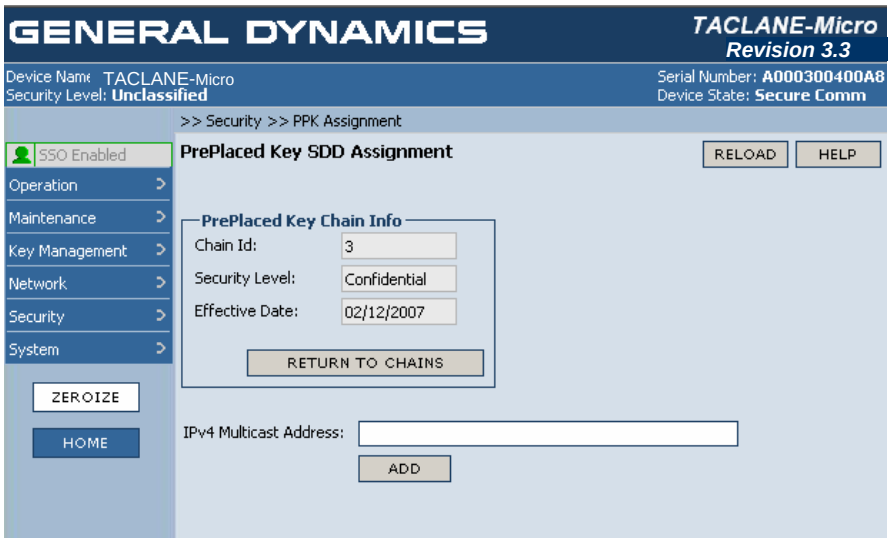
Step	Action
1.	From the MAIN MENU, select Security => PPK Assignment. Result: The following screen is displayed:



2.	Select the radio button next to the desired PPK Chain Id. Select MANAGE ASSIGNMENTS. **If the PrePlaced Key type is User**, the following screen is displayed: \ 
3.	Select ADD to add a new user address assignment. Result: The following screen is displayed: 

Continued on next page

(U) Assigning a PPK to an IP Address, continued

Step	Action
4.	Select the radio button next to the desired Assignment Type. Enter the CT Address and the PT Address. Note: If the Multicast Address radio button is selected, only the CT Address is an enterable text field.
5.	Select YES to save changes.
6.	**If the PrePlaced Key type is SDD**, the following screen is displayed: 
7.	Enter the multicast address.
8.	Select ADD to add the assignment.

6.3 (U) Enable/Disable a PPK Assignment

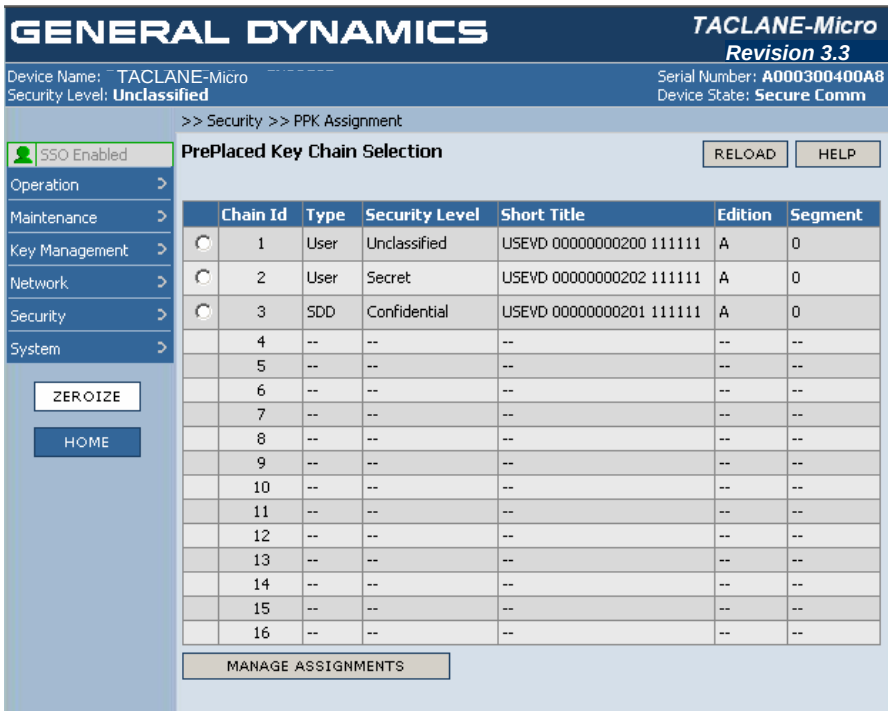
Introduction

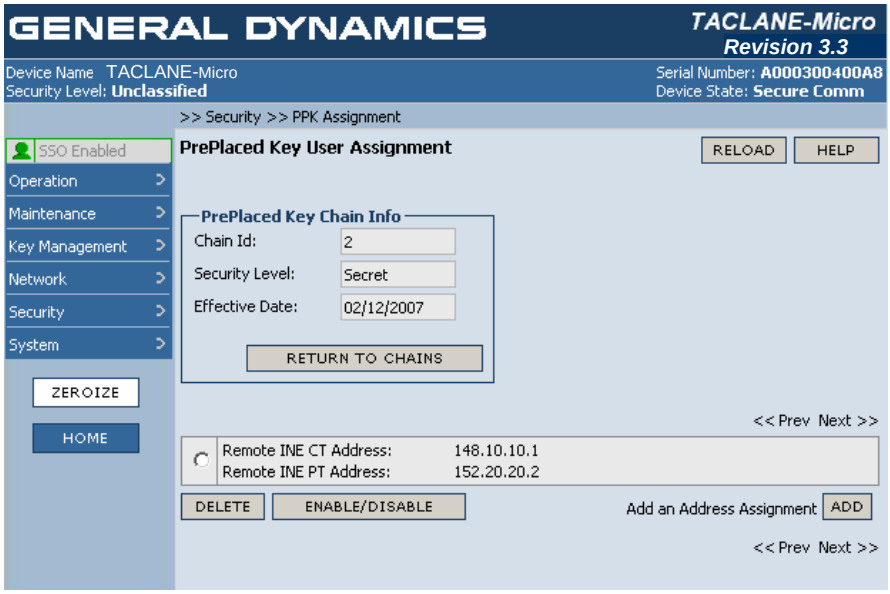
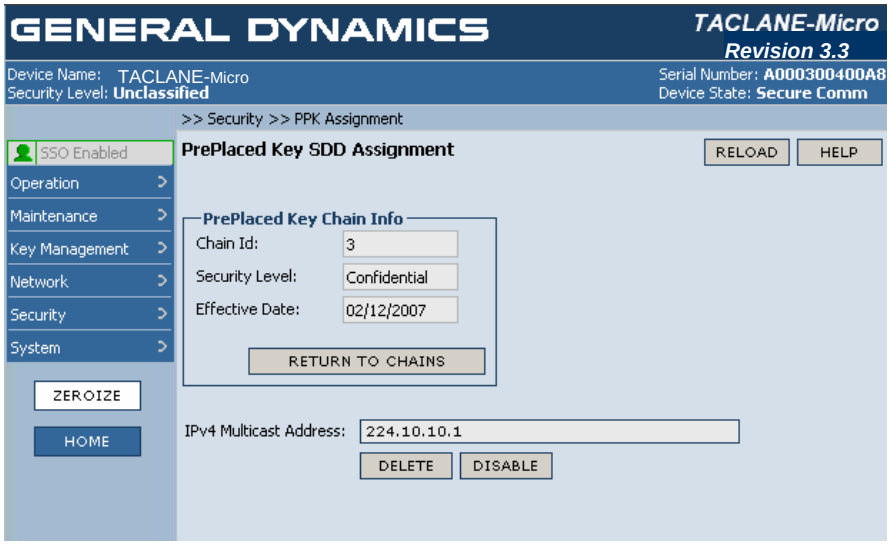
(U//FOUO) The operator can enable or disable a PPK assignment. This involves enabling or disabling an assigned remote TACLANE IP address to a PPK. This capability allows an assignment to be disabled temporarily without destroying the associated address entry.

Procedure

(U//FOUO) Follow these steps to enable or disable a PPK assignment:

Step	Action
1.	From the MAIN MENU, select Security => PPK Assignment. Result: The following screen is displayed:



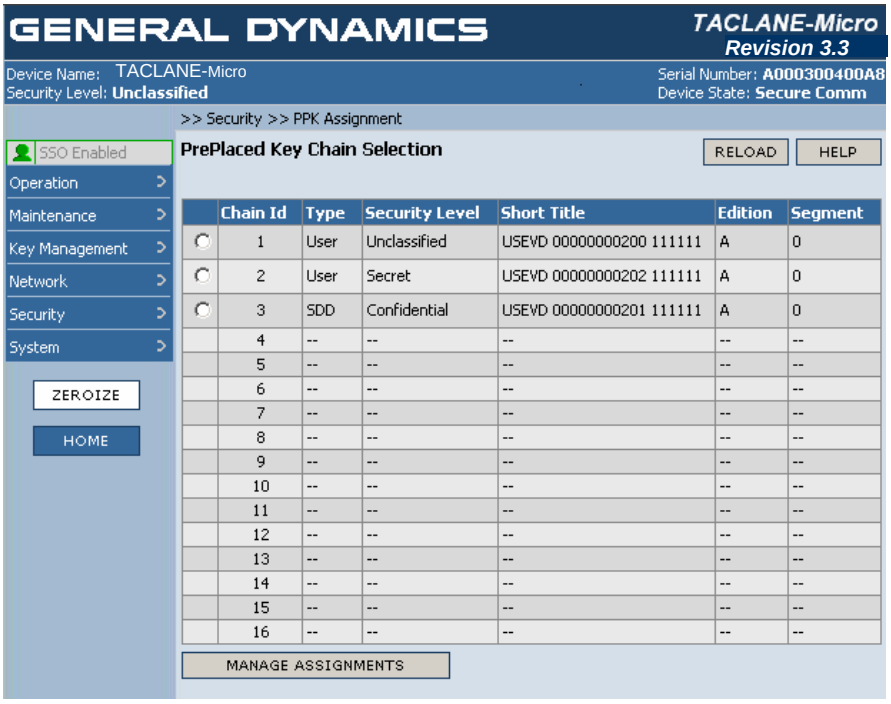
2	Select the radio button next to the desired PPK Chain Id. Select MANAGE ASSIGNMENTS. **If the PrePlaced Key type is User**, the following screen is displayed: 
3.	Select the radio button next to the desired Remote INE Address(es) or the Remote INE Multicast Address. Select ENABLE/DISABLE to enable or disable the PPK user assignment. Note: Remote INE Address(es) in italics are disabled.
4.	**If the PrePlaced Key type is SDD**, the following screen is displayed: 
5.	If the PPK assignment is disabled, select ENABLE to enable the PPK SDD assignment. If the PPK assignment is enabled, select DISABLE to disable the PPK SDD assignment.
6.	If disabling the PPK SDD Assignment, select OK to confirm.

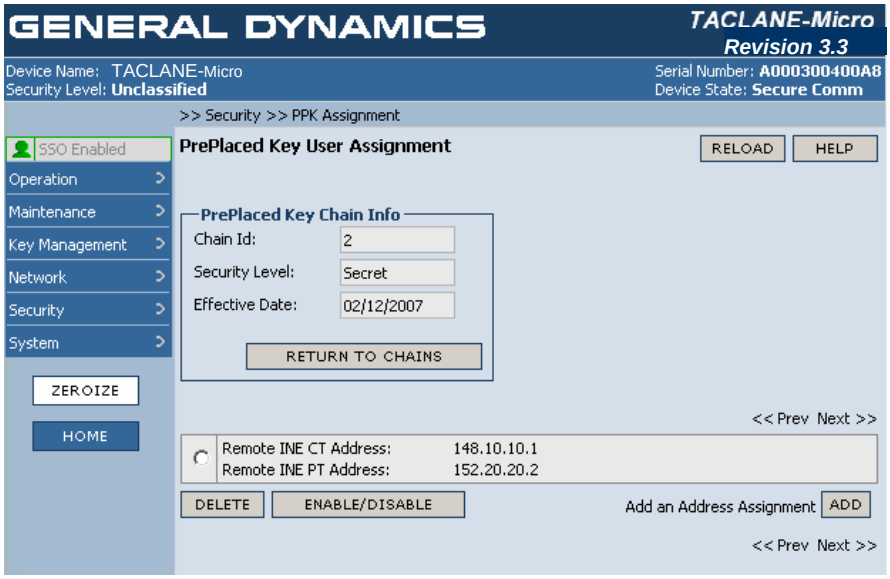
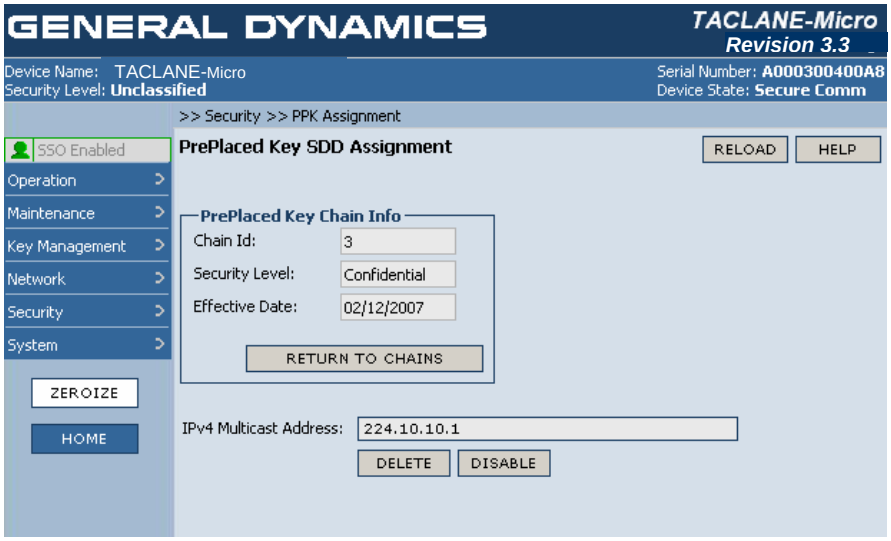
6.4 (U) Delete a PPK Assignment

Introduction (U//FOUO) The SSO operator can delete a PPK assignment.

Notes (U//FOUO) Only the SSO can delete a PPK assignment.

Procedure (U//FOUO) Follow these steps to delete a PPK assignment:

Step	Action
1.	From the MAIN MENU, select Security =>PPK Assignment. Result: The following screen is displayed: 

2.	Select the radio button next to the desired PPK Chain Id. Select MANAGE ASSIGNMENTS. **If the PrePlaced Key type is User**, the following screen is displayed: 
3.	Select the radio button next to the desired Remote INE Address(es) or the Remote INE Multicast Address. Select DELETE to delete the PrePlaced Key assignment.
4.	**If the PrePlaced Key use is SDD**, the following screen is displayed: 
5.	Select DELETE to delete the PrePlaced Key assignment.
6.	If deleting the PPK SDD Assignment, select OK to confirm.

6.5 (U) Entering Initialized State

Introduction

(U//FOUO) The operator may enter Initialized state.

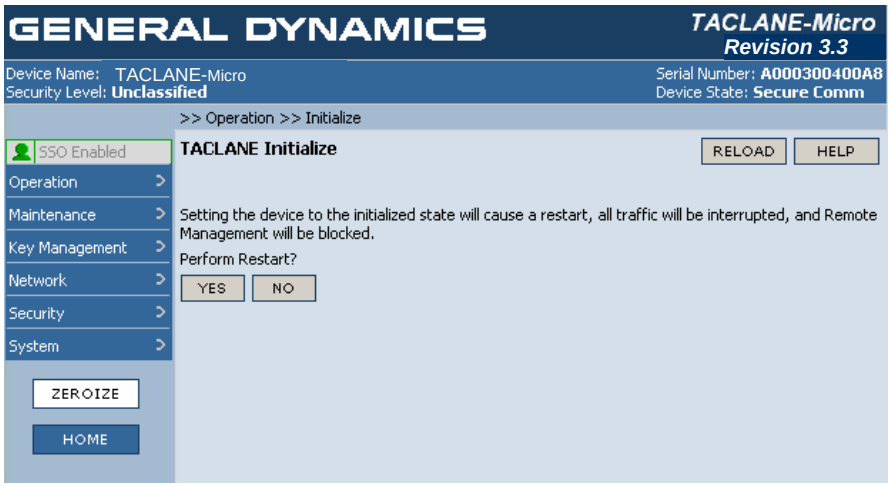
Notes

(U//FOUO) The following notes apply to Initialized:

- TACLANE must be offline or secure comm in order to enter initialized state.
- Transitioning to Initialized from any other state forces a device restart.
- Initialized state is a quiescent state that enables configurations to be set that will be applied upon state transition. This is convenient because some configurations force a restart, except for when they are performed in this state.

Procedure

(U//FOUO) Follow these steps to enter Initialized:

Step	Action
1.	From the MAIN MENU, select Operation => Initialize. Result: The following screen is displayed: 
2.	Select YES to transition to Initialized, which will restart the TACLANE.

6.6 (U) Entering Offline State

Introduction

(U//FOUO) The operator may enter Offline state to secure local traffic.

PPK SA Establishment

(U//FOUO) Upon transition to the Offline state (with security level set) from the Initialized state, SAs for properly configured PPK Assignments will be established.

(U//FOUO) If configured, the SDD SA will be setup in the Offline state (with security level set).

IKE SA Processing

(U//FOUO) Upon transition to the Offline state (from the Initialized state), the INE will configure and activate the PT and CT Ethernet links. (The CT link is activated only if a security level is defined.)

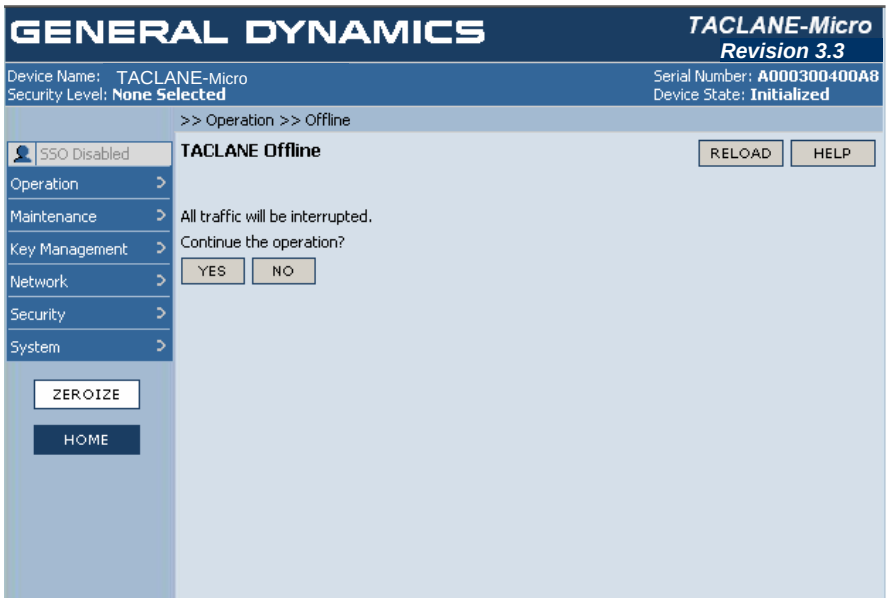
Notes

(U//FOUO) The following notes apply to entering Offline:

- TACLANE must be initialized or secure comm in order to enter offline.
- The IP addresses are required to be configured on the PT and CT interfaces before transitioning to offline.

Procedure

(U//FOUO) Follow these steps to enter offline mode:

Step	Action
1.	From the MAIN MENU, select Operation => Offline. Result: The following screen is displayed: 
2.	Select YES to transition to Offline.

6.7 (U) Entering Secure Communications State

Introduction

(U//FOUO) The operator may enter Secure Communications state to process all user and management traffic.

PPK Takes Precedence Over FIREFLY

(U//FOUO) For SAs, a PPK assignment takes precedence over generating a FIREFLY TEK.

Automated Peer TACLANE Discovery

(U//FOUO) TACLANEs support automated peer TACLANE discovery for SAs, through the HAIPE IS Secure Dynamic Discovery (SDD) protocol, as described in HAIPE IS v1.3.5. Once a peer TACLANE is identified, the following occurs:

- PPK assignments are checked for a match based on the remote TACLANE IP address. If a match is found, the corresponding PPK is for the security association.
- Existing security associations using FIREFLY TEKs are checked for a match based on the remote TACLANE IP address. If a match is found, the corresponding existing security association (using a FIREFLY TEK) is used to secure the IP traffic.

(U//FOUO) If there is no matching PPK assignment or security association (using a FIREFLY TEK), and an operational FIREFLY vector set is usable at the current security level, the following occurs: a new security association is created and the initiator and responder peer TACLANEs cooperatively generate a FIREFLY TEK using their FIREFLY vector sets.

Remote TACLANE Static Routes

(U//FOUO) If automated peer TACLANE discovery is not desirable, remote TACLANE static routes can be defined. This eliminates the need for automated peer TACLANE discovery. (See the section "Configuring Remote TACLANE Static Routing.") When static routes are configured, PPK and FIREFLY can both be used to secure communications without use of automated peer TACLANE discovery.

Securing Multicast Traffic

(U//FOUO) TACLANEs support static multicast.

- A static multicast group is configured on the TACLANE by assigning a PPK to the static multicast group address.
- Remote TACLANE IP addresses that are a mix of multicast and unicast IP addresses may be assigned to the same PPK.
- TACLANE will encrypt all PT IP datagram traffic destined for the specified multicast (Class D) IP address and send the CT ESP IP datagrams to the same multicast IP address.
- Received CT ESP IP datagrams destined for the specified multicast IP address are decrypted and the PT IP datagrams are sent to the same multicast address.
- Multicast IP datagram traffic is not supported for FIREFLY.

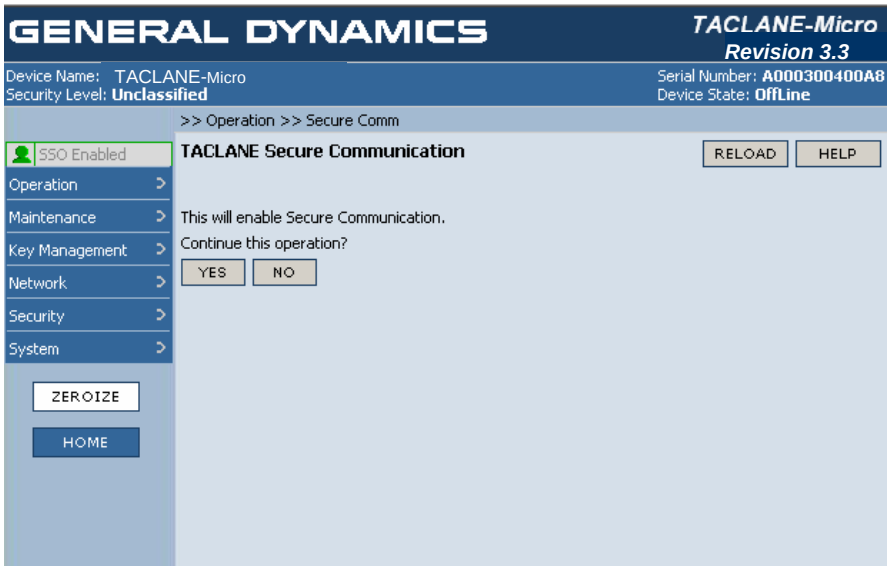
Notes

(U//FOUO) The following notes apply to entering secure comm:

- TACLANE must be offline, with a security level selected, in order to enter secure communications mode.
- TACLANE must have a valid IP/Ethernet configuration.
- All communicating TACLANEs must be at the same security level.
- If FIREFLY TEKs are used, each communicating TACLANE must have a unique valid operational FIREFLY vector set, and the FIREFLY vector sets must be valid for the current security level.
- If PPKs are used, all communicating TACLANEs must have valid PPK assignments with the same PPK, at the same security level, with the same effective date, under the same PPK ID.

Procedure

(U//FOUO) Follow these steps to enter secure communications mode:

Step	Action
1.	From the MAIN MENU, select Operation => Secure Comm. Result: The following screen is displayed: 
2.	Select YES to transition to secure communications. Note: The TACLANE is now in secure communications mode. The RUN status LED is blinking, indicating that the TACLANE is ready to process traffic.

6.8 (U) Security Association Info – SA Table

Introduction

(U//FOUO) The operator may view, modify or delete Security Associations while in offline or in secure comm mode.

Notes

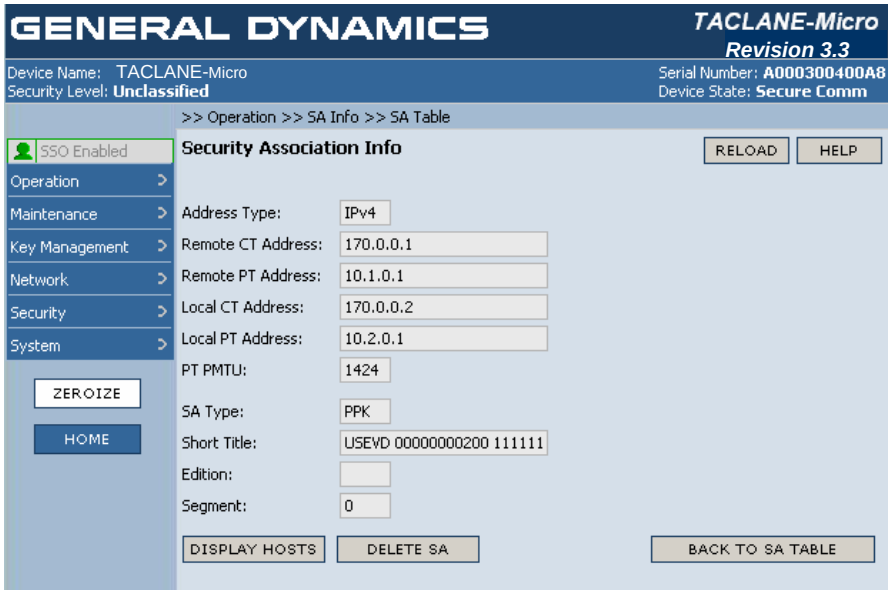
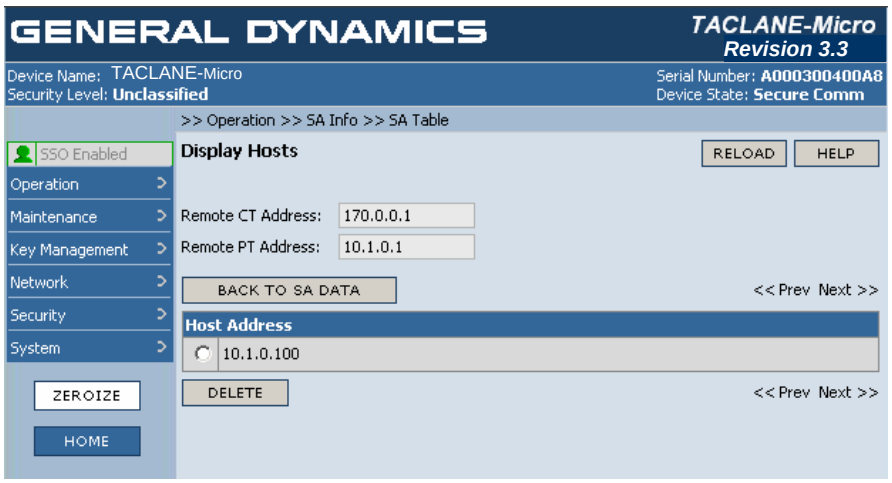
(U//FOUO) The following notes apply to displaying SA information:

- TACLANE must be offline or in secure comm state to display SA information.
- Static routes are not displayed here; one must go to static routes screens to see the static routing table.

Procedure

(U//FOUO) Follow these steps to display SA information:

Step	Action
1.	From the MAIN MENU, select Operation => SA Info => SA Table. Result: The following screen is displayed:  Note: The full IP CT address of the first remote INE in the SA table is displayed in the 'Remote INE CTs from' entry box.
2.	Enter an IP CT Address in the 'Remote INE CTs from' entry box for direct access to an SA. Select GO to display the SA Table starting with the entered Remote INE CT.
3.	Select the radio button next to the desired address.

4.	Select VIEW/MODIFY. Result: The following screen is displayed: 
5.	Select DELETE SA to delete this Security Association.
6.	Select DISPLAY HOSTS to display the known hosts protected by this SA. Result: The following screen is displayed: 
7.	Select the radio button next to the desired Host Address.
8.	Select DELETE to delete the host from the SA or Security Association.
9.	Select BACK TO SA DATA to return to the Security Association Info screen.
10.	Select BACK TO SA TABLE to return to the Security Associations screen.

6.9 (U) Configuring Remote TACLANE Static Routing

Introduction

(U//FOUO) The TACLANE operator can define static routes which associate destination IP network identifiers with remote TACLANEs protecting that target. More basically, a static route answers the following question: which TACLANE should the SA be established with for communications to this remote network or target?

(U//FOUO) In addition to defining remote TACLANE static routes for particular IP network addresses, the TACLANE operator can also define one default static route (to a remote TACLANE).

Remote TACLANE Static Routing Table

(U//FOUO) The operator may define a remote TACLANE routing table to associate destination IP networks identifiers with remote TACLANEs:

- Up to 1024 route entries may be defined. Entries are pooled; across all security levels. A default route may be defined as one of the route entries, which supersedes all other routes.
- Entries consist of a remote TACLANE CT IP address, remote TACLANE PT IP address, destination network ID, and prefix length. (When the target destination is in the destination network then use the TACLANE at the specified TACLANE CT address.)
- The TACLANE may include routes to itself, which will be ignored. This enables a common static routing table to be used for a group of TACLANEs. Common static routing tables reduce configuration burden and complexity. **It is recommended that these routes be included even when a CT default route is defined.**
- Multiple destination IP networks identifiers may be associated with the same remote TACLANE IP address (thus a TACLANE may protect multiple subnets or targets).
- Validation checks on table entries include:
  - No duplicate table entries (no two entries with the same network ID and subnet mask). (The same network ID may be defined in multiple entries as long as the subnet masks are different.)
- A "longest match" search of the table based on network ID is used to determine the remote TACLANE to which the IP traffic should be sent.
- GEM X can also configure the routing table. One routing table can be generated by the GEM X and distributed to all the TACLANEs.

Default Static Route

(U//FOUO) The operator can define one default route entry for the TACLANE by setting the network ID and prefix length to 0.0.0.0/0.

(U//FOUO) **When a default static route is defined, the TACLANE will never try to use the SDD dynamic discovery.**

Static Routing Features

(U//FOUO) Remote TACLANE static routing:

- Eliminates the need for the CT network to have knowledge of routes to the PT networks behind TACLANEs and vice versa.
- Eliminates the need for router tunnel and NAT workarounds.
- Allows the CT and PT interfaces of the TACLANE to operate in two different IP networks/subnetworks.
- Supports proxy-ARP for destinations covered by routing table entries.
- ARP for off-net destinations if PT and/or CT gateway is not defined.

Sequence to Identify the Remote TACLANE

(U//FOUO) The TACLANE is capable of both static routing and SDD. When processing user traffic, TACLANE follows a particular sequence in order to identify the remote TACLANE associated with the destination host. Static routing has a higher precedence, so the routing table is always searched first. Specifically, the sequence is:

1. check for specific static route in remote TACLANE static routing table
2. if static route not found, use the default static route, if it is defined
3. if neither of the above are true, try to use SDD (assumes SDD PPK has been filled and assigned to a multicast address).

(U//FOUO) **When a default static route is defined, SDD Probes will never be sent because the default route always produces a "match". If a user wants the TACLANE to try SDD, then a default static route must not be configured.**

PT Proxy-ARP Support

(U//FOUO) TACLANE proxy-ARP replies to an ARP request received by the PT interface when the target address is covered by a static routing table entry. TACLANE will not proxy-ARP reply to a PT host based solely on a default route. The target IP address in the PT ARP request must be covered by a static routing table entry other than the default route.

PT Default Gateway or ARP Used to Deliver PT IP Traffic

(U//FOUO) If the optional PT default gateway IP address is configured, all off-net decrypted PT IP traffic will be delivered to the PT default gateway.

(U//FOUO) If the optional PT default gateway is not configured, TACLANE will ARP for all off-net destination IP addresses for decrypted PT IP traffic*.

*Assumes proxy-ARP support in PT routers. Proxy-ARP allows a router to reply to a received ARP request for a host in a network that is in the router's routing table.

CT Default Gateway or ARP Used to Deliver CT IP Traffic

(U//FOUO) If the optional CT default gateway IP address is configured, all off-net encrypted CT IP traffic will be delivered to the CT default gateway.

(U//FOUO) If the optional CT default gateway is not configured, TACLANE will ARP for all off-net destination IP addresses for encrypted CT IP traffic*.

*Assumes proxy-ARP support in CT routers. Proxy-ARP allows a router to reply to a received ARP request for a host in a network that is in the router's routing table.

(U//FOUO) When a CT default gateway is defined, it is recommended that a route for the local TL-protected network also be included in the static routing table.

Network ID, Prefix length and Static Routing

(U//FOUO) The TACLANE does not have to be restarted after changing static routing table entries. However, the SAs that used modified or deleted entries will still exist. These can be removed manually or by restarting.

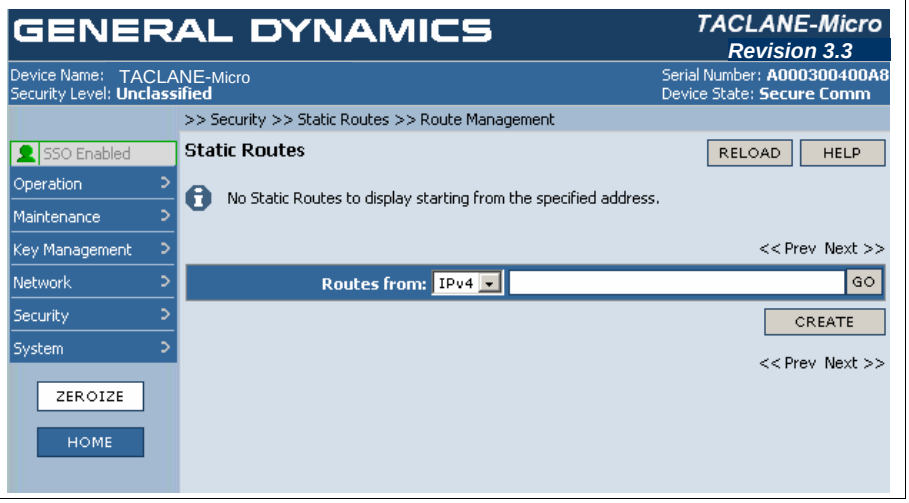
Notes

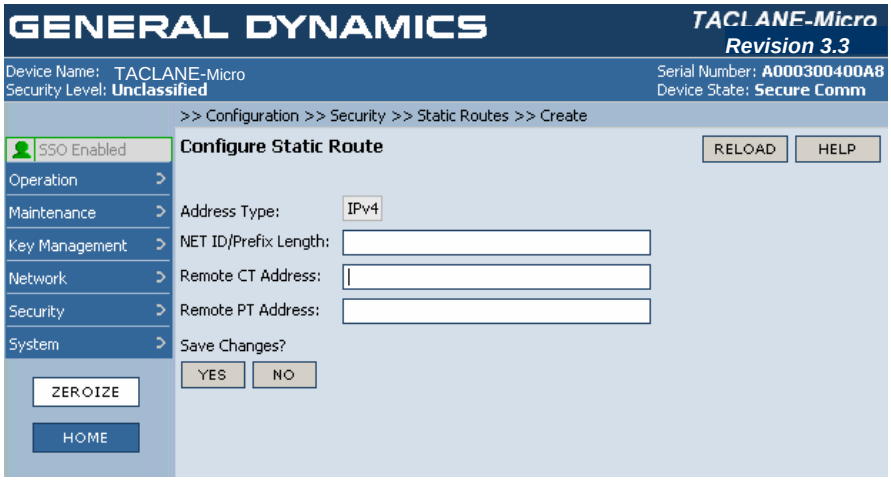
(U//FOUO) The following notes apply to configuring remote TACLANE static routes:

- Routes can be associated with subnets, portions of subnets, or specific host addresses. The granularity of scope is controlled by the prefix setting.

Procedure

(U//FOUO) Follow these steps to configure remote TACLANE static routes:

Step	Action
1.	From the MAIN MENU, select Security => Static Routes => Route Management. Result: The following screen is displayed: 

2.	Select CREATE. Result: The following screen is displayed:  Note: The routing table entry with longest matching network ID and prefix length combination will be determined to select the remote TACLANE to send the IP traffic to. Note: For IPv4, one default route TACLANE table entry can be defined by setting the NET ID and prefix length to 0.0.0.0/0. Example static routing table entries: Entry 1: Network ID/Prefix Length: 0.0.0.0/ 0 TL CT IP: 148.10.2.1 (default route) Entry 2: Network ID/Prefix Length: 200.12.0.0/16 TL CT IP: 148.10.4.11 Entry 3: Network ID/Prefix Length: 200.12.3.0/24 TL CT IP: 148.10.3.10 For the target host IP address 200.12.2.43, Entry 2 is the "longest match," so data for 200.12.2.43 will be encrypted and sent to 148.10.4.11. For the target host IP address 200.12.3.25, Entry 3 is the "longest match," so traffic for 200.12.3.25 will be encrypted and sent to 148.10.3.10. For the target host IP address 10.24.105.26, neither Entry 2 nor Entry 3 is a match, so Entry 1 (the default route) is used. Traffic for 10.24.105.26 will be encrypted and sent to 148.10.2.1.
3.	Enter the Network ID/Prefix Length, Remote CT Address, and Remote PT Address.
4.	Select YES to save changes.

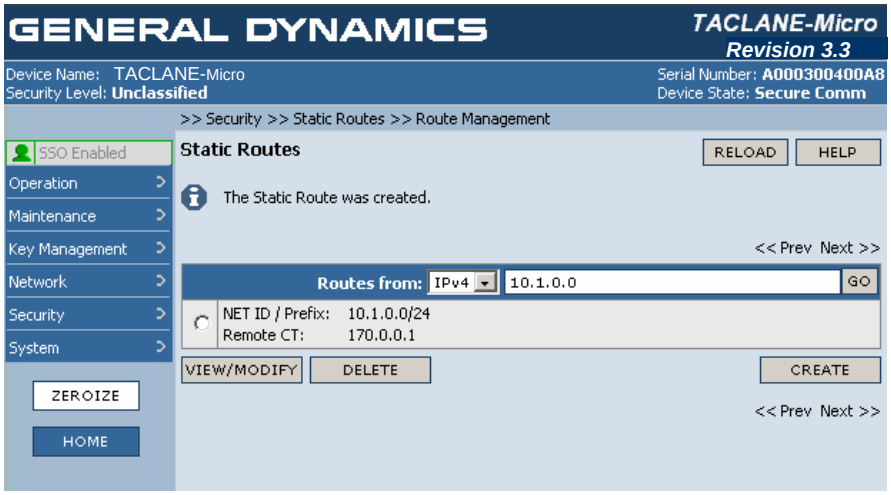
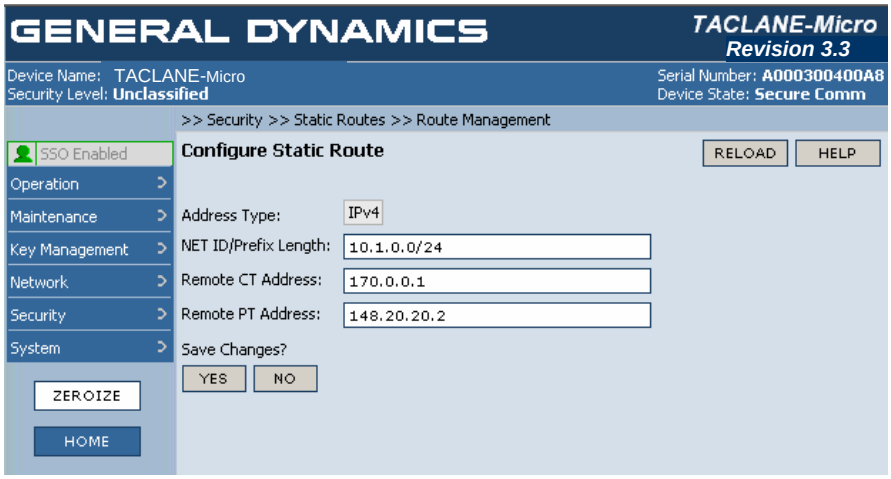
6.10 (U) Modifying Remote TACLANE Static Routes

Introduction

(U//FOUO) The operator can modify the remote TACLANE routing table. See the section "Configuring Remote TACLANE Static Routing" for more information.

Procedure

(U//FOUO) Follow these steps to modify remote TACLANE static routes:

Step	Action
1.	From the MAIN MENU, select Security => Static Routes => Route Management. Result: The following screen is displayed: 
2.	Select the radio button next to the desired Static Route. Select VIEW/MODIFY. Result: The following screen is displayed: 
3.	Update the Network ID/Prefix Length, Remote CT INE Address, and/or Remote PT INE Address.

4.	Select YES to save changes.

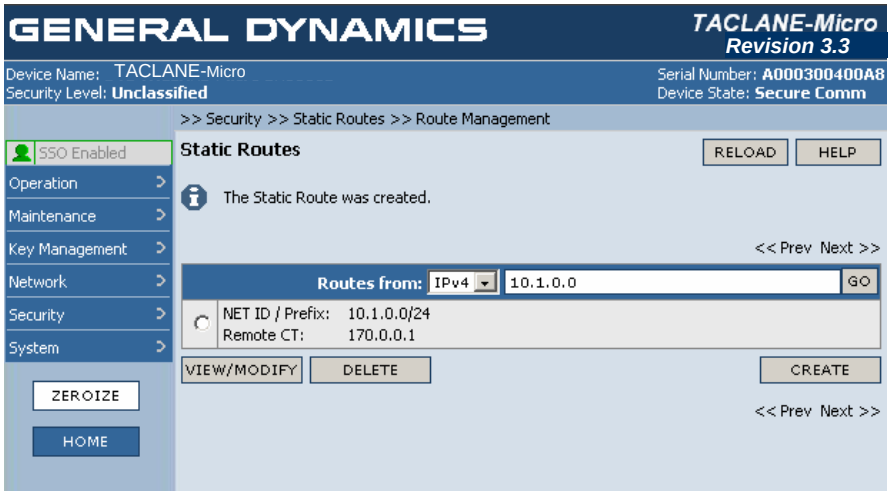
6.11 (U) Deleting Remote TACLANE Static Routes

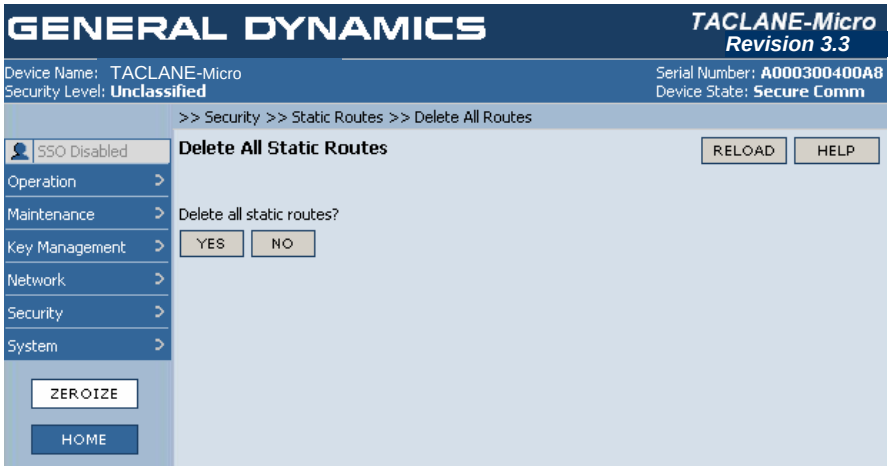
Introduction

(U//FOUO) The operator can delete a remote TACLANE routing table entry or the entire routing table.

Procedure

(U//FOUO) Follow these steps to delete remote TACLANE static routes:

Step	Action
1.	**To delete a static route**, from the MAIN MENU, select Security => Static Routes =>Route Management. Result: The following screen is displayed: 
2.	Select the radio button next to the route to delete. Select DELETE to delete the route.

3.	**To delete all static routes**, from the MAIN MENU, select Security => Static Routes => Delete All Routes. Result: The following screen is displayed: 
4.	Select YES to confirm deletion of all static routes.

6.12 (U) Configuring Security Association

Introduction

(U//FOUO) The SSO operator can configure the method in which the FIREFLY TEKs are automatically updated every 24 hours. FIREFLY TEKs can be updated either deterministically, using the ACCORDION algorithm, or by performing a new IKE exchange and generating a new TEK (MTEK/MTEK update).

(U//FOUO) The TACLANE operator configures the DAILY MTEK parameter to:

1) *ENABLE* – when enabled, MTEK/MTEK (IKE exchange) is the method used for the daily FIREFLY key update.

2) *DISABLE* (the default value) – when disabled, local ACCORDION update is the method used for the daily FIREFLY key update.

The TACLANE operator can configure the status of the SA Host Administrative Timeout and the SA Timeout value.

(U//FOUO) The TACLANE operator configures the SA Host Administrative Timeout to:

1) *ENABLE* (the default value) – when enabled, the SA Host Administrative Timeout function is enabled.

2) *DISABLE* – when disabled, the SA Host Administrative Timeout is inactive.

(U//FOUO) When the SA Host Administrative Timeout is enabled, the TACLANE operator configures the SA Host Administrative value to:

1-1440 (the default value = 720)

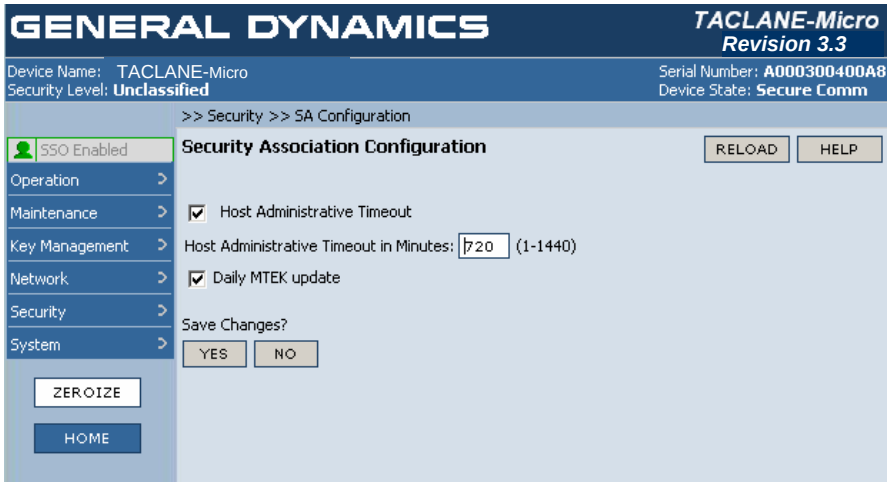
Notes

(U//FOUO) The following notes apply to configuring the security association:

- Only the SSO has the privilege to configure the security association.
- The SA Host Administrative Timeout specifies the maximum time that a host can be associated with a specific SA before requiring a refresh. Upon timeout the host is removed from the SA Host table. It is refreshed upon receipt of traffic to stimulate association with an SA. The SA Timeout is the maximum Time that an SA can remain without being reestablished. Both of these timers support dynamically changing networks. They should be set long enough to minimize volatility of configuration and short enough to facilitate adequate response to network changes.

(U) Configuring Security Association, continued

Procedure (U//FOUO) Follow these steps to configure the security associations setting:

Step	Action
1.	From the MAIN MENU, select Security => SA Configuration. Result: The following screen is displayed: 
2.	Select the checkbox next to Host Administrative Timeout to ENABLE or DISABLE the parameter. If the box is checked, (a checkmark is present in the box) then Host Administrative Timeout is enabled. If the box is empty (no checkmark present in the box) then Host Administrative Timeout is disabled.
3.	Enter the Timeout value in minutes if the Host Administrative Timeout is enabled.
4.	Select the checkbox next to Daily MTEK Update to ENABLE or DISABLE the parameter. If the box is checked, (a checkmark is present in the box) then Daily MTEK Update is enabled. If the box is empty (no checkmark present in the box) then Daily MTEK Update is disabled.
5.	Select YES to save changes.

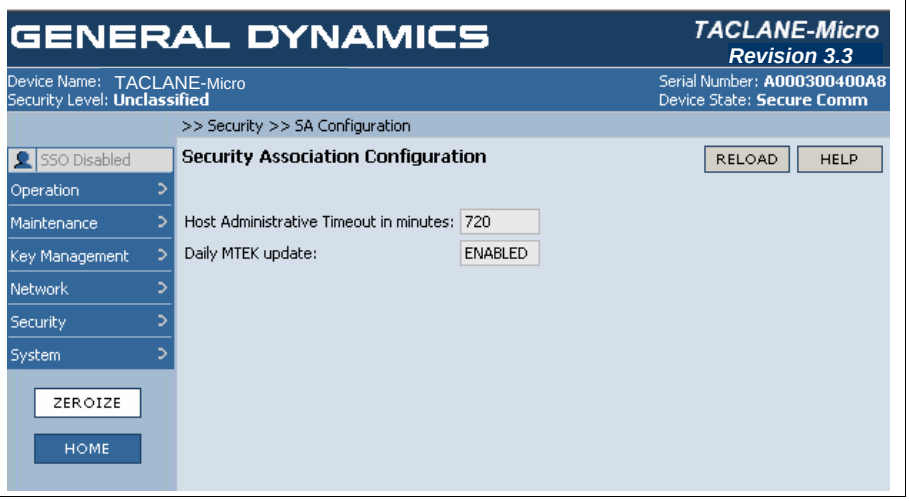
6.13 (U) Displaying the SA Configuration Information

Introduction

(U//FOUO) The operator can display the SA Configuration information, which includes the TACLANE's Host Administrative Timeout setting and the MTEK Update setting.

Procedure

(U//FOUO) Follow these steps to display the SA Configuration information:

Step	Action
1.	From the MAIN MENU, select Security => SA Configuration. Result: The following screen is displayed: 

7.0 (U) CONFIGURING IP TRAFFIC FLOW SECURITY PARAMETERS

General Notes

(U//FOUO) The TACLANE includes IP Traffic Flow Security (TFS) features that are required by the HAIPE IS Traffic Flow Security specification. When configured appropriately, the IP TFS features in the TACLANE prevent/reduce compromise of sensitive information due to certain types of attacks. This chapter explains how each IP TFS parameter may be configured by the Site Security Officer (SSO) and how the IP TFS configuration information can be displayed.

(U//FOUO) There are important security and performance trade-offs that should be considered when enabling and disabling TFS countermeasures. For descriptions of these trade-offs along with recommended network and equipment configurations that minimize security risks, please refer to the TACLANE Security Features Users Guide.

(U//FOUO) TFS configuration update has been extended to allow online updates of TFS parameters. Although the design permits this, there is a slight chance that a false alarm may be detected when traffic loading is over 10 Mbps. Therefore it is recommended not to change TFS parameters during high traffic periods. If the false alarm is detected, the TACLANE-Micro will restart and recover with the new configuration.

7.1 (U) Configuring Fixed Packet Length Parameters

Introduction

(U//FOUO) Fixed Packet Length (FPL) parameters can be configured only by the SSO. The purpose of Fixed Packet Length processing is to obscure the sizes of plaintext IP packets before they are encrypted and transmitted on the CT network. When FPL processing is enabled, all user data packets (including IP multicast datagrams) received on the PT side of the TACLANE are padded to a fixed length if shorter than the configured fixed length, or fragmented (or optionally discarded) if longer than the configured fixed length. Fixed Packet Length parameters do not affect the processing of IP packets received on the CT side. All the TACLANE software versions correctly discard the padding added by FPL processing. Fixed Packet Length configuration has no impact on interoperability; FPL parameters can be configured independently at each TACLANE.

Notes

(U//FOUO) The following notes apply to configuring Fixed Packet Length parameters:

- Only the SSO has the privilege to configure FPL parameters.
- Audit log entries are generated when FPL parameters are modified.

Fixed Packet Length Parameters

(U//FOUO) The following two Fixed Packet Length parameters can be configured by the SSO:

- Mode: The fixed packet mode can be set to: ON/FRAGMENT, ON/DISCARD or OFF. When the mode is set to ON/FRAGMENT, FPL processing is performed with the incoming PT user data packets fragmented if they are longer than the configured fixed packet length. All fragments will be equal to the fixed packet length, with the last fragment being padded if necessary. When the mode is set to ON/DISCARD, FPL processing is performed with the incoming PT user data packets discarded if they are longer than the configured fixed packet length. When the mode is set to OFF, no FPL processing is done. The default value for this parameter is ON/FRAGMENT.
- Length: This is the IP packet length (both the IP header and the payload), in bytes, to which all incoming PT user data packets are padded or fragmented. The IP packet length can be set to any one of 27 values ranging from 176 to 1424, in increments of 48. The default length is 800 bytes. Note that the specified length is prior to encryption. The resulting CT encrypted IP packets will be at least 60 bytes longer due to the addition of the AH and ESP headers (this assumes no fragmentation due to the TACLANE MTU size).

Continued on next page

(U) Configuring Fixed Packet Length Parameters, continued

Fixed Packet Length Processing

(U//FOUO) When the fixed packet mode is set to ON/FRAGMENT (default setting):

- Incoming PT IP user data packets longer than the fixed packet length are fragmented. All fragments will be equal to the fixed packet length, with fragments being padded if necessary. (See the SFUG for more details on fragmentation.) Fragmentation will be performed regardless of the value of the Don't Fragment (DF) bit in the IP header.
- Incoming PT IP user data packets shorter than the fixed packet length are padded to the fixed packet length.

(U//FOUO) When the fixed packet mode is set to ON/DISCARD:

- Incoming PT IP user data packets longer than the fixed packet length are discarded. If the DF bit is set, a destination unreachable message is sent to the originator.
- Incoming PT IP user data packets shorter than the fixed packet length are padded to the fixed packet length.

(U//FOUO) When the fixed packet mode is set to OFF:

- No fixed packet processing is done. The length and fragment/discard parameters are ignored.

(U//FOUO) Once the CT traffic is decrypted by the receiving TACLANE:

- Any padding that was added by the encrypting TL is discarded.
- No reassembly of plaintext fragments is done. All decrypted fragments are sent to destination hosts for reassembly.
- This receive processing is the same for all TACLANE software versions.

(U//FOUO) Note: Fixed Packet Length processing applies to all ESP IP datagrams, including IP multicast datagrams. Control messages such as ARP are not affected by FPL processing.

Continued on next page

(U) Configuring Fixed Packet Length Parameters, continued

Caveats

(U//FOUO) The following caveats apply to Fixed Packet Length parameters:

- When using TACLANEs in a nested configuration, the fixed packet mode of the inner TLs must not be set to ON/DISCARD so that the encrypted traffic from the outer TLs is not discarded. Nesting may fail if the mode for an inner TL is set to ON/DISCARD. To ensure that user data packets are not discarded in a nested configuration, either:
  - set the fixed packet lengths for the inner TACLANEs at least 96 bytes (two 48-byte increments) longer than the fixed packet lengths of the outer TACLANEs, or
  - set the fixed packet mode for the inner TLs to ON/FRAGMENT. While this does not provide optimal performance, it will ensure that packets are not discarded.

FPL and MTU

(U//FOUO) When configuring the FPL and MTU parameters, it is important to consider their effects on TACLANE processing. Improper configurations can cause excessive fragmentation, which will have a negative impact on performance.

(U//FOUO) When FPL processing is enabled, the fixed packet length affects the size of packets prior to encryption. When necessary, fragmentation is performed on plaintext datagrams. Since each fragment is encrypted separately, no reassembly is performed by the destination TACLANE. Each fragment is decrypted and sent to its PT destination host. Reassembly of fragments created because of FPL processing is performed by destination hosts.

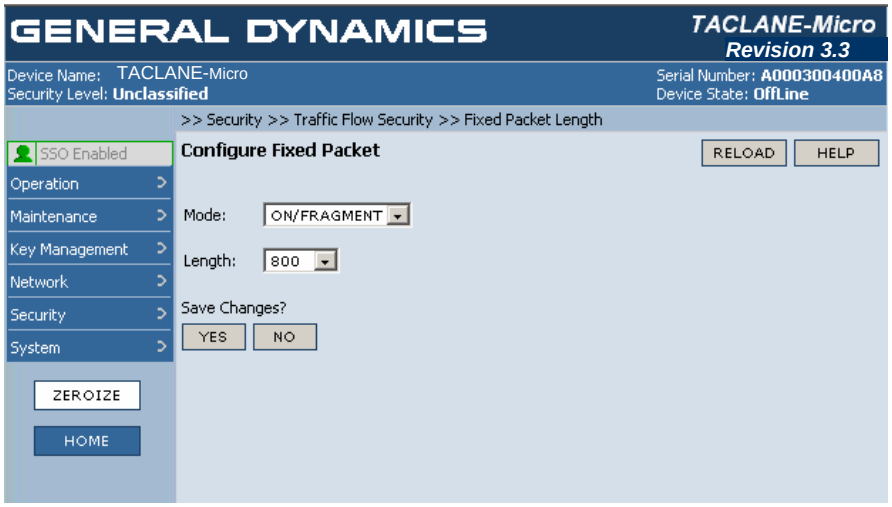
(U//FOUO) In contrast, the TL MTU determines which packets are fragmented following encryption. Since MTU fragmentation is performed on encrypted packets, the fragments must be received and reassembled by the destination TACLANE before each packet can be decrypted. If the MTU is not set to at least 60 bytes more than the FPL, then every packet will be fragmented on the CT side, causing severe performance degradation. For information on configuring the TL MTU size, see Section on "Modifying the TACLANE MTU Size."

Continued on next page

(U) Configuring Fixed Packet Length Parameters, continued

Procedure

(U//FOUO) Follow these steps to configure the Fixed Packet Length parameters:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security => Fixed Packet Length Result: The following screen is displayed: 
2.	Use the Mode pull down menu to select the mode ON/FRAGMENT, ON/DISCARD, or OFF options.
3.	Use the Length pull down menu to select the fixed packet length. The minimum value is 176 and the maximum value is 1424, in increments of 48.
4.	Select YES to save changes.

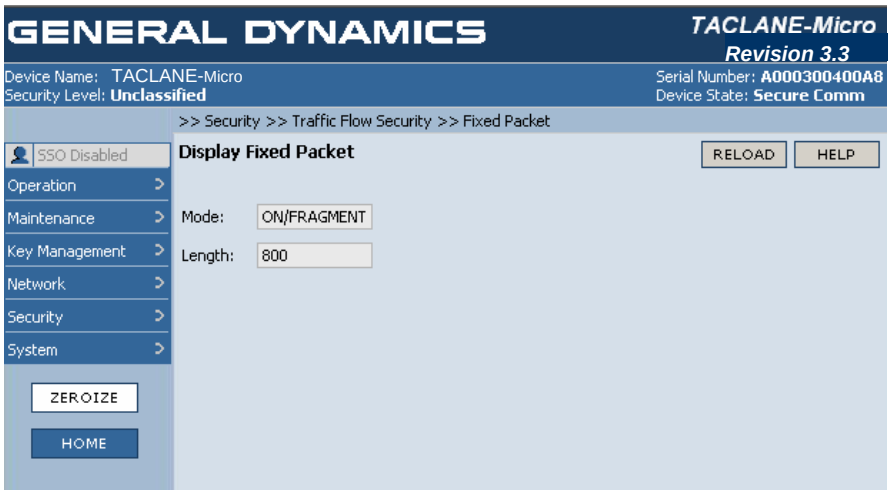
7.2 (U) Displaying Fixed Packet Length Information

Introduction

(U//FOUO) The operator can display the fixed packet length information.

Procedure

(U//FOUO) Follow these steps to display the fixed packet length information:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security => Fixed Packet Length. Result: The following screen is displayed: 

7.3 (U) Configuring Payload Sequence Number Checking

Introduction

(U//FOUO) Payload Sequence Number (PSEQN) checking can only be configured by the SSO. The purpose of sequence numbers is to facilitate identification and rejection of replayed encrypted packets. TACLANE includes a unique sequence number within each ESP datagram that it sends. When PSEQN checking is enabled at the receiving TACLANE, each sequence number is checked; packets with sequence numbers that have already been received or are so old that it cannot be determined whether they were already received are discarded.

Notes

(U//FOUO) The following notes apply to configuring PSEQN checking:

- Only the SSO has the privilege to configure PSEQN parameters
- An audit log entry is generated when the PSEQN check parameter is modified.

PSEQN Processing

(U//FOUO) TACLANE assigns a unique Payload Sequence Number to each outgoing ESP datagram. The PSEQN is located in the encrypted part of the ESP datagram so that it cannot be altered during transit. A PSEQN is always included, regardless of the setting of the PSEQN check parameter. Each Security Association (connection with a remote TACLANE) has its own series of sequence numbers, starting with 1.

(U//FOUO) Audit log entries are generated for received ESP datagrams with invalid PSEQNs.

(U//FOUO) Note: Payload sequence numbers are not checked for IP multicast packets.

PSEQN Check Parameter

(U//FOUO) The PSEQN check parameter can only be configured by the SSO. It can be either Enabled or Disabled.

(U//FOUO) It is important to note that the PSEQN check setting only affects the receive processing of encrypted traffic (CT to PT). It has no affect on the encryption and transmission of ESP datagrams.

(U//FOUO) When the PSEQN check parameter is Enabled, packets received undergo PSEQN checking and only valid (non-replayed) traffic will be accepted.

(U//FOUO) When the PSEQN check parameter is set to Disabled, no PSEQN checking is done. In this case, all ESP datagrams are considered valid regardless of PSEQN value.

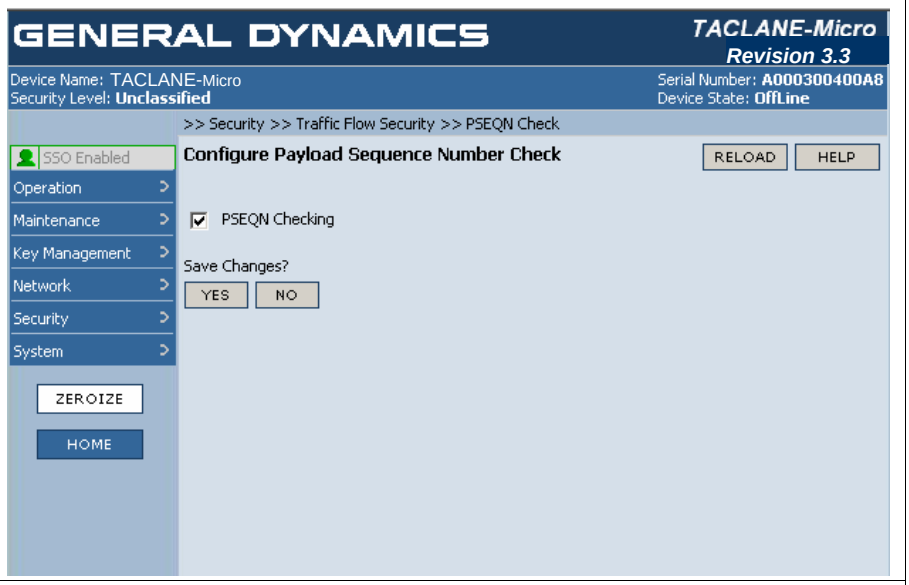
(U//FOUO) The default setting for this parameter is Enabled.

Continued on next page

(U) Configuring Payload Sequence Number Checking, continued

Procedure

(U//FOUO) Follow these steps to configure the PSEQN check parameter:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security => PSEQN Check. Result: The following screen is displayed: 
2.	Select the checkbox next to PSEQN Checking. If the box is checked, (a checkmark is present in the box) then PSEQN Checking is enabled. If the box is empty (no checkmark present in the box) then PSEQN Checking is disabled.
3.	Select YES to save the changes.

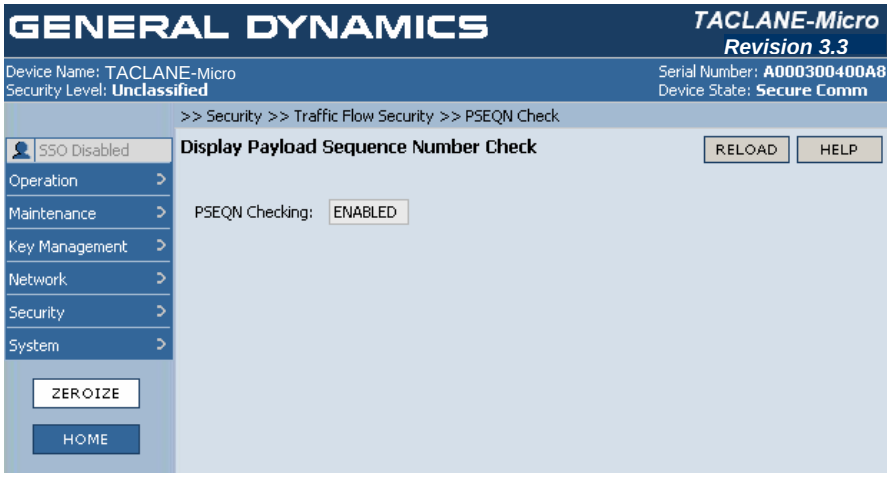
7.4 (U) Displaying Payload Sequence Number Check Information

Introduction

(U//FOUO) The operator can display the payload sequence number check information.

Procedure

(U//FOUO) Follow these steps to display the payload sequence number check information:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security => PSEQN Check. Result: The following screen is displayed: 

7.5 (U) Configuring TOS/DSCP Bypass

Introduction

(U//FOUO) The TOS bypass parameter can only be configured by the SSO. The 8-bit TOS field in the IP header consists of the 6-bit Differentiated Services (DS) field and the 2-bit Explicit Congestion Notification (ECN) field. The six bits of the DS field are used as a code point and referred to as the Differentiated Services Code Point (DSCP). The TOS bypass parameter only applies to PT-to-CT traffic and provides the TACLANE SSO the following options:

- "Enabled" – bypass (or copy) the 8-bit TOS value from PT IP header to the CT IP header. However, if the PT's 6-bit DSCP value is not one of the enabled DSCP values (see the "Accepted DSCP Values" on the HMI screen), then the TOS constant value is used.
- "Disabled" – do not bypass (or copy) the 8-bit TOS value from PT IP header to the CT IP header. Instead, always use the operator-defined TOS Constant value in the CT IP header.

Notes

(U//FOUO) The following notes apply to configuring the TOS bypass parameter:

- Only the SSO has the privilege to configure the TOS bypass parameter.
- An audit log entry is generated when the TOS bypass parameter is modified.

TOS Bypass Parameter and Processing

(U//FOUO) The TOS bypass parameter can be configured as either Enabled or Disabled. The default setting for this parameter is Disabled.

(U//FOUO) When TOS bypass is set to Enabled, the TOS value from each PT IP header is compared against the (operator-defined) Accepted DSCP Values. If the DSCP value is one of the accepted DSCP values, then it is copied to the CT IP header. If the DSCP value is not one of the accepted values, then the TOS constant value is used. Note that the bypass is from PT to CT, but not in the opposite direction.

(U//FOUO) When TOS bypass is set to Disabled, all eight bits of the TOS field in each CT IP header are set to the TOS Constant value.

(U//FOUO) The default setting for this parameter is Disabled.

Continued on next page

(U) Configuring TOS/DSCP Bypass, continued

Table of Standard DSCP Values

(U//FOUO) The following table lists the 21 standard DSCP values:

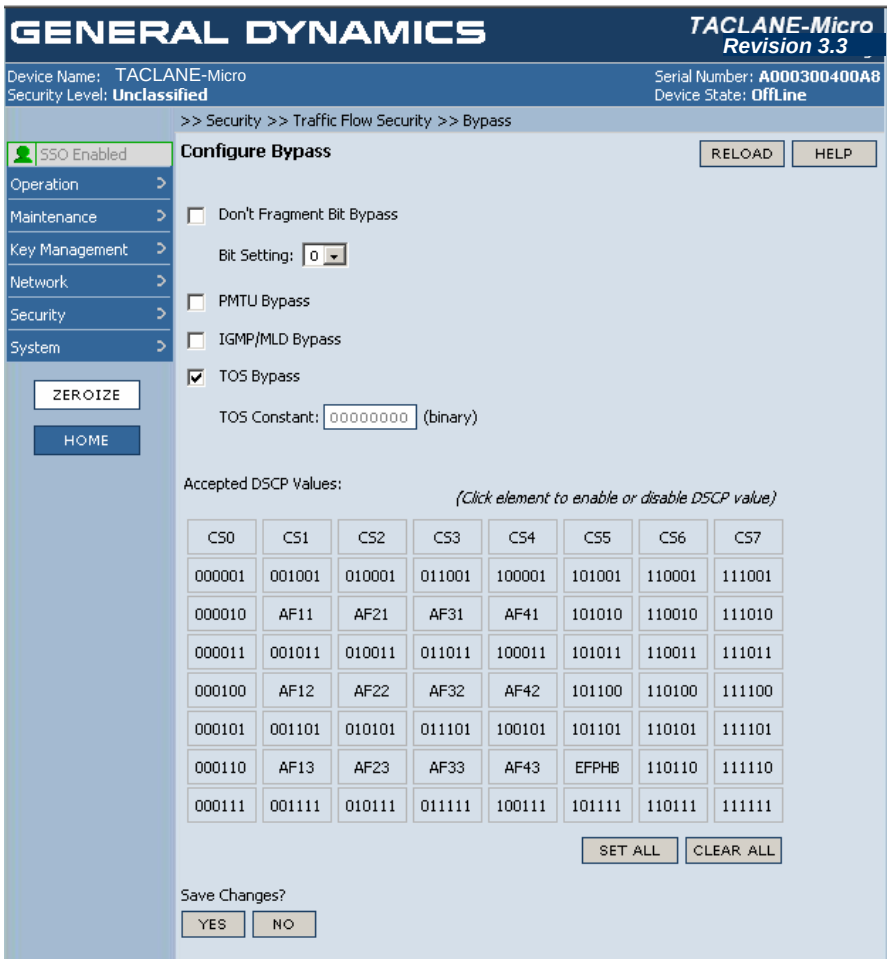
Name	DSCP Value	Reference
CS0	000000	RFC 2474
CS1	001000	RFC 2474
CS2	010000	RFC 2474
CS3	011000	RFC 2474
CS4	100000	RFC 2474
CS5	101000	RFC 2474
CS6	110000	RFC 2474
CS7	111000	RFC 2474
AF11	001010	RFC 2597
AF12	001100	RFC 2597
AF13	001110	RFC 2597
AF21	010010	RFC 2597
AF22	010100	RFC 2597
AF23	010110	RFC 2597
AF31	011010	RFC 2597
AF32	011100	RFC 2597
AF33	011110	RFC 2597
AF41	100010	RFC 2597
AF42	100100	RFC 2597
AF43	100110	RFC 2597
EFPHB	101110	RFC 3246

Continued on next page

(U) Configuring TOS/DSCP Bypass, continued

Procedure

(U//FOUO) Follow these steps to configure the TOS bypass parameter:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security => Bypass. Result: The following screen is displayed: 
2.	Select the checkbox next to TOS Bypass. If the box is checked, (a checkmark is present in the box) then TOS Bypass is enabled. If the box is empty (no checkmark present in the box) then TOS Bypass is disabled.
3.	**If TOS Bypass is disabled,** enter the 8-bit, binary constant in the TOS Constant field.
4.	**If TOS Bypass is enabled,** Select the accepted DSCP values by clicking on the applicable DSCP boxes within the table. Boxes that are highlighted are the acceptable DSCP values. SET ALL and CLEAR ALL are provided to simplify operator selection.
5.	Select YES to save changes.

7.6 (U) Configuring Don't Fragment (DF) Bit Bypass

Introduction

(U//FOUO) When the TACLANE processes a packet on the PT side, it must determine whether to send the packet, fragment the packet, or discard the packet. If the packet is sent or forwarded, it must determine what to set for the DF bit for the CT IP header. The DF Bit bypass parameter can be configured by the TACLANE SSO operator to be:

- "Disabled" – always sets the DF bit in the CT IP header to the Bit Setting parameter value.
- "Enabled" – bypasses or copies the incoming DF bit value to the CT IP header DF bit value.

(U//FOUO) The default setting for this parameter is Disabled.

(U//FOUO) The DF Bit bypass parameter can only be configured by the SSO.

Notes

(U//FOUO) The following notes apply to configuring the DF Bit bypass parameter:

- Only the SSO has the privilege to configure the DF Bit bypass parameter.
- An audit log entry is generated when the DF Bit bypass parameter is modified.

DF Bit Bypass Parameter and Processing

(U//FOUO) The DF Bit bypass parameter can be configured as either Enabled or Disabled. The default setting for this parameter is Disabled. Note that the bypass is from PT to CT, but not in the opposite direction.

(U//FOUO) When the DF Bit bypass is set to Disabled, the DF bit in the CT IP header is always set to the value in the Bit Setting parameter.

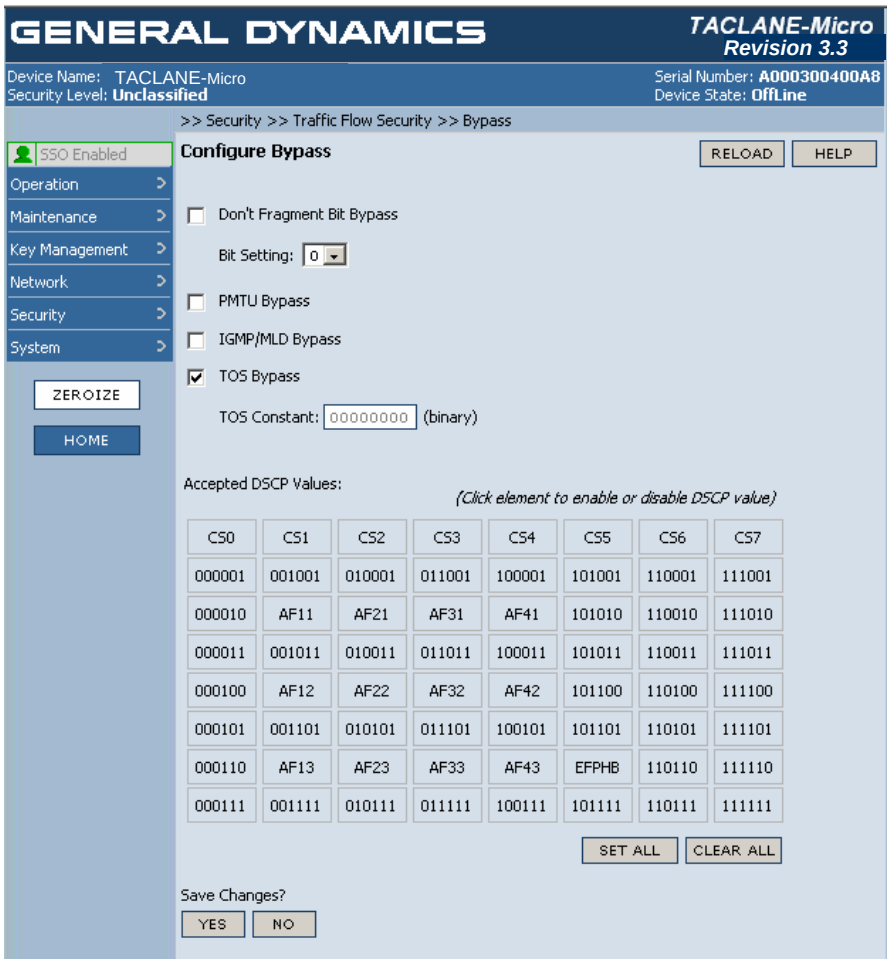
(U//FOUO) When the DF Bit bypass is set to Enabled, the DF bit in the CT IP header is set to the incoming DF bit value (bypass).

Continued on next page

(U) Configuring Don't Fragment (DF) Bit Bypass, continued

Procedure

(U//FOUO) Follow these steps to configure the DF Bit bypass parameter:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security =>Bypass. Result: The following screen is displayed: 
2.	Select the checkbox next to Don't Fragment Bit Bypass. If the box is checked, (a checkmark is present in the box) then Don't Fragment Bit Bypass is enabled. If the box is empty (no checkmark present in the box) then Don't Fragment Bit Bypass is disabled.
3.	If Don't Fragment Bit Bypass is disabled, select the Bit Setting value from the Bit Setting pull down menu.
4.	Select YES to save changes.

7.7 (U) Configuring PMTU Bypass

Introduction

(U//FOUO) The TACLANE supports a Path Maximum Transfer Unit (PMTU) discovery function that, if enabled, can help to avoid fragmentation over the CT network. The TACLANE's Path Maximum Transfer Unit (PMTU) Bypass parameter can be configured by the SSO to be either Enabled or Disabled.

(U//FOUO) If the TACLANE's PMTU Bypass parameter is set to Enabled, when the TACLANE receives an ICMP Destination Unreachable message (indicating fragmentation is needed) on its CT interface, the TACLANE will update its PMTU.

(U//FOUO) If the TACLANE's PMTU Bypass parameter is set to Disabled, when the TACLANE receives an ICMP Destination Unreachable message (indicating fragmentation is needed) on its CT interface, the TACLANE will discard the message.

(U//FOUO) The PMTU bypass parameter can only be configured by the SSO.

Notes

(U//FOUO) The following notes apply to configuring the PMTU Bypass parameter:

- Only the SSO has the privilege to configure the PMTU bypass parameter.
- An audit log entry is generated when the PMTU bypass parameter is modified.

PMTU Bypass Parameter and Processing

(U//FOUO) If the PMTU Bypass is Enabled, when the TACLANE receives an ICMP Destination Unreachable message (indicating fragmentation is needed) on its CT interface, the TACLANE will update its PMTU.

(U//FOUO) If the PMTU Bypass is Disabled, when the TACLANE receives an ICMP Destination Unreachable message (indicating fragmentation is needed) on its CT interface, the TACLANE will discard the message.

(U//FOUO) The default setting for this parameter is Disabled.

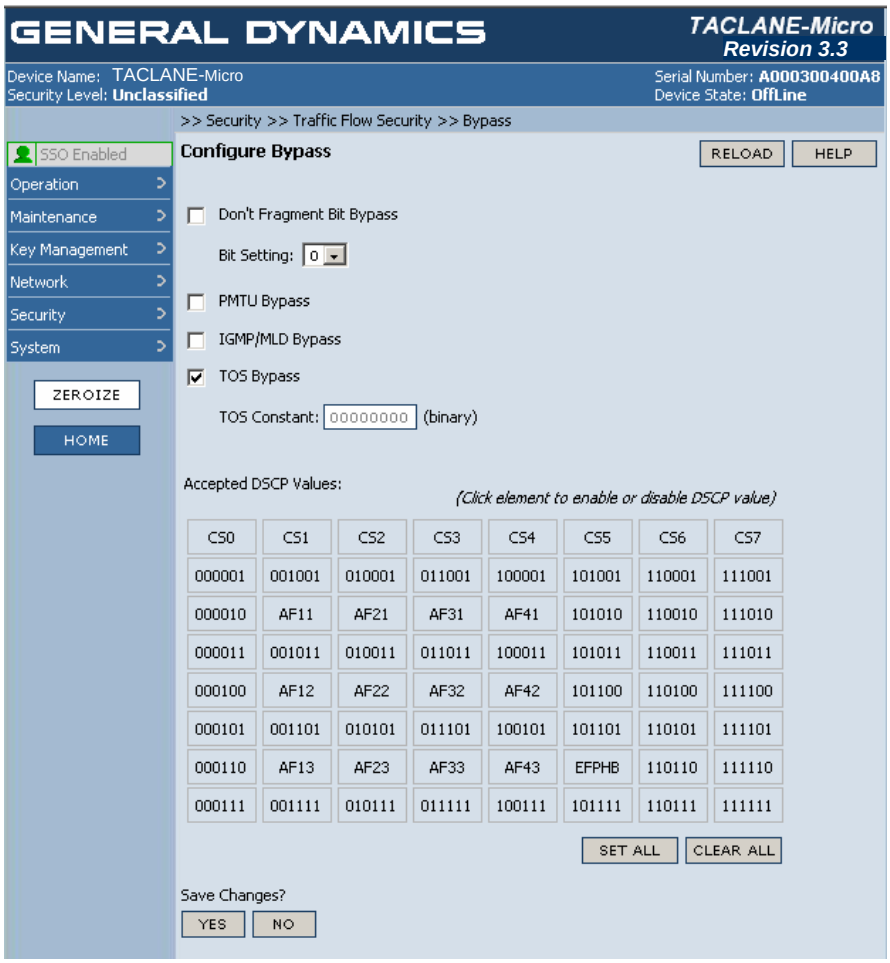
(U//FOUO) ICMP messages received through the PT interface (and not destined for the TACLANE's PT IP address) are encrypted and treated as user traffic.

Continued on next page

(U) Configuring PMTU Bypass, continued

Procedure

(U//FOUO) Follow these steps to configure the PMTU Bypass parameter:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security =>Bypass. Result: The following screen is displayed: 
2.	Select the checkbox next to PMTU Bypass. If the box is checked, (a checkmark is present in the box) then PMTU Bypass is enabled. If the box is empty (no checkmark present in the box) then PMTU Bypass is disabled.
3.	Select YES to save changes.

7.8 (U) Configuring IGMP/MLD Bypass

Introduction

(U//FOUO) The Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD) is the protocol used by IPv4 systems to report their IP multicast group memberships to neighboring multicast routers. IGMP messages provide IP multicast message delivery to host group IP addresses (224.0.0.0 to 239.255.255.255).

(U//FOUO) The TACLANE's IGMP/MLD Bypass parameter, configurable as Enabled or Disabled, determines whether the TACLANE will regenerate IGMP traffic for user multicast traffic.

Notes

(U//FOUO) The following notes apply to configuring the IGMP/MLD bypass parameter:

- Only the SSO has the privilege to configure the IGMP bypass parameter.
- An audit log entry is generated when the IGMP bypass parameter is modified.

IGMP Bypass Parameter and Processing

(U//FOUO) When the IGMP/MLD Bypass is Enabled, the TACLANE does not encrypt PT IGMP messages as user multicast traffic, but instead regenerates the IGMP messages on the CT side. When the IGMP/MLD Bypass is Enabled, the TACLANE regenerates user IGMP messages traveling from both CT-to-PT as well as from PT-to-CT.

(U//FOUO) When the IGMP/MLD Bypass is Disabled, the TACLANE does not participate in the IGMP protocol. It treats all PT IGMP messages from the PT network as user multicast traffic to be encrypted. And, the TACLANE treats all IGMP messages from the CT network as user multicast traffic to be decrypted. Therefore, IGMP PDUs received on the CT interface that are not encapsulated in ESP will be discarded.

(U//FOUO) The default for the IGMP/MLD Bypass parameter is Disabled.

(U//FOUO) Setting the IGMP/MLD Bypass parameter to Enabled is necessary for cooperation with multicast router(s) located in the CT network. Refer to Appendix B of the Operator's Manual for more details on IGMP configuration.

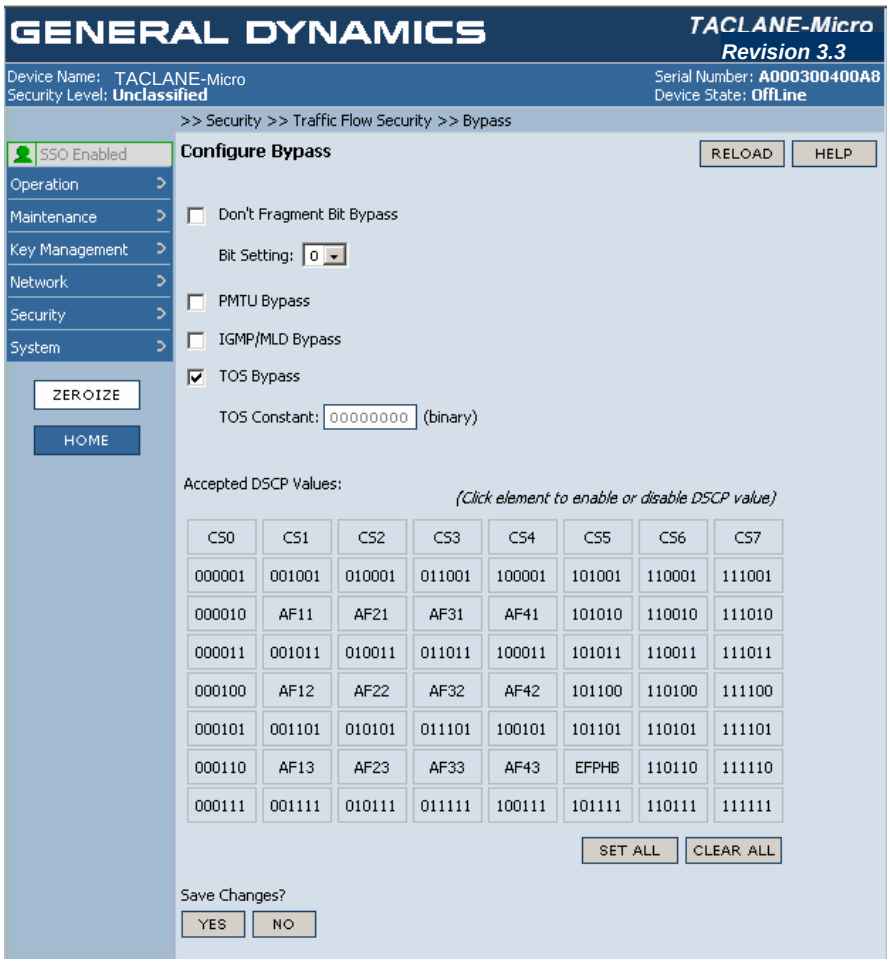
(U//FOUO) Note that the TACLANE also supports IGMP on the CT side in order to support the HAIPE IS Secure Dynamic Discovery (SDD) multicast traffic. The IGMP Bypass parameter, however, has no affect on the TACLANE's IGMP support for SDD traffic. Regardless of whether the IGMP/MLD Bypass parameter is Enabled or Disabled, the TACLANE will support IGMP for SDD traffic whenever the SDD multicast group is configured (i.e., assigned to the SDD PPK).

Continued on next page

(U) Configuring IGMP/MLD Bypass, continued

Procedure

(U//FOUO) Follow these steps to configure the IGMP bypass parameter:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security =>Bypass. Result: The following screen is displayed: 
2.	Select the checkbox next to IGMP/MLD Bypass. If the box is checked, (a checkmark is present in the box) then IGMP/MLD Bypass is enabled. If the box is empty (no checkmark present in the box) then IGMP/MLD Bypass is disabled.
3.	Select YES to save changes.

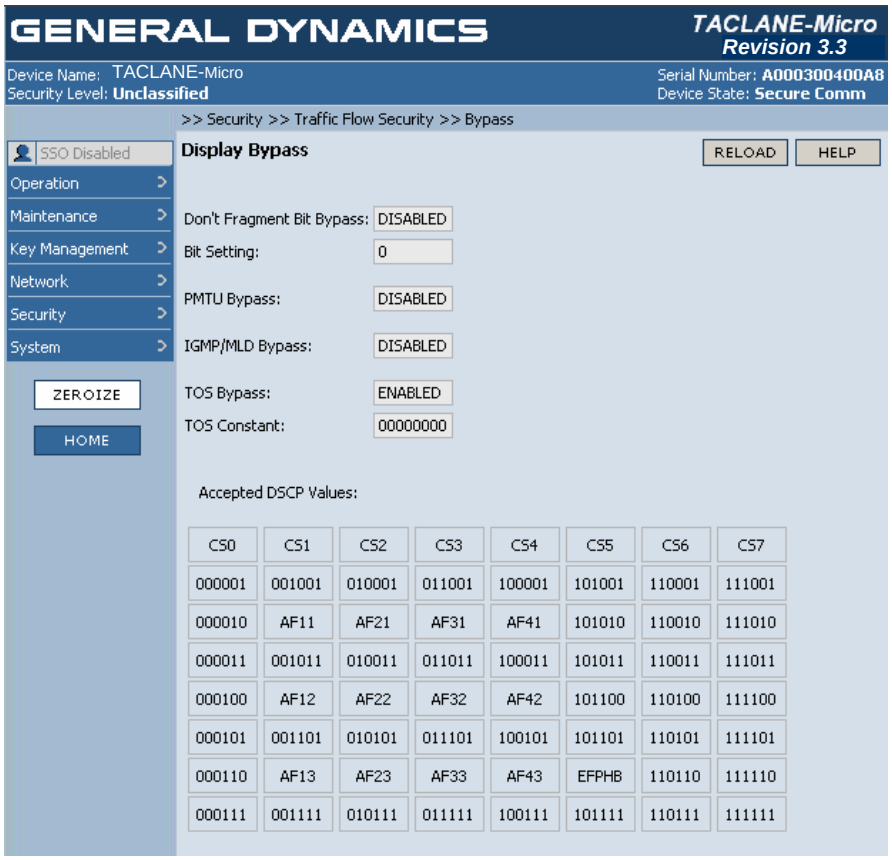
7.9 (U) Displaying Bypass Information

Introduction

(U//FOUO) The operator can display the bypass information.

Procedure

(U//FOUO) Follow these steps to display the bypass information:

Step	Action
1.	From the MAIN MENU, select Security => Traffic Flow Security => Bypass. Result: The following screen is displayed: 

8.0 (U) CONFIGURING ACCESS CONTROL AND THE NETWORK MANAGER

8.1 (U) Enable/Disable Access Mode

Introduction

(U//FOUO) TACLANE access mode can be enabled or disabled by the SSO operator. The access mode check only applies to security associations using FIREFLY TEKs.

(U//FOUO) When disabled, all security associations using FIREFLY TEKs that pass mandatory access control checks are allowed.

(U//FOUO) When enabled, this additional access mode check is performed: Only security associations using FIREFLY TEKs created using remote FIREFLY vector sets with KMIDs on the Access Control List (ACL) are allowed. (See "Creating an ACL Entry.")

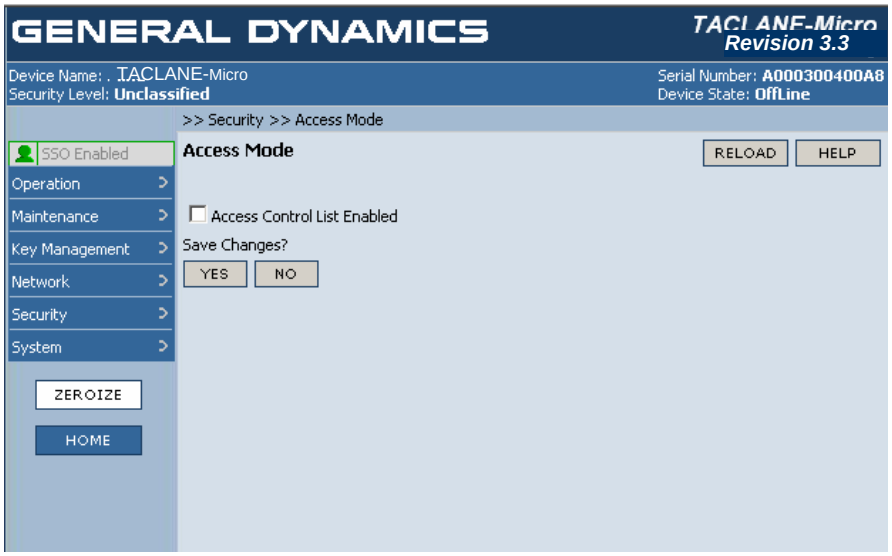
Notes

(U//FOUO) The following notes apply to enable or disable access mode:

- Only the SSO has the privilege to configure the access mode.
- Access mode is disabled by default.

Procedure

(U//FOUO) Follow these steps to enable or disable access mode:

Step	Action
1.	From the MAIN MENU, select Security => Access Mode. Result: The following screen is displayed: 

(U) Enable/Disable Access Mode, continued

Procedure (continued)

Step	Action
2.	Select the checkbox next to Access Control List Enabled. If the box is checked, (a checkmark is present in the box) then ACL is enabled. If the box is empty (no checkmark present in the box) then ACL is disabled.
3.	Select YES to save changes.

8.2 (U) Creating an ACL Entry

Introduction

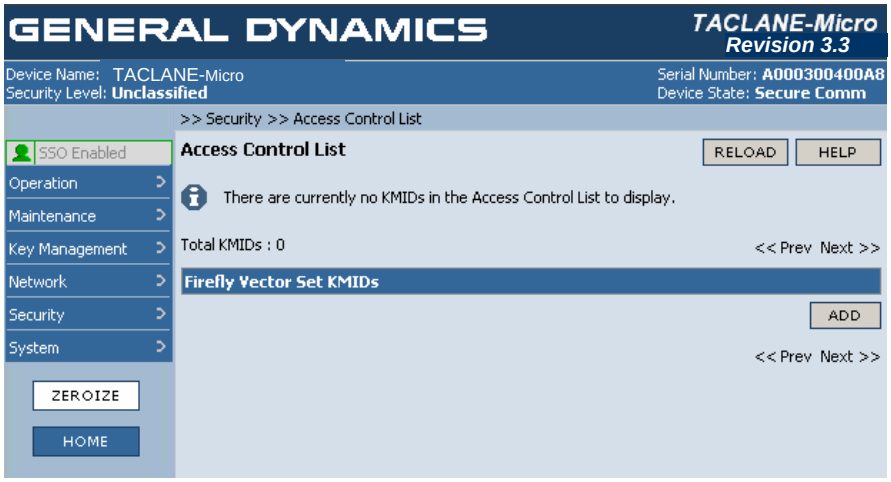
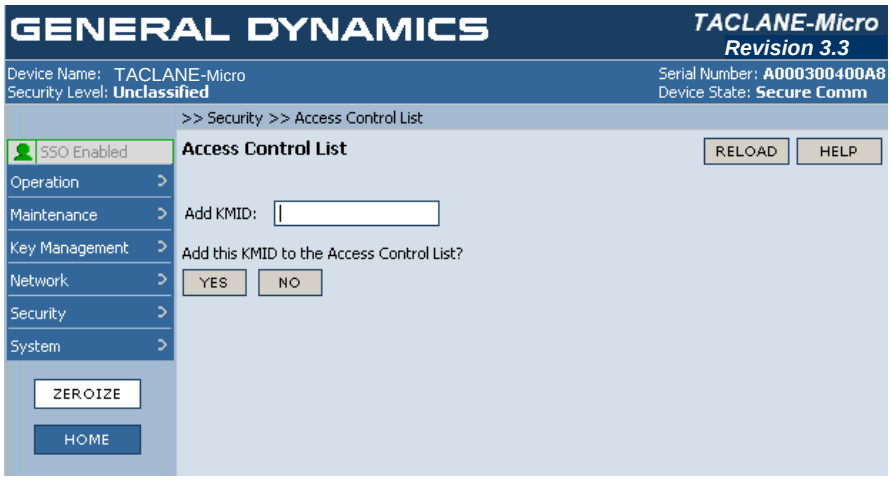
(U//FOUO) The SSO operator can create Access Control List (ACL) entries. The ACL consists of a list of up to 256 KMIDs. These KMIDs are associated with remote FIREFLY vector sets. When discretionary access control is enabled, only security associations associated with remote FIREFLY vector sets with KMIDs on the ACL are allowed. (See "Enable/Disable Access Mode") There is one ACL and it applies to all security levels.

Notes

(U//FOUO) The following notes apply to creating an ACL entry:

- Only the SSO has the privilege to configure an ACL entry.
- There is one ACL and it applies to all security levels.
- The ACL is limited to a maximum of 256 entries.

Procedure (U//FOUO) Follow these steps to create an ACL entry:

Step	Action
1.	From the MAIN MENU, select Security => Access Control List. Result: The following screen is displayed: 
2.	Select ADD. Result: The following screen is displayed: 
3.	Enter the KMID value. Note: The KMIDs must be unique for each ACL entry.
4.	Select YES to save the ACL entry.

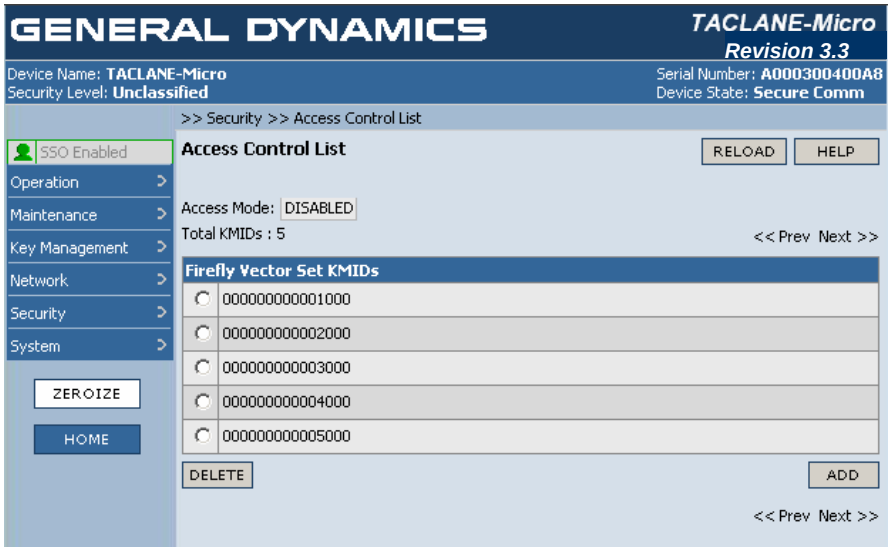
8.3 (U) Deleting Access Mode and ACL Entries

Introduction

(U//FOUO) The SSO operator can delete Access Control List (ACL) entries. The ACL consists of a list of up to 256 KMIDs. These KMIDs are associated with remote FIREFLY vector sets.

Procedure

(U//FOUO) Follow these steps to delete an ACL entry:

Step	Action
1.	From the MAIN MENU, select Security => Access Control List. Result: The following screen is displayed: 
2.	Select the radio button next to the ACL entry to be deleted.
3.	Select DELETE to delete the ACL entry.

8.4 (U) Display an ACL Entry

Introduction

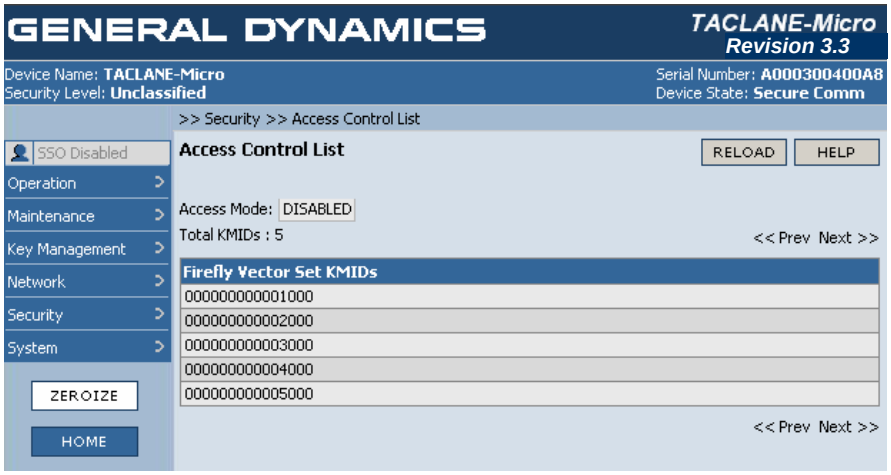
(U//FOUO) The operator can display Access Control List (ACL) entries. The ACL consists of a list of up to 256 KMIDs (see previous section for how to create these ACL entries). The KMIDs are associated with remote FIREFLY vector sets.

Notes

(U//FOUO) Displaying the ACL information is not limited to the SSO. The ACL information may be displayed in the initialized, offline or secure comm mode.

Procedure

(U//FOUO) Follow these steps to display the ACL:

Step	Action
1.	From the MAIN MENU, select Security => Access Control List. Result: The following screen is displayed: 

8.5 (U) Configuring the Network Manager

Introduction

(U//FOUO) The SSO operator can configure the TACLANE to be managed by a remote network manager. The operator can configure up to nine network managers. For each manager, the SSO operator configures the following parameters:

- manager name
- password.

(U//FOUO) For each manager, the SSO operator may configure the following notification (traps) parameters:

- Enable/Disable (defaulted to Enable)
- PT or CT side of the TACLANE with which the remote manager interfaces
- IP address of the remote manager
- Port number (defaulted to 162).

CT vs. PT Side Management

(U//FOUO) A TACLANE can be managed from either its Plaintext (PT) or Ciphertext (CT) interface. CT-side management traffic is encrypted between the TACLANE fronting the GEM X and the managed TACLANE. PT-side management traffic is not encrypted; it is intended to be used only to manage the TACLANE fronting the GEM X.

Network Managers

(U//FOUO) The following notes apply to the network managers:

- The TACLANE supports up to 9 network managers.
- ManagerX, where 'X' equals the current number of SNMP managers currently configured for the ECU, plus one, is the default manager name for each SNMP manager.
- The TACLANE will not have default Network Managers.
- The local HMI operator needs to configure at least 1 Network Manager to enable remote management. The same Network Manager Name and password must be defined at a Security Manager Workstation before the TACLANE can be managed by that Network Manager from the Security Manager Workstation.

Continued on next page

(U) Configuring the Network Manager, continued

Secure Remote Management Using SNMP

(U//FOUO) TACLANEs can be managed by GEM X using SNMPv3 using the portions of the standard MIBs listed below:

- RFC 1213
  - System Group
- RFC 1573
  - Interfaces Group
  - IP Group (IP address table only).

(U//FOUO) GEM X provides remote security management of TACLANEs using the TACLANE Enterprise MIB. Services for TACLANEs include:

- TACLANE discovery (When configured to do so, a TACLANE automatically attempts to contact its authorized manager upon startup.)
- IP PPK assignments
- Audit data upload (TACLANE can store a maximum of 2,048 audit entries)
- Remote TACLANE static routing table download
- Changing the system date and time for TACLANEs
- Remote online/offline/restart control
- Trap management (TACLANE sends audit data exceeds threshold and low battery SNMP traps)
- Configuring an Access Control List (ACL), which is a list of up to 256 KMIDs with which the TACLANE can set up security associations.

(U//FOUO) GEM X also provides network management of TACLANE-protected network elements using SNMPv3. Please refer to the appropriate GEM X Operator's Manual for more information on configuring the TACLANE fronting the GEM X and for more information on GEM X.

Notes

(U//FOUO) The following notes apply to a local HMI operator configuring the network manager parameters:

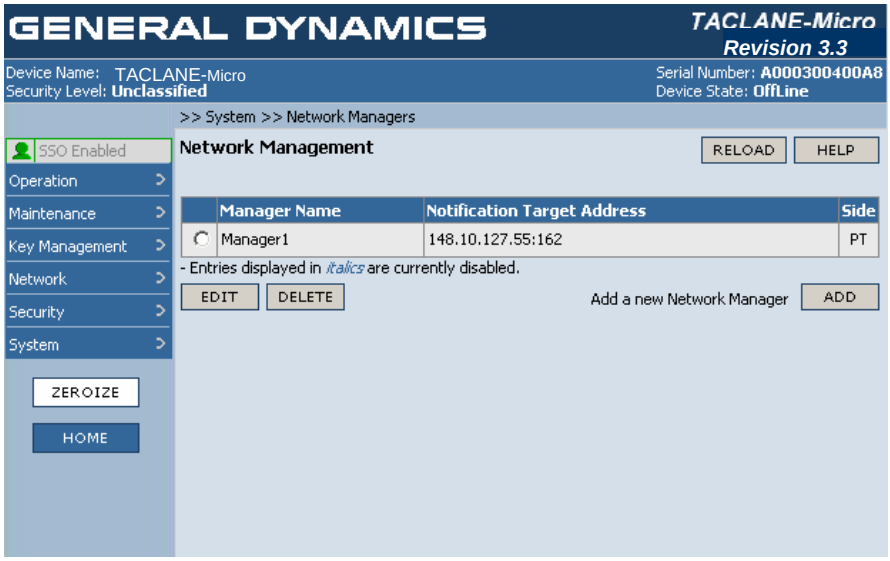
- Only the SSO can configure a network manager.

Continued on next page

(U) Configuring the Network Manager, continued

Procedure

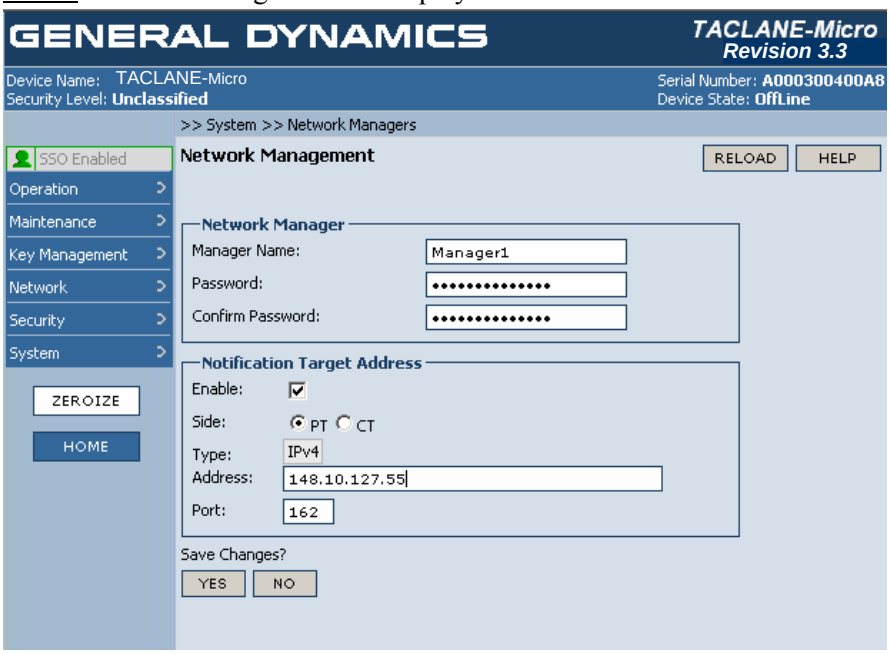
(U//FOUO) Follow these steps to configure the network manager:

Step	Action
1.	From the MAIN MENU, select System => Network Managers. Result: The following screen is displayed: 

Continued on next page

(U) Configuring the Network Manager, continued

Procedure (continued)

Step	Action
2.	**To define the network manager**, select ADD. **To modify the network manager**, select the radio button next to the desired network manager and select EDIT. Result: The following screen is displayed: 
3.	Enter or update the Manager Name and Password. Note the Manager name cannot be changed when modifying a Network Manager.
4.	Notification Target is a term used to describe a management station that will receive traps from this ECU. To configure TACLANE to send TRAPs to this manager, select to enable the Notification Target Address (this is the default), select the interface communicating to the network manager, and enter the Notification Target IP Address. Optionally, the UDP port that TRAPS will be sent to may be changed from the standard 162, to an alternate port.
5.	Select YES to save changes.

8.6 (U) Deleting the Network Manager

Introduction

(U//FOUO) The operator can delete the network manager configuration information.

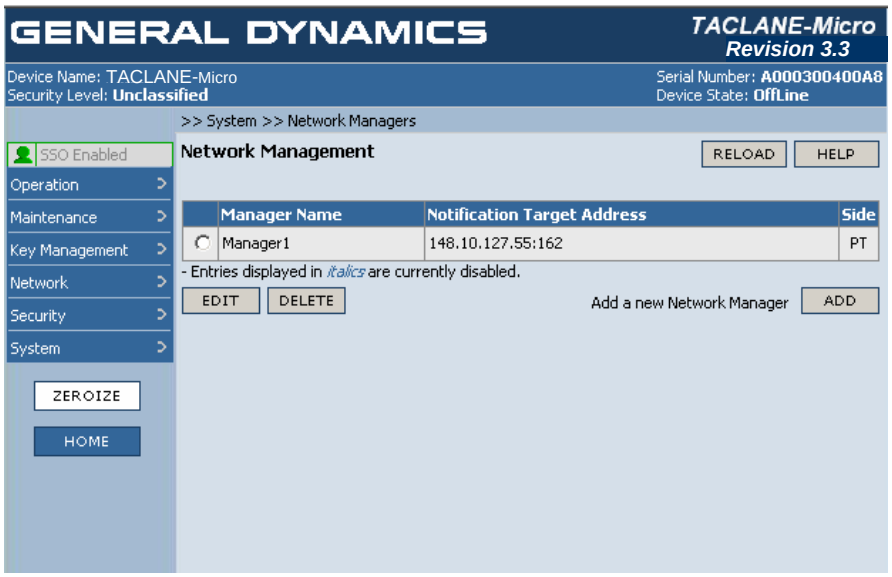
Notes

(U//FOUO) The following notes apply to deleting the network manager:

- Only the SSO can perform this function.

Procedure

(U//FOUO) Follow these steps to delete the network manager:

Step	Action
1.	From the MAIN MENU, select System => Network Managers. Result: The following screen is displayed: 
2.	Select the radio button next to the desired Network Manager and select DELETE.

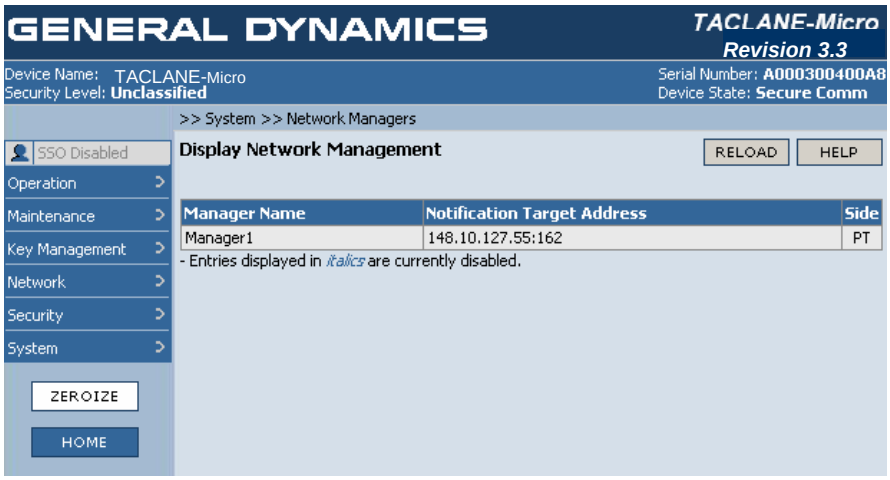
8.7 (U) Displaying Network Manager Information

Introduction

(U//FOUO) The operator can display the information associated with the network manager configuration.

Procedure

(U//FOUO) Follow these steps to display the network manager information:

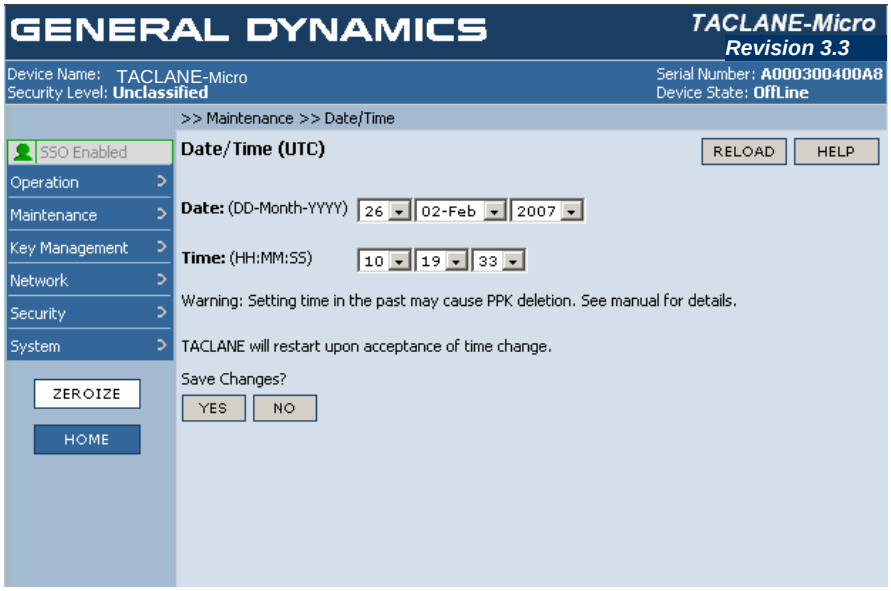
Step	Action
1.	From the MAIN MENU, select System => Network Managers. Result: The following screen is displayed:  Note: Specific values depend on the particular configuration. Note: Entries displayed in *italics* are currently disabled.

9.0 (U) MAINTAINING TACLANE

9.1 (U) Setting the Date and Time

Introduction	(U//FOUO) The SSO operator can set the TACLANE date and time.
Note	(U//FOUO) All communicating TACLANEs must have their date and time set within 55 minutes of each other to ensure that no communications blackout periods occur. Only the SSO can access this command.
Clock Drift	(U//FOUO) Nominal TACLANE clock drift is maximum 2 min./month. TACLANE date and time should be checked for accuracy at least once every 6 months and adjusted if needed.
Setting the Date and Time by Remote Manager	(U//FOUO) The Remote Manager can remotely change the system date and time.

Procedure (U//FOUO) Follow these steps to set the date and time:

Step	Action
1.	From the MAIN MENU, select Maintenance => Date/Time. Result: The following screen is displayed: 
2.	Select the desired day, month and year from the pull down menus. Select the desired hour, minute and seconds from the pull down menus. Note: Changing the time ahead may expire and automatically delete PPKs. Changing the time backwards may cause a PPK to not be used until the date catches up with the PPK's update count.
3.	Select YES to save changes. Note: This will cause the TACLANE to restart.

9.2 (U) Creating a CIK

Introduction

(U//FOUO) A CIK is a Crypto Ignition Key used to unlock wrapped key stored within the TACLANE. A TACLANE from the factory comes with one valid user CIK (shipped separately) as well as one spare CIK. The operator can use the Create CIK function to create up to two additional CIKs.

Create CIK (Make a Copy)

(U//FOUO) A spare blank CIK is included with the TACLANE. General Dynamics recommends that the operator use this spare CIK to create a second user CIK. The original user CIK should be tagged and kept in a safe place. The second user CIK should then be used instead of the original user CIK for normal TACLANE operation.

Important CIK Notes

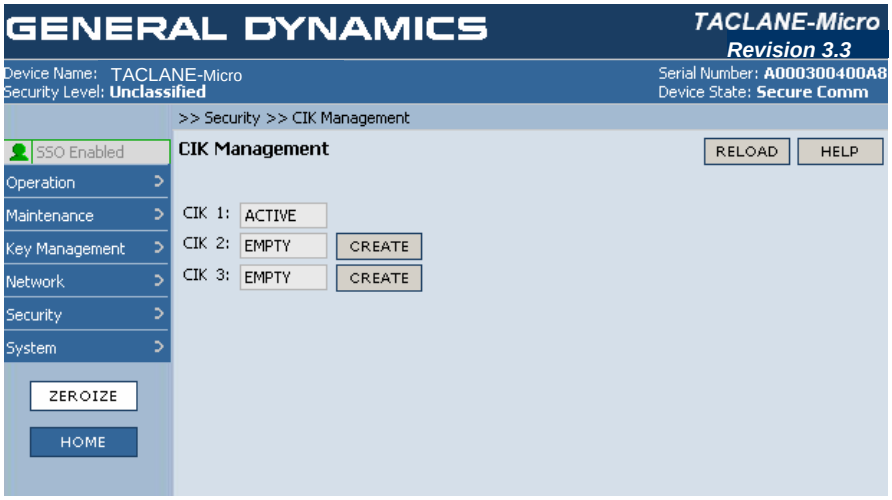
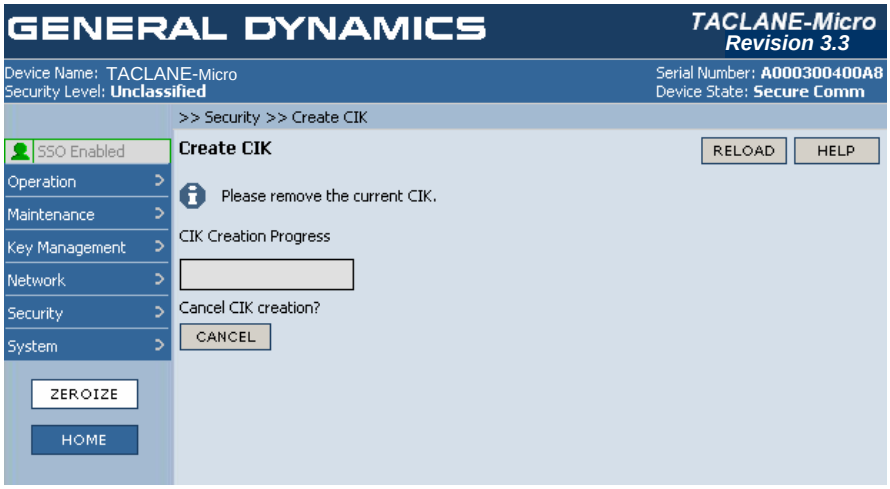
(U//FOUO) The CIK snaps into place when inserted. It is recommended that the CIK not have additional weight, such as a key ring, connected to it when installed in the TACLANE.

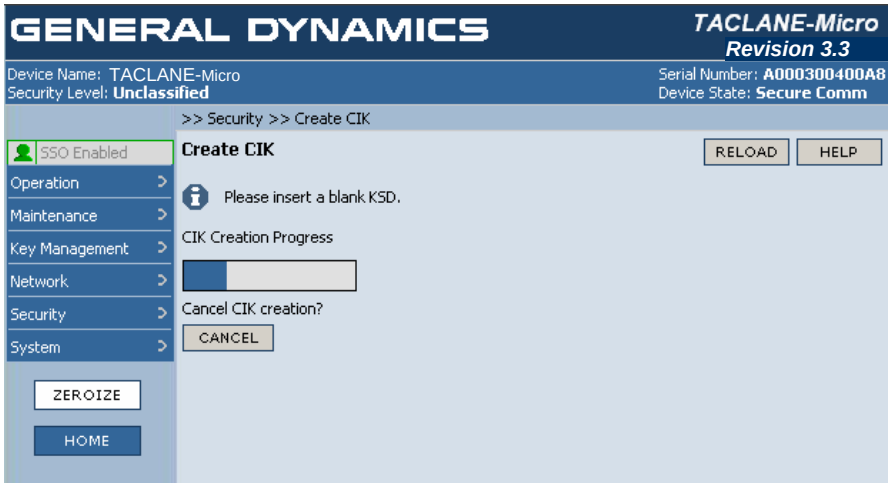
Notes

(U//FOUO) The following notes apply to creating a CIK:

- Only the SSO has the privilege to create a CIK
- Up to two additional CIKs may be created (three total)
- CIKs already associated with this TACLANE-Micro will be detected, so that they will not be destroyed. **Warning: CIKs associated with other TACLANE-Micros will be overwritten if used to create a CIK.**
- The operator has five minutes to complete the CIK creation. If the CIK creation is not completed within five minutes, the TACLANE resets automatically.

Procedure (U//FOUO) Follow these steps to create a CIK:

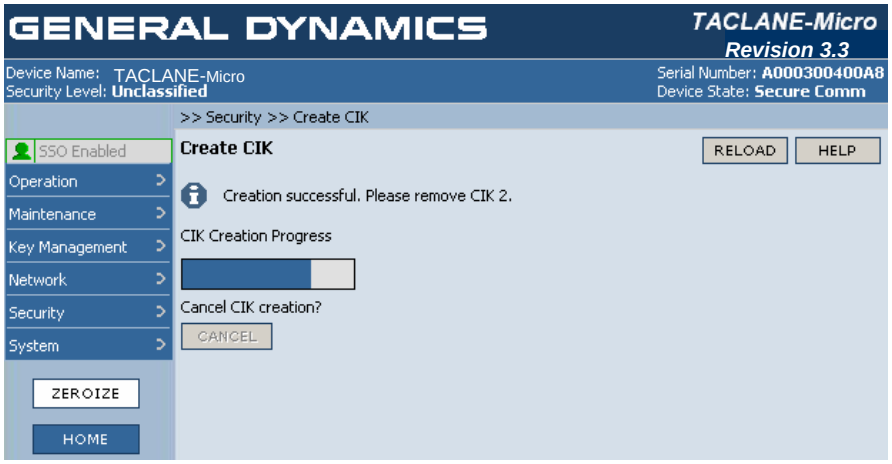
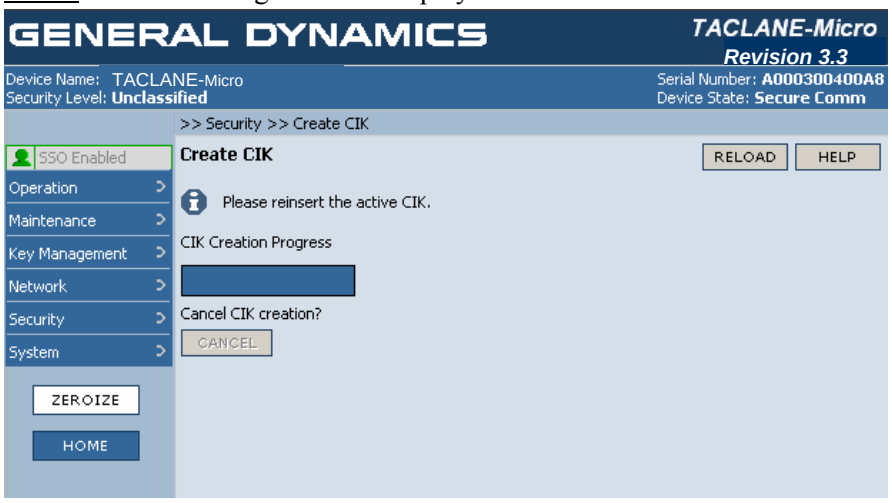
Step	Action
1.	From the MAIN MENU, select Security => CIK Management. Result: The following screen is displayed: 
2.	Select CREATE next to the CIK to be created. Result: The following screen is displayed:  Note: If the CIK create is not completed within five minutes, the TACLANE automatically restarts.

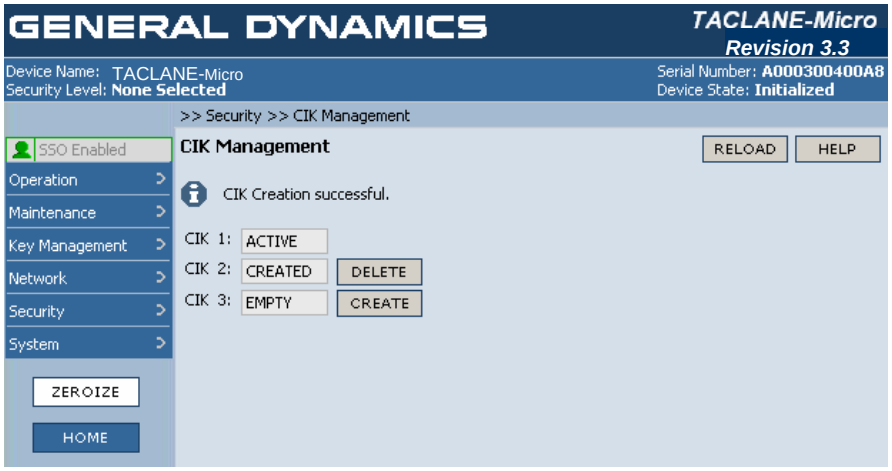
3.	Remove the CIK from the TACLANE. Result: The following screen is displayed: 

Continued on next page

(U) Creating a CIK, continued

Procedure (continued)

Step	Action
4.	Insert a blank CIK. Result: The following screen is displayed: 
5.	Remove the CIK from the TACLANE-Micro. Result: The following screen is displayed: 

6.	Insert the active CIK. Result: The following screen is displayed: 

9.3 (U) Deleting a CIK

Introduction

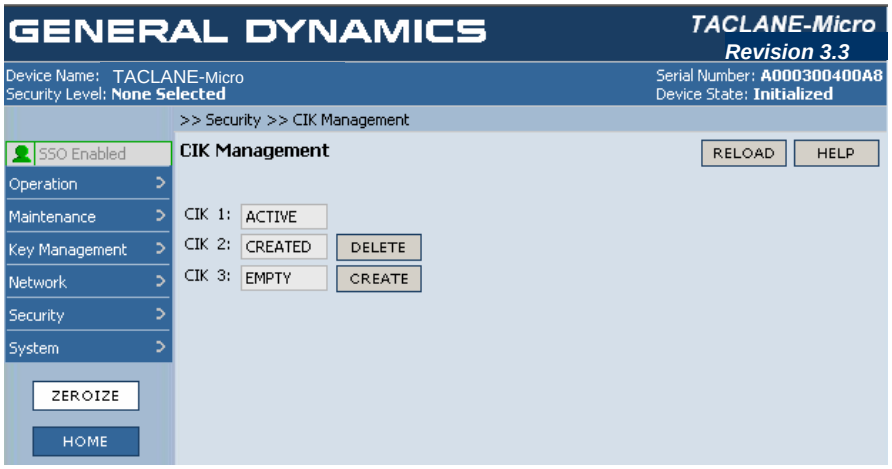
(U//FOUO) The SSO operator can delete a User CIK.

Notes

(U//FOUO) The following notes apply to deleting a CIK:

- Only the SSO has the privilege to delete a CIK
- A CIK may not delete itself
- The active CIK cannot be deleted.

Procedure (U//FOUO) Follow these steps to delete a CIK:

Step	Action
1.	From the MAIN MENU, select Security => CIK Management. Result: The following screen is displayed: 
2.	Select DELETE next to the CIK to be deleted.

9.4 (U) Displaying CIK Information

Introduction (U//FOUO) The operator can display the CIK configuration information.

Procedure (U//FOUO) Follow these steps to display the CIK information:

The display capabilities have been integrated with the create capabilities. See section 9.2.

9.5 (U) Restarting the TACLANE

Introduction

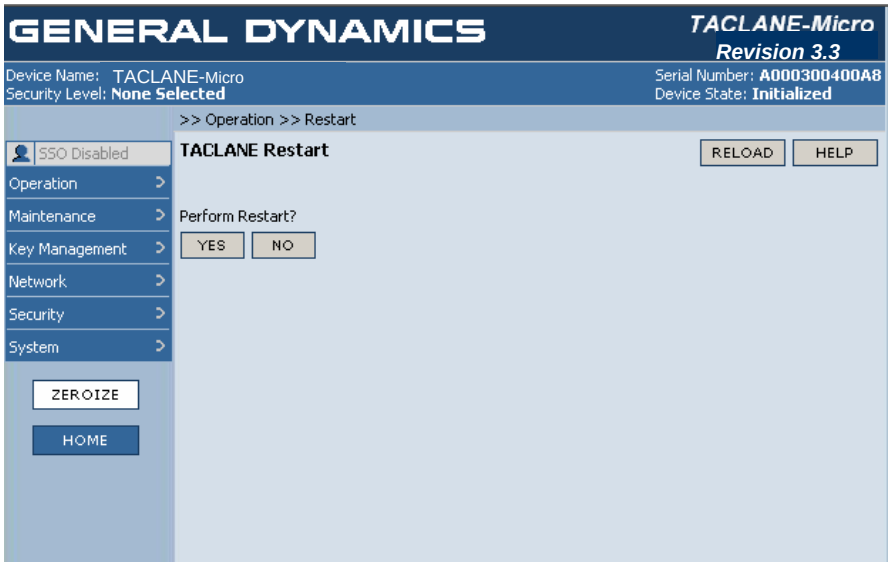
(U//FOUO) The operator can restart the TACLANE. Restarting the TACLANE will cause the TACLANE to perform a series of diagnostic tests.

Note

(U//FOUO) All security associations are lost on a restart.

Procedure

(U//FOUO) Follow these steps to restart the TACLANE:

Step	Action
1.	From the MAIN MENU, select Operation => Restart. Result: The following screen is displayed: 
2.	Select YES to perform the restart.

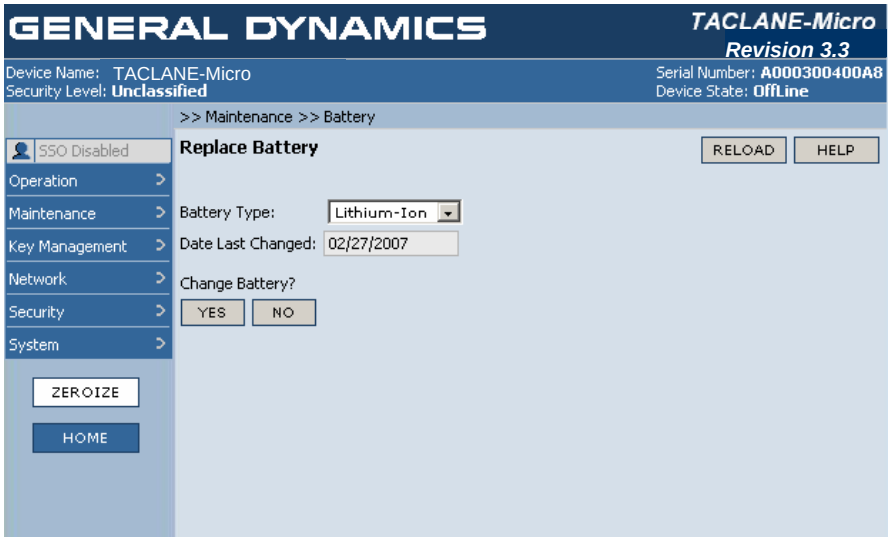
9.6 (U) Configure Battery Configuration

Introduction

(U//FOUO) The operator can configure the type of battery used in the TACLANE-Micro.

Procedure

(U//FOUO) Follow these steps to configure the battery:

Step	Action
1.	From the MAIN MENU, select Maintenance => Battery. Result: The following screen is displayed: 
2.	Select the battery type from the Battery Type pull-down menu. Note: The Date Last Changed displays the current date as the date that the battery was changed.
3.	Select YES to save changes.

9.7 (U) Displaying Battery Installed Date and Type

Introduction

(U//FOUO) The operator can display the type of battery and the date on which the battery was installed.

Procedure

(U//FOUO) Follow these steps to display the battery installed date and type:

The display capabilities have been integrated with the configure capabilities. See section 9.6.

9.8 (U) Configuring Download Servers

Introduction

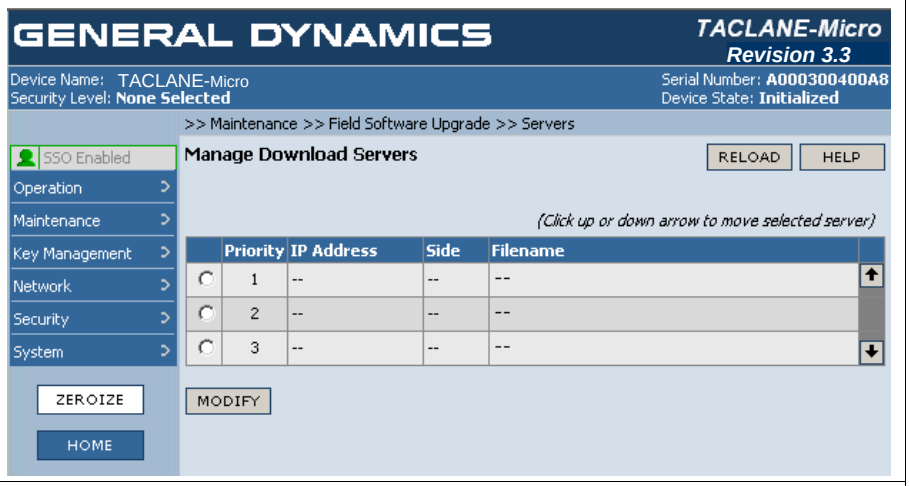
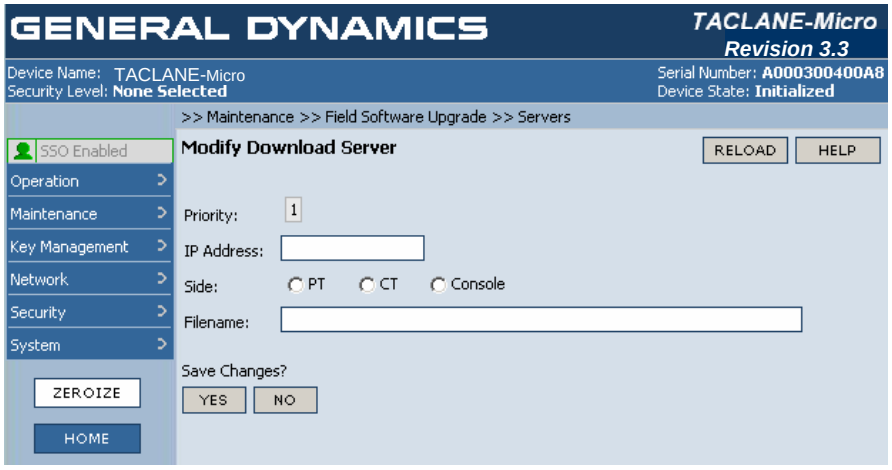
(U//FOUO) The operator can configure up to three FSU download servers.

Important Notes

(U//FOUO) The following notes apply to configuring FSU download servers:

- Only the SSO can access this command
- The download servers cannot be modified if an FSU download is in process
- The download servers are listed in order of use during FSU (i.e., download server with Priority = 1 is attempted first, followed by download server with Priority = 2, etc).

Procedure (U//FOUO) Follow these steps to configure FSU download servers:

Step	Action
1.	From the MAIN MENU, select Maintenance => Field Software Upgrade => Servers. Result: The following screen is displayed: 
2.	Select the radio button next to the desired download server. Select MODIFY to configure the FSU download server. Result: The following screen is displayed: 
3.	Enter the IP Address of the download server, the side with which the download server interfaces the TACLANE, and the Filename of the FSU file on the download server (including any path information). Note: The file name including the path information must be 231 or fewer characters.
4.	Select YES to save changes.

9.9 (U) Delete Download Servers

Introduction

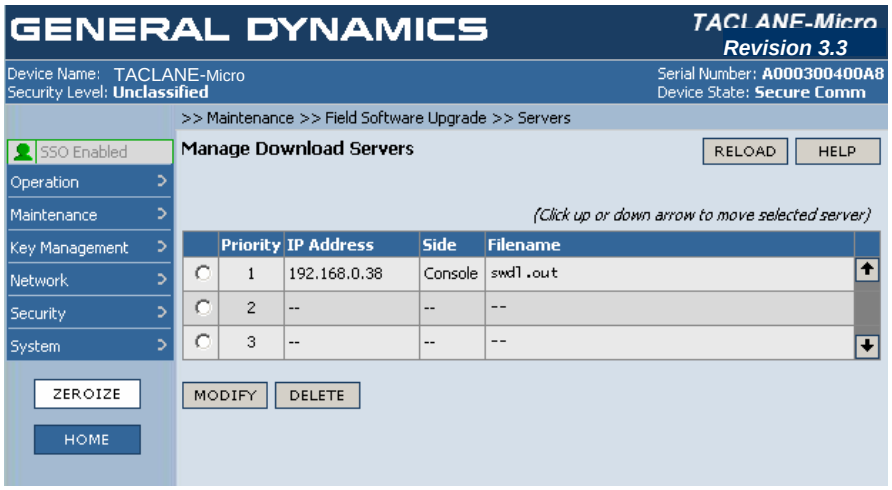
(U//FOUO) The operator can delete an FSU download server.

Important Notes

(U//FOUO) The following notes apply to deleting FSU download servers:
- Only the SSO can access this command
- A download server cannot be deleted if an FSU download is in process.

Procedure

(U//FOUO) Follow these steps to deleting an FSU download servers:

Step	Action
1.	From the MAIN MENU, select Maintenance => Field Software Upgrade => Servers. Result: The following screen is displayed: 
2.	Select the radio button next to the download server.
3.	Select DELETE to delete the FSU download server.

9.10 (U) Displaying Download Servers

Introduction

(U//FOUO) The operator can display FSU download servers.

Important Notes

(U//FOUO) The following notes apply to displaying FSU download servers:

- Only the SSO can access this command.

Procedure

(U//FOUO) Follow these steps to displaying FSU download servers:

The display capabilities have been integrated with the configure capabilities. See section 9.8.

9.11 (U) Configure Download TFTP Settings

Introduction

(U//FOUO) The operator can configure TFTP settings for FSU. These settings are used during the TFTP file transfer (i.e., download) from the download server.

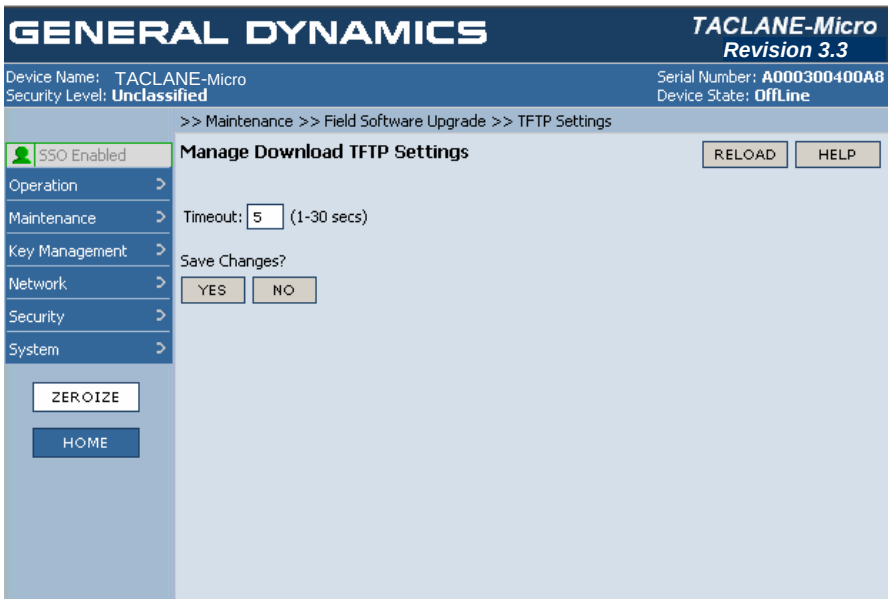
Important Notes

(U//FOUO) The following notes apply to configuring TFTP settings:

- Only the SSO can access this command.

Procedure

(U//FOUO) Follow these steps to configure TFTP settings:

Step	Action
1.	From the MAIN MENU, select Maintenance => Field Software Upgrade => TFTP Settings. Result: The following screen is displayed: 
2.	Enter the Timeout value in seconds.
3.	Select YES to save changes.

9.12 (U) Download a FSU File

Introduction

(U//FOUO) The operator can download an FSU file via the PT, CT, or Console port to load a new software release into the TACLANE. The port on which the file is downloaded is determined by the download server configuration.

Important Notes

(U//FOUO) The following notes apply to performing an FSU download:

- A stable power environment must be maintained throughout the procedure. Use of an uninterruptible power supply (UPS) is recommended.
- Only the SSO can access this command.
- Path information included in the filename field will be ignored.
- The base directory on the TFTP server must be set to the directory where the FSU file resides because this is where the TACLANE-Micro will look for it.
- **If you are using FIREFLY, a new FIREFLY vector set will be needed after FSU is performed.**

Major and Minor Releases

(U//FOUO) The version of TACLANE software being loaded cannot digress beyond a previous major release, because it will not be compatible. Major releases must be upgraded consecutively and cannot be skipped. Minor releases can be skipped and overwritten with earlier minor releases in the same major release. General Dynamics will specify major and minor TACLANE software releases in their release notes.

(U//FOUO) The TACLANE-Micro's first release, Release 3.3, is a major release.

(U//FOUO) Note: Image decryption will fail for a release that is not permitted as an upgrade to a currently installed TACLANE software release.

Requirements

(U//FOUO) Before beginning an FSU download, make sure that you have the following:

- A configured FSU download server containing the FSU file to be downloaded
- TFTP server configured and running on the download server.

Continued on next page

(U) Download a FSU File, continued

TFTP File Server Settings

(U//FOUO) Before beginning an FSU download the TFTP server on the download server that will be used for the download must be configured and running.

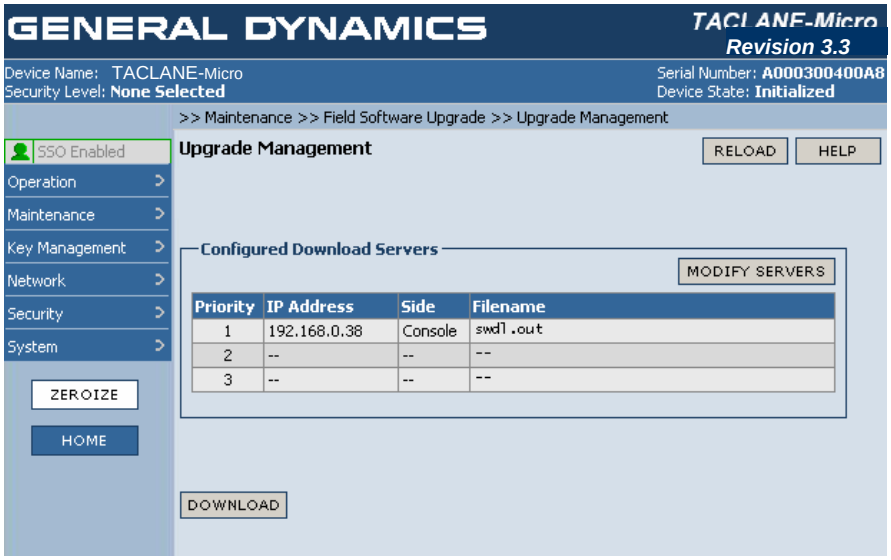
- TFTP Port: 69
- Base Directory: location of FSU file on server
- Server Interface: IP address of server.

Tip

(U//FOUO) If an error occurs during the procedure, such as a tamper condition or continuous alarm state, Field Tamper Recovery may be used to reset the unit and generate a new User CIK. See Section 10.3, "Performing a Field Tamper Recovery" for instructions. Then return to this section and retry the Field Software Upgrade.

Procedure

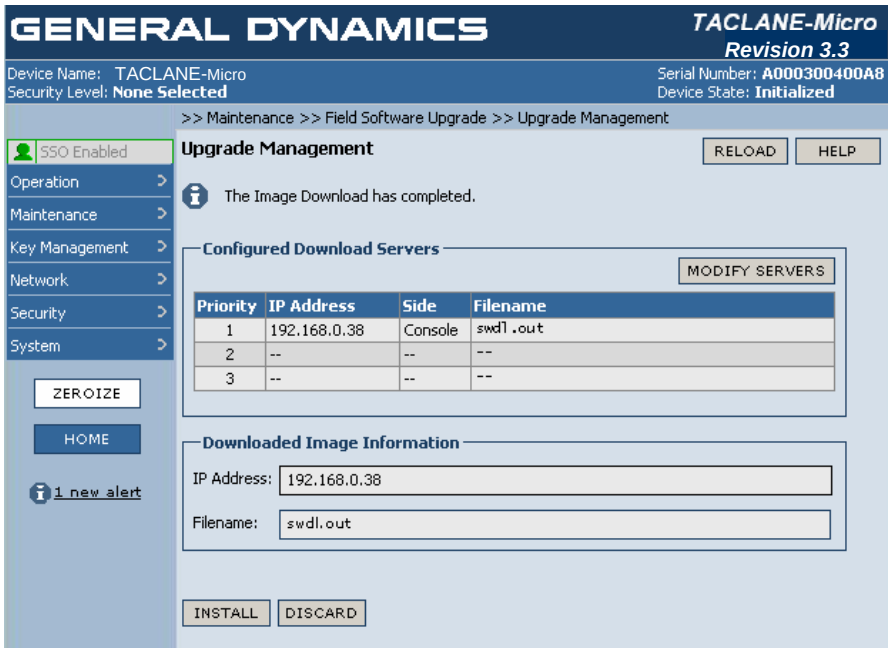
(U//FOUO) Follow these steps to perform a Field Software Upgrade:

Step	Action
1.	From the MAIN MENU, select Maintenance => Field Software Upgrade => Upgrade Management. The TACLANE will display the currently configured download servers. Result: The following screen is displayed: 

Continued on next page

(U) Download a FSU File, continued

Procedure (continued)

Step	Action
2.	Select DOWNLOAD to initiate the transfer operation. Once the transfer operation has successfully completed, the following screen is displayed: 
3.	Select INSTALL to install the new file (See Section 9.13 "Install a FSU File").
4.	Select DISCARD to delete the FSU file.

9.13 (U) Install a FSU File

Introduction

(U//FOUO) The operator can install a new software release (a previously transferred FSU file) into the TACLANE.

Important Notes

(U//FOUO) The following notes apply to performing an install FSU:

- Only the SSO can access this command.
- The install process can take four minutes to write the image to flash.
- If the installation process is interrupted, the TACLANE-Micro will continue to use the previous image. FSU will not complete and will need to be redone.
- **If you are using FIREFLY, a new FIREFLY vector set will be needed after FSU is performed.**

Major and Minor Releases

(U//FOUO) The version of TACLANE software being loaded cannot digress beyond a previous major release, because it will not be compatible. Major releases must be upgraded consecutively and cannot be skipped. Minor releases can be skipped and overwritten with earlier minor releases in the same major release. General Dynamics will specify major and minor TACLANE software releases in their release notes.

(U//FOUO) The TACLANE-Micro's first release, Release 3.3, is a major release.

(U//FOUO) Note: Image decryption will fail for a release that is not permitted as an upgrade to a currently installed TACLANE software release. On failure of an install the release that was in effect prior to the start of the FSU install remains in effect.

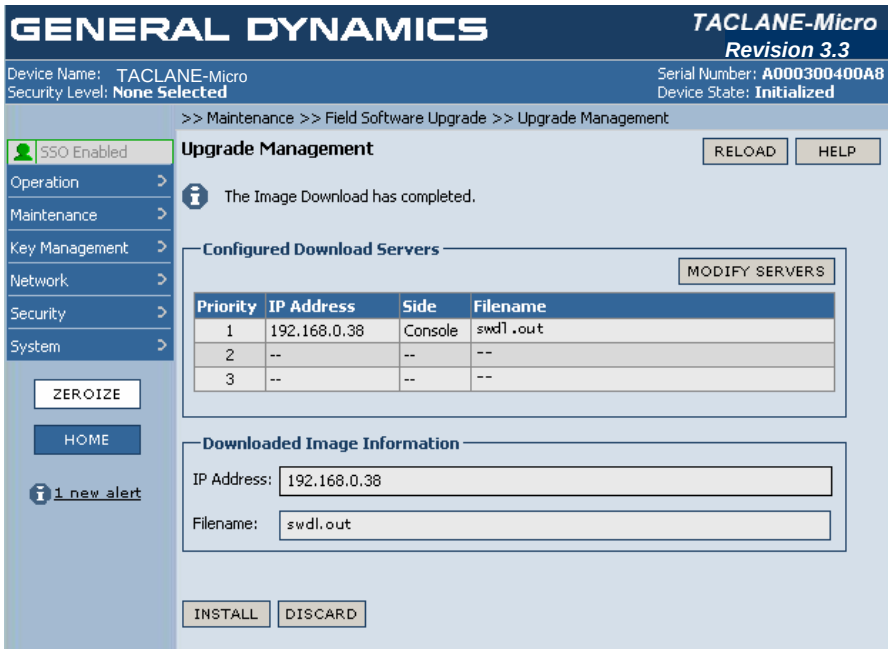
Tip

(U//FOUO) If an error occurs during the procedure, such as a tamper condition or continuous alarm state, Field Tamper Recovery may be used to reset the unit and generate a new User CIK. See Section 10.3, "Performing a Field Tamper Recovery" for instructions. Then return to this section and retry the Field Software Upgrade.

Continued on next page

(U) Install a FSU File, continued

Procedure (U//FOUO) Follow these steps to perform a Field Software Upgrade:

Step	Action
1	From the MAIN MENU, select Maintenance => Field Software Upgrade => Upgrade Management. Result: The following screen is displayed:  Note: Specific version information depends on the particular TACLANE configuration.
2.	Select INSTALL to initiate the install operation. The progress of the FSU file decryption process is displayed on the screen for the operator. Note: Only a single FSU installation can be in progress at any time.
3.	When all images have been successfully written, the Field Software Upgrade installation is complete. The status of the installation is displayed to the operator.

FSU Installation Results

(U//FOUO) If the installation fails then the FSU file must first be discarded before another FSU file can be downloaded and subsequently installed.

(U//FOUO) If the installation is successful, the TACLANE must be restarted for the new release to take effect. No other FSU operations (download or installation) can be executed until a restart takes place.

(U//FOUO) On restart, the TACLANE will autorecover to the operational state that preceded the FSU installation and the new release will be in effect.

9.14 (U) Zeroizing the TACLANE

Introduction

(U//FOUO) The TACLANE supports three types of zeroization: 1) Panic zeroize which deletes all keys in the TACLANE, 2) Selective zeroize which deletes a particular key (for details, see sections 4.4 and 4.8 of this document), and 3) tamper zeroize which is the result of a tamper condition of the unit and all keys are deleted.

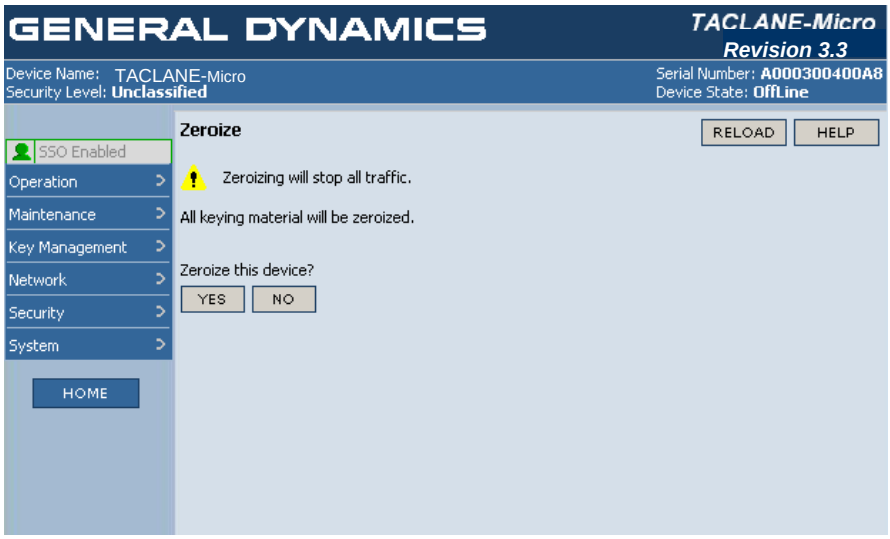
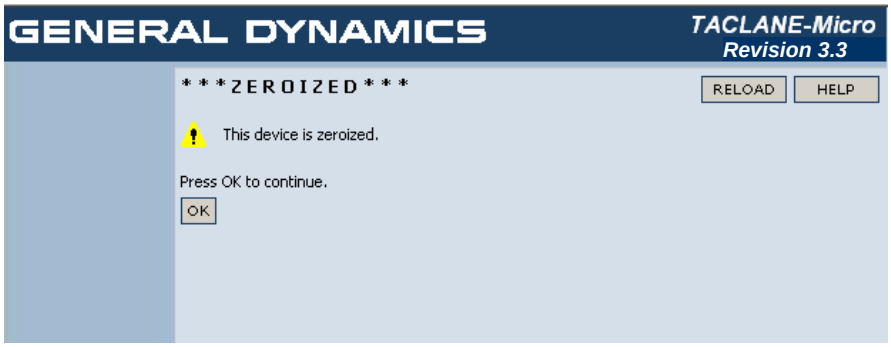
(U//FOUO) This section describes how the operator can invoke a panic zeroize. An operator can initiate a panic zeroize either from the TACLANE front panel zeroize button or from the HMI Zeroize command.

Notes

(U//FOUO) The following notes apply to panic zeroizing the TACLANE:

- A panic zeroize deletes all keys.
- TACLANE may be filled with keys again immediately after a panic zeroize.
- On startup after a panic zeroize, TACLANE displays a "TACLANE zeroized" screen to alert the operator that a panic zeroize occurred. After the operator presses OK to continue, the message does not appear again until the next panic zeroize occurs.

Procedure (U//FOUO) Follow these steps to initiate a panic zeroize:

Step	Action
1.	**To initiate a panic zeroize from the front panel**, depress and release the ZEROIZE button three times within a ten second interval. Note: This initiates a panic zeroize whether TACLANE is powered ON or OFF.
2.	**To initiate a panic zeroize from the display**, select the ZEROIZE button from the MAIN MENU. Result: The following screen is displayed: 
3.	Select YES to zeroize and restart the TACLANE. Note: When the TACLANE starts up, the following screen is displayed:  Select OK to acknowledge the message display indicating the device has been zeroized."

9.15 (U) System Information

Introduction

(U//FOUO) The operator can display the following TACLANE system information which identifies the particular TACLANE unit:

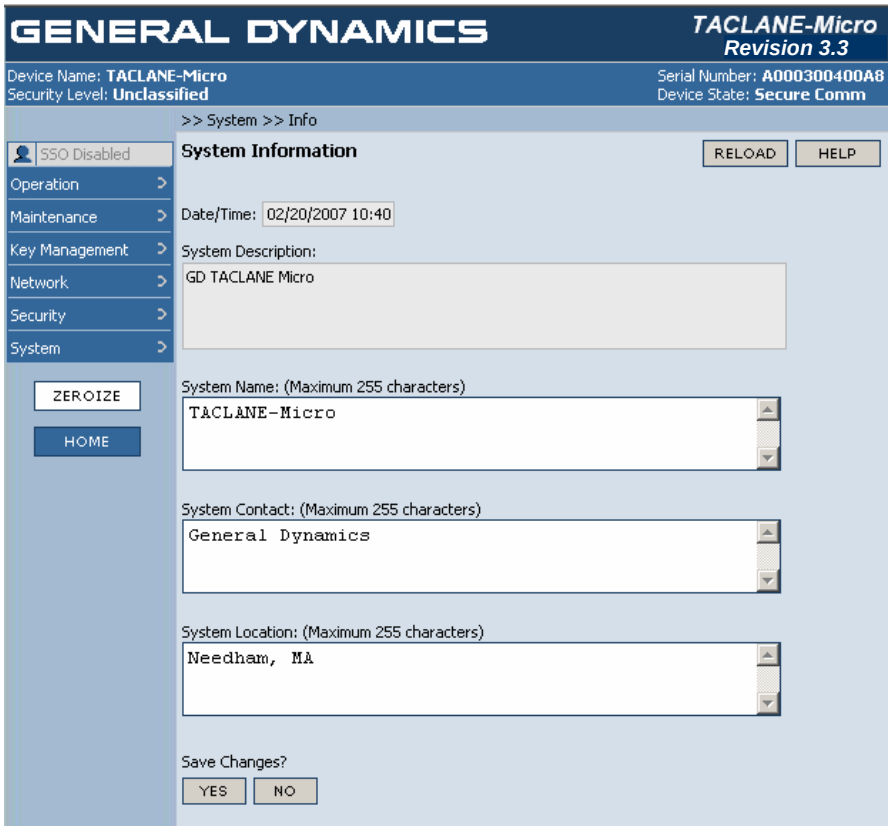
- TACLANE System Description – the up to 255-character, user-configurable system description.
- TACLANE System Name – the up to 255-character, user-configurable system name.
- TACLANE System Contact – the up to 255-character, user-configurable system contact information.
- TACLANE System Location – the up to 255-character, user-configurable system location.

(U//FOUO) The operator can modify the following TACLANE system information:

- TACLANE System Name
- TACLANE System Contact
- TACLANE System Location.

Procedure

(U//FOUO) Follow these steps to display and/or configure the TACLANE system information:

Step	Action
1.	From the MAIN MENU, select System => Info. Result: The following screen is displayed: 
2.	Enter data into the System Name, System Contact and/or System Location text boxes.
3.	Select YES to save changes.

9.16 (U) Enable SSO Privileges

Introduction

(U//FOUO) This command allows the TACLANE-Micro SSO operator to gain access to the SSO-privileged HMI commands through entering the valid 9-digit SSO PIN.

Factory Default SSO PIN

(U//FOUO) The TACLANE-Micro delivered from the factory has the following default SSO PIN: 123456789.

(U//FOUO) If over 180 days have passed since the TACLANE unit has left the factory, then the PIN Expired screen will appear after the operator first enters the Enable SSO Privileges command with the (expired) factory default PIN. In this case, the PIN Expired screen will include a new SSO PIN that the operator can accept or reject. In this example, the specific sequence would be:

1. Operator attempts to enable privileges (Enable Privileges command) by entering the factory default PIN (123456789).
2. The HMI then displays the "PIN EXPIRED" screen that includes a new PIN, and prompts the operator as to whether to accept the PIN or not.
3. Operator records the PIN value and accepts the new PIN.
4. Operator then must return to the Enable Privileges command and enter the new PIN value in order to access the SSO privileged mode.

(U//FOUO) If a TACLANE is ever tampered, the SSO PIN will be reset back to its default PIN (123456789).

Enable SSO Privileges Denied

(U//FOUO) If the operator fails to enter a valid SSO PIN after 5 consecutive attempts, the TACLANE automatically restarts. After the TACLANE restarts, the operator is able to access all the non-privileged HMI functions. If the operator wishes to gain access to the Enable SSO Privileges command again, the operator must select the Enable SSO Privileges command.

SSO PIN Expiration

(U//FOUO) The SSO PIN is valid for 180 days.

(U//FOUO) If an SSO PIN has been entered (via Enable SSO Privileges) and the screen indicates that it is an expired SSO PIN, then the operator is not allowed access to the SSO privileged commands without first generating a new SSO PIN.

(U//FOUO) It is possible to update the SSO PIN prior to the SSO PIN expiration.

(U) Enable SSO Privileges, continued

SSO Privileges Expiration

(U//FOUO) After 15 minutes of no SSO operator activity, the SSO access to the privileged commands expires. To gain access again, the SSO operator needs to reissue the Enable SSO Privileges command and enter the valid SSO PIN.

(U//FOUO) If the TACLANE is ever restarted, the operator will need to re-enter the PIN to enable access to the SSO privileged commands.

Forgotten PIN

(U//FOUO) If the operator has forgotten the current SSO PIN, the only way to regain SSO privileges of the TACLANE is to perform the Field Tamper Recovery (see section 10.3) on the TACLANE, which resets the PIN to the factory default SSO PIN ("123456789").

Notes

(U//FOUO) The following notes apply to the enable SSO privileges function:

- This command is only accessible if currently not in the SSO privileged mode.
- Refer to section 9.18 ("Generate SSO PIN") for more information on how to generate an SSO PIN.
- Following a depot tamper recovery and then attempting to enable SSO privileges by entering the default PIN, the restart progress bar may be displayed at the console if an interface timeout occurs. The TACLANE-Micro may not be restarting. The operator can reload the screen or reopen the browser.

Continued on next page

(U) Enable SSO Privileges, continued

SSO-privileged HMI Commands

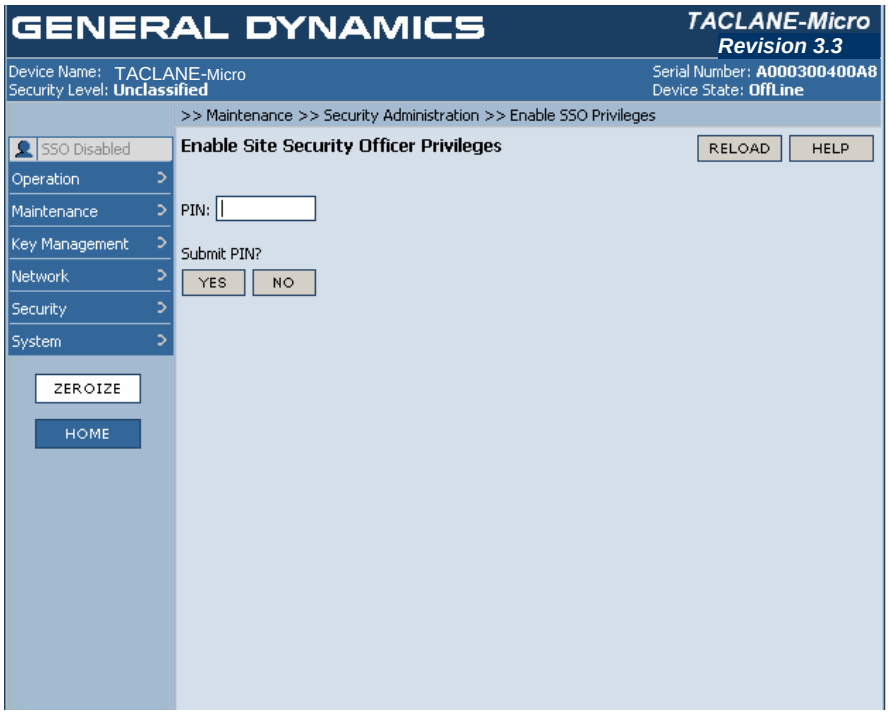
(U//FOUO) The table below lists the various TACLANE-Micro HMI commands. Use the legend to identify the privileged commands that require SSO privileges to access.

Operation	Maintenance	Key Management	Network	Security	System
Restart (I, O, S, R)	**Security Administration**	FIREFLY Vector Set (I, O, S, P)	Dynamic Discovery (I, O, S, P)	Access Mode (I, O, S, SSO)	Audit Log Threshold (I, O, S, P)
Security Level (I, O, S, SSO) (R if in sec level)	Enable SSO Privileges (I, O, S)	PrePlaced Key (I, O, S, P)	Ethernet Comm (I, O, S)	Access Control List (I, O, S, P)	Info (I, O, S)
Initialize (O, S, R)	Disable SSO Privileges (I, O, S, SSO)		**IP Comm**	CIK Management (I, O, S, P)	Network Managers (I, O, S, P)
Offline (I, S)	Generate SSO PIN (I, O, S, SSO)		IPv4 Addresses (I, O, S)	PPK Assignment (I, O, S, P)	
Secure Comm (O, L)	Battery (I, O, S)		MTU (I, O, S)	SA Configuration (I, O, S, P)	
SA Info	Date/Time (I, O, S, SSO, R)		PING Configuration (I, O, S)	**Static Routes**	
SA Table (O, S)	**Field Software Upgrade**			Route Management (I, O, S)	
	Servers (I, O, S, SSO)			Delete All Routes (I, O, S)	
	TFTP Settings (I, O, S, SSO)			**Traffic Flow Security**	**Legend**
	Upgrade Management (I, O, S, SSO)			Fixed Packet Length (I, O, S, P)	S – Secure Comm (Cryptography Active Mode)
	Logs			Bypass (I, O, S, P)	O – Offline Mode
	Event Log (I, O, S)			PSEQN Check (I, O, S, P)	I – Initialized Mode
	Audit Log (I, O, S)				L – In Security Level
	Delete Audit Log (I, O, S, SSO)				P – Contains Additional Functionality for SSO-Privileged Operator
					R – Restart Occurs
					SSO – SSO-Privileges Required to Access this Page.

Continued on next page

(U) Enable SSO Privileges, continued

Procedure (U//FOUO) Follow these steps to enable SSO privileges:

Step	Action
1.	From the MAIN MENU, select Maintenance => Security Administration => Enable SSO Privileges Result: The following screen is displayed: 
2.	Enter the valid SSO PIN and then select YES to submit this PIN for validation.

9.17 (U) Disable SSO Privileges

Introduction

(U//FOUO) This command allows the SSO operator to disable access to the SSO-privileged HMI commands on a TACLANE.

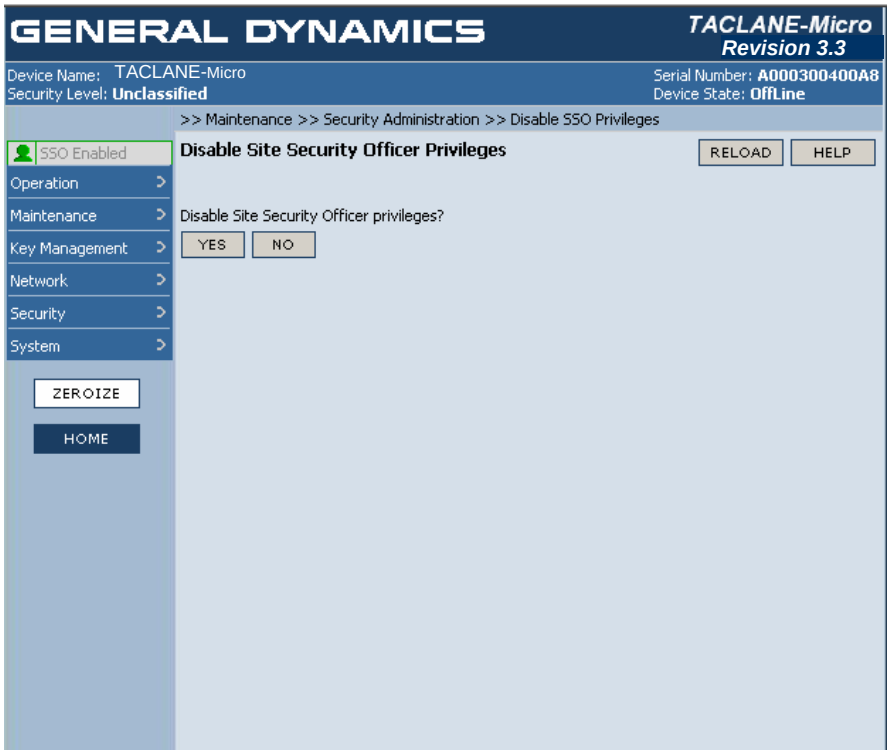
Notes

(U//FOUO) The following notes apply to the disable SSO privileges function:

- Only the SSO can access this command.

Procedure

(U//FOUO) Follow these steps to disable SSO privileges:

Step	Action
1.	From the MAIN MENU, select Maintenance => Security Administration => Disable SSO Privileges. Result: The following screen is displayed: 
2.	Select YES to disable the current SSO privileges.

9.18 (U) Generate SSO PIN

Introduction

(U//FOUO) This command allows the SSO operator to generate/update the 9-digit SSO PIN for a TACLANE. The SSO PIN is a 9-digit machine-generated PIN. When generating a PIN, the PIN is displayed and it must be acknowledged by the operator before it overwrites the previous SSO PIN.

(U//FOUO) It is critical that the operator saves the SSO PIN. Forgetting the SSO PIN will require that the TACLANE unit undergo a Field Tamper Recovery in order to access the privileged commands.

SSO PIN Expiration

(U//FOUO) The SSO PIN is valid for 180 days.

(U//FOUO) If an SSO PIN has been entered (via Enable SSO Privileges) and the screen indicates that it is an expired SSO PIN, then the operator is not allowed access to the SSO privileged commands without first generating a new SSO PIN.

(U//FOUO) It is possible to update the SSO PIN prior to the SSO PIN expiration.

Factory Default SSO PIN

(U//FOUO) The TACLANE-Micro delivered from the factory has the following default SSO PIN: 123456789.

(U//FOUO) If over 180 days have passed since the TACLANE unit has left the factory, then the PIN Expired screen will appear after the operator first enters the Enable SSO Privileges command with the (expired) factory default PIN. In this case, the PIN Expired screen will include a new SSO PIN that the operator can accept or reject. In this example, the specific sequence would be:

1. Operator attempts to enable privileges (Enable Privileges command) by entering the factory default PIN (123456789).
2. The HMI then displays the "PIN EXPIRED" screen that includes a new PIN, and prompts the operator as to whether to accept the PIN or not.
3. Operator records the PIN value and accepts the new PIN.
4. Operator then must return to the Enable Privileges command and enter the new PIN value in order to access the SSO privileged mode.

(U//FOUO) If a TACLANE is ever tampered, the SSO PIN will be reset back to its default PIN ("123456789").

Forgotten PIN

(U//FOUO) If the operator has forgotten the current SSO PIN, the only way to regain SSO privileges of the TACLANE is to perform the Field Tamper Recovery on the TACLANE (see section 10.3), which resets the PIN to the factory default SSO PIN ("123456789").

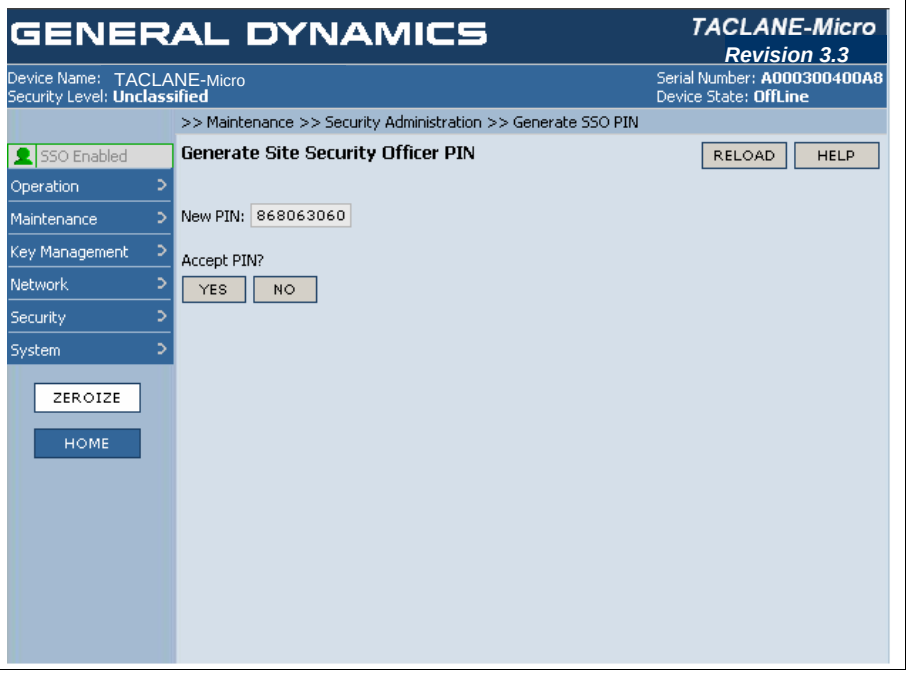
Notes

(U//FOUO) The following notes apply to the generate SSO PIN function:

- Only the SSO can access this command.
- After generating a new PIN, the operator is not yet in the SSO privileged mode. The operator must select the Enable Privileges command and enter the PIN in order to be in the SSO privileged mode.
- The TACLANE supports one SSO PIN. After the SSO PIN is updated, the previous SSO PIN is no longer valid.
- **It is critical that the operator saves the SSO PIN. Forgetting the SSO PIN requires that the TACLANE unit undergo a Field Tamper Recovery.**

Procedure

(U//FOUO) Follow these steps to update the SSO PIN:

Step	Action
1.	From the MAIN MENU, select Maintenance => Security Administration =>Generate SSO PIN. Result: The following screen is displayed: 

2.	Select YES to accept the PIN. Note 1: The operator must accept the PIN within five minutes of being prompted, otherwise the PIN generation fails. Note 2: It is very important that the operator record this new PIN value and save it. This PIN is needed to enter the SSO privileged mode. Note 3: In order to enter the privileged mode, the operator must select the Enable SSO Privileges command and enter this new PIN.

9.19 (U) Audit Log Threshold

Introduction

(U//FOUO) This command allows the SSO operator to configure the warning threshold on the TACLANE-Micro audit log. Once this threshold is reached, the operator is notified.

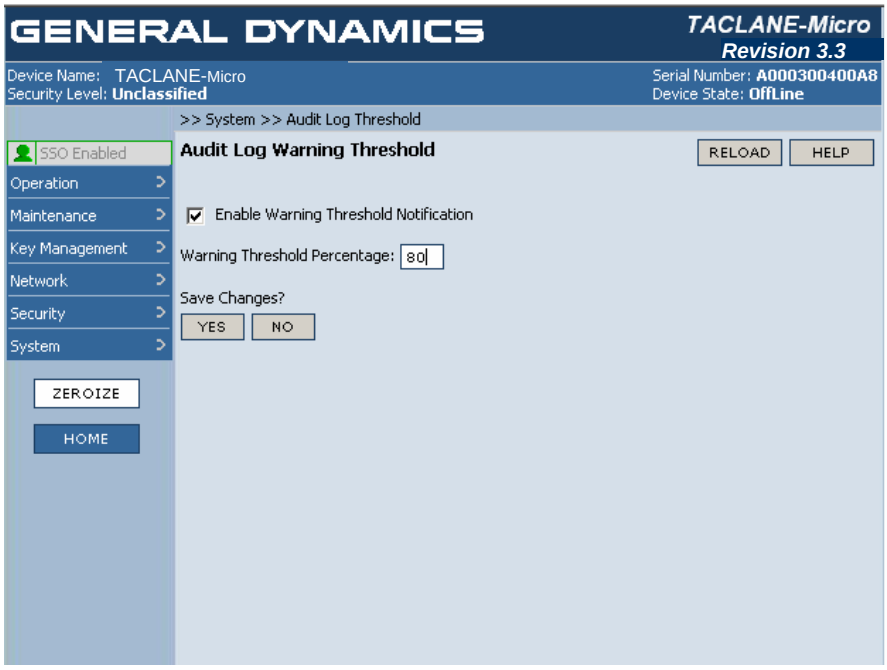
Notes

(U//FOUO) The following notes apply to the Audit Log Threshold function:

- Only the SSO can access this command.

Procedure

(U//FOUO) Follow these steps to enter an audit log threshold:

Step	Action
1.	From the MAIN MENU, select System => Audit Log Threshold. Result: The following screen is displayed: 
2.	Select the checkbox next to Enable Warning Threshold Notification. If the box is checked, (a checkmark is present in the box) then Enable Warning Threshold Notification processing is enabled (a notification is sent to the operator when the audit log threshold is reached). If the box is empty (no checkmark present in the box) then Enable Warning Threshold Notification processing is disabled. Enter the Warning Threshold Percentage value. Note: If the threshold is set to zero, no warning will be sent.
3.	Select YES to save changes.

9.20 (U) Delete Audit Log

Introduction

(U//FOUO) This command allows the SSO operator to delete all Security Audit Log records on a TACLANE.

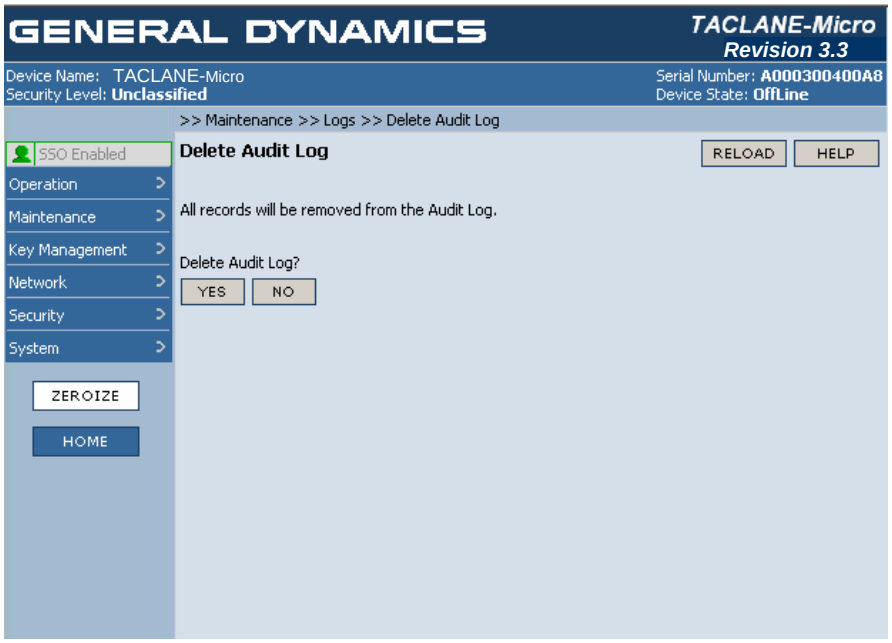
Notes

(U//FOUO) The following notes apply to the Delete Audit Log function:

- Only the SSO can access this command.

Procedure

(U//FOUO) Follow these steps to delete audit log:

Step	Action
1.	From the MAIN MENU, select Maintenance => Logs => Delete Audit Log. Result: The following screen is displayed: 
2.	Select YES to delete the audit log.

9.21 (U) Display Audit Log

Introduction

(U//FOUO) This command allows the operator to display the Security Audit Log records on a TACLANE.

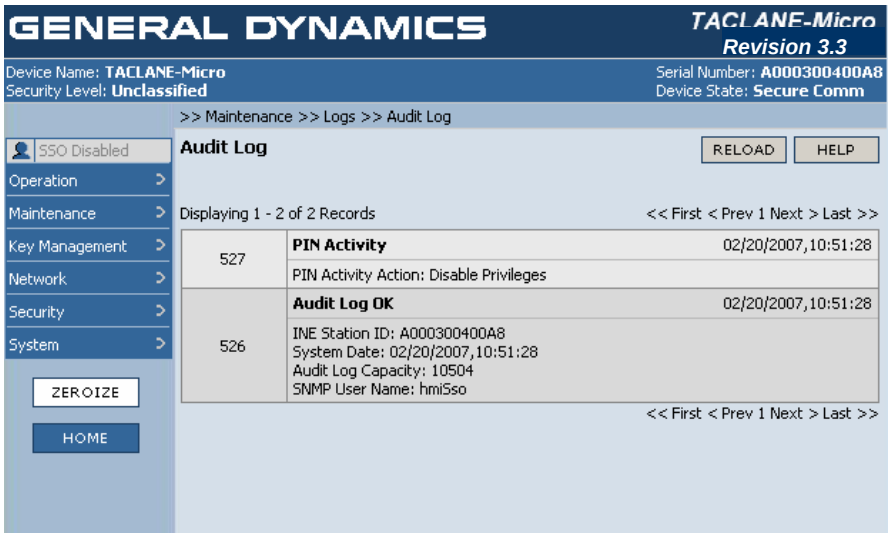
Notes

(U//FOUO) The following notes apply to the Display Audit Log function:

- When the Audit Log reaches the maximum records (5663), the oldest block of the Audit Log is removed (809 records) to allow additional events to be logged.

Procedure

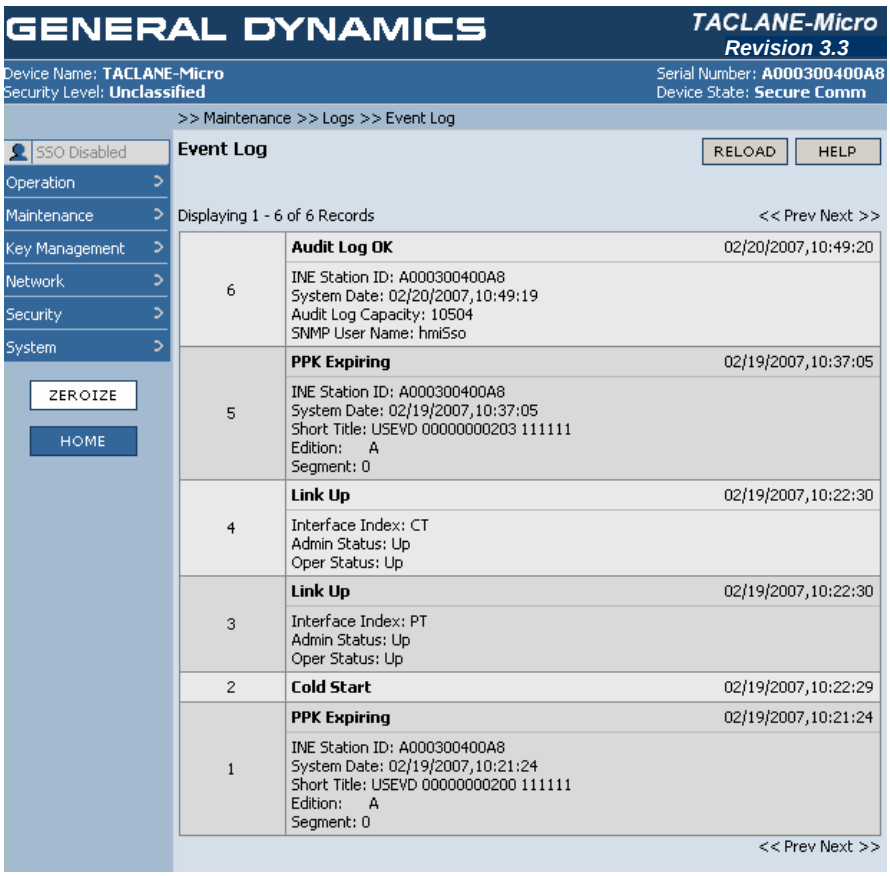
(U//FOUO) Follow these steps to display the audit log:

Step	Action
1.	From the MAIN MENU, select Maintenance => Logs => Audit Log. Result: The following screen is displayed: 
2.	Select NEXT to display the next page of audit log records, PREV to display the previous page of audit log records or select the page number to display a particular page of audit log records, if available.

9.22 (U) Display Event Log

Introduction (U//FOUO) This command allows the operator to display the Event Log records on a TACLANE.

Procedure (U//FOUO) Follow these steps to display the event log:

Step	Action
1.	From the MAIN MENU, select Maintenance => Logs => Event Log. Result: The following screen is displayed: 
2.	Select NEXT to display the next page of event log records, PREV to display the previous page of event log records or select the page number to display a particular page of event log records, if available.

10.0 (U) TROUBLESHOOTING TACLANE

10.1 (U) Alarm

Introduction

(U//FOUO) An alarm is the result of an internal failure. When a TACLANE is in an alarm condition, the ALARM status LED is illuminated.

(U//FOUO) Note: The ALARM status LED is illuminated briefly during diagnostics. This is normal.

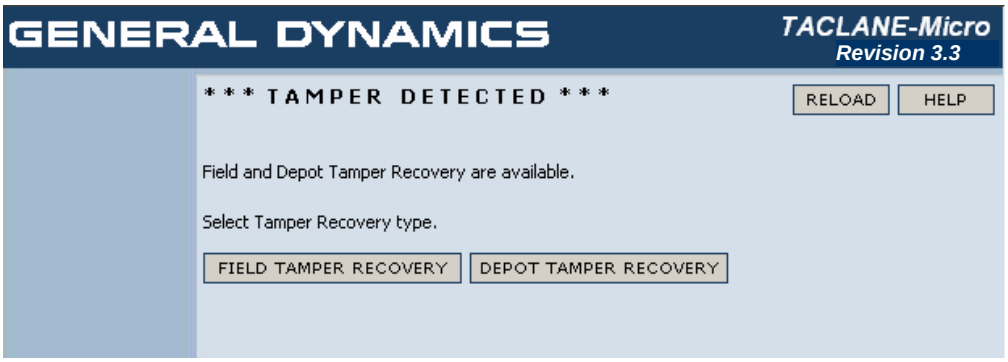
Alarm Recovery

(U//FOUO) TACLANE automatically attempts to recover from an alarm. TACLANE automatically resets during alarm recovery and attempts to return to the previous operating mode. After two successive alarms of the same type, the TACLANE will halt (i.e., it will stop attempting to restart). Power can be cycled by the operator to attempt to recover from a repeated alarm condition. If the condition persists, the TACLANE must be returned to the depot for repair. Note the circumstances surrounding the alarm, as this information may be useful to depot personnel.

10.2 (U) Tamper

Introduction

(U//FOUO) Tamper is the result of opening the TACLANE chassis, loss of battery power when powered off, or removal of the battery while the TACLANE is powered off. When a TACLANE is in a tamper condition, the TAMPERED status LED is illuminated.



(U//FOUO) Note: All keys are automatically deleted when a tamper condition is detected.
Depot Tamper Recovery is a factory level option and not discussed in this manual.

Tamper Recovery

(U//FOUO) A tampered unit can be recovered in the field. See Section 10.3, "Performing a Field Tamper Recovery," for more information.

10.3 (U) Performing a Field Tamper Recovery

Introduction

(U//FOUO) The operator can perform a Field Tamper Recovery (FTR) using a Recovery CIK to recover a TACLANE that has become tampered. FTR can also be used 1) to create CIK1 if there are no valid CIKs, 2) to reset the SSO PIN, and 3) may help recover a TACLANE from a continuous alarm state. In cases where the unit is not already tampered, first tamper the unit by removing the battery with the power off. Then follow the Field Tamper Recovery procedure below.

Important Note

(U//FOUO) Before performing a Field Tamper Recovery, the TACLANE operator must determine if the tamper was benign (e.g., depleted battery). The unit must be visually inspected, ensuring that the tamper seals are intact.

Evidence of physical tampering must be reported to NSA in accordance with TACLANE doctrine.

New CIK

(U//FOUO) Obtain a CIK before beginning this procedure. This CIK will become CIK1 for this TACLANE. Do not use a CIK that is required for another TACLANE as that will make it invalid for the other TACLANE.

Field Tamper Recovery CIK

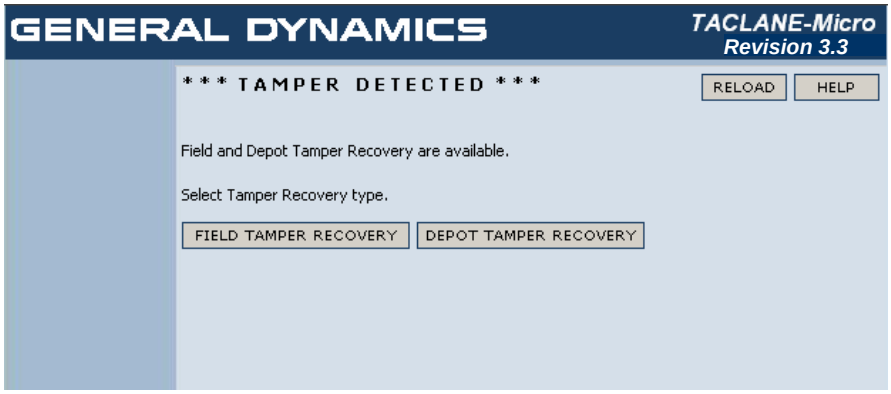
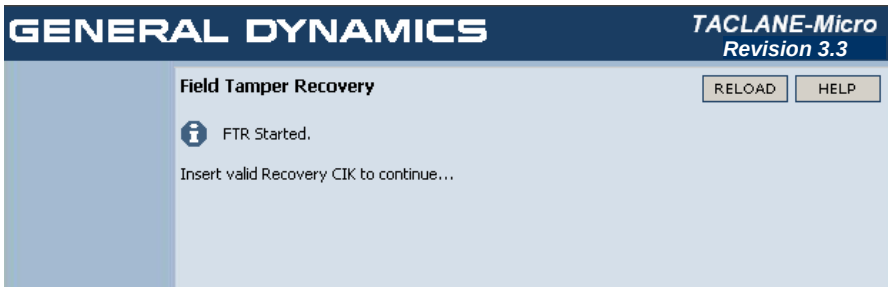
(U//FOUO) A Recovery CIK is unique to its associated TACLANE. The Recovery CIK should be tagged with the serial number of the associated TACLANE. It can be used to recover its associated TACLANE from tamper a maximum of five times. After it has been used five times, a Recovery CIK is no longer valid. The tag attached to the Recovery CIK should be used to identify its associated TACLANE and to keep a record of the number of times that Recovery CIK is used for tamper recovery.

The Recovery CIK is classified SECRET, and must be handled according to NSA doctrine.

Battery Replacement

(U//FOUO) A benign tamper is typically due to a depleted battery. It is recommended that the battery be replaced during a Field Tamper Recovery.

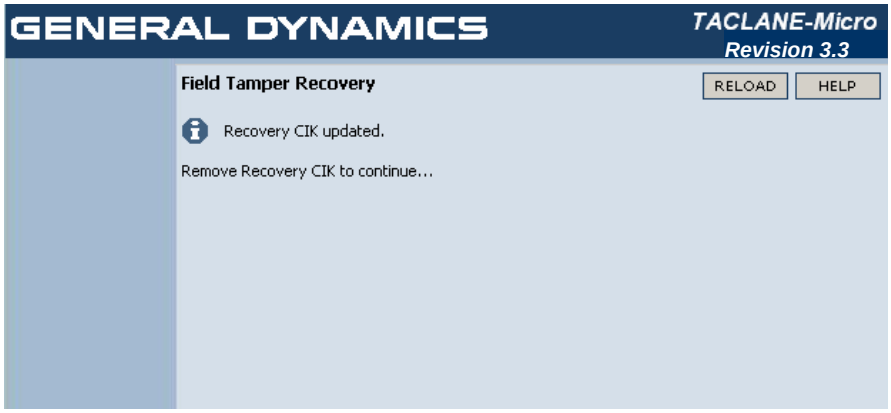
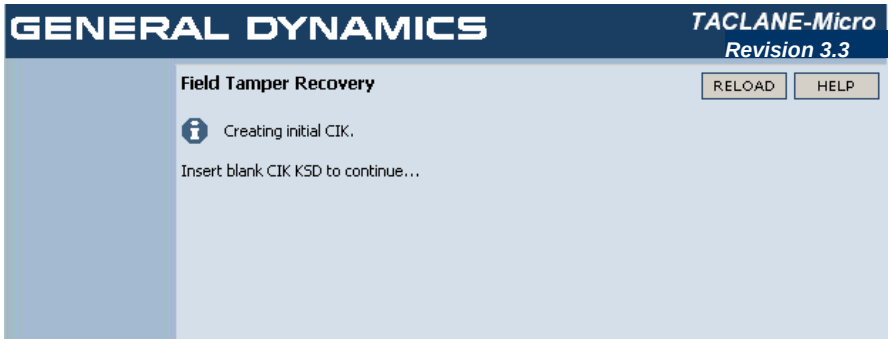
Procedure (U//FOUO) Follow these steps to perform a Field Tamper Recovery:

Step	Action
1.	Replace the TACLANE's battery (See Section 10.5, "Replacing the Battery"). Note: The battery installed date cannot be updated until the TACLANE is recovered from tamper.
2.	Power off the tampered TACLANE.
3.	If a CIK is inserted, remove the CIK.
4.	Turn on the TACLANE. Result: The following screen is displayed:  Note: If the HMI displays only the DTR button, then the Recovery CIK has been used five times. Once the Recovery CIK has been used five times, the TACLANE must be returned to the depot.
5.	Select the FTR button on the HMI display. Result: The following screen is displayed: 

Continued on next page

(U) Performing a Field Tamper Recovery, continued

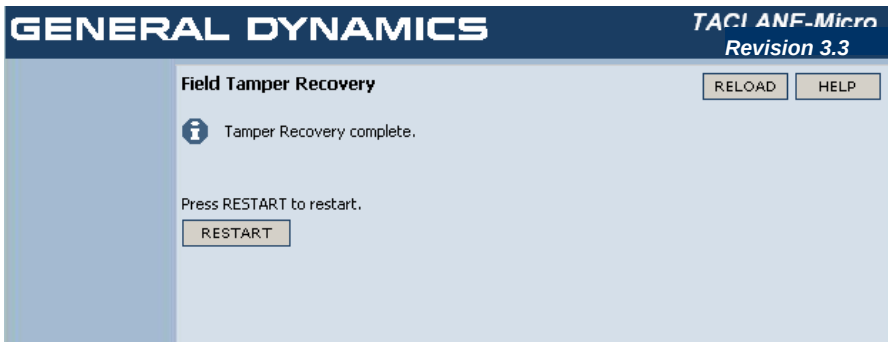
Procedure (continued)

6.	Insert the Recovery CIK. Result: The following screen is displayed:  Note: If the HMI displays "Not Recovery CIK" and restarts, then an invalid CIK is inserted. Remove the invalid CIK and start from the beginning of this procedure.
7.	Remove the Recovery CIK. 
8.	Insert CIK. This can be a CIK that was used for the TL before this FTR operation. **The CIK inserted at this point will become CIK1 for this TACLANE. Do not use a CIK that is associated with another TACLANE as that will make the CIK invalid for that other TACLANE.** If the HMI displays "Error Creating CIK. Tamper Recovery Failed" and the TACLANE restarts, the CIK is damaged. Remove the CIK and attempt the FTR with a different KSD.
9.	The Recovery CIK tag contains five numbered lines for recording tamper recoveries. At this time, initial and date the first available line, indicating that a Field Tamper Recovery has been performed.

Continued on next page

(U) Performing a Field Tamper Recovery, continued

Procedure (continued)

Step	Action
10.	The TACLANE indicates that Field Tamper Recovery is complete. Result: The following screen is displayed: 
11.	Select RESTART to continue. The TACLANE will restart and return to the INITIAL state.
12.	Set the date and time (See Section 9.1, "Setting the Date and Time").
13.	Update the battery installed date (See Section 10.5, "Replacing the Battery," for instructions).
14.	At this point, the TACLANE is reset to factory defaults (See Appendix A, "Factory Default Settings"). The configuration needs to be restored and key material needs to be filled.

10.4 (U) Checking for a Low Battery

Introduction

(U//FOUO) If the battery voltage depletes below acceptable levels during TACLANE operation, the BATTERY status LED on the front panel is illuminated. In addition, the battery power level is continuously monitored.

Note

(U//FOUO) If the battery low status LED is illuminated, the battery should be replaced. See Section 10.5, "Replacing the Battery."

Procedure

(U//FOUO) Follow this step to check for a low battery:

Step	Action
1.	Check whether the battery low status LED is illuminated. If the battery low status LED is illuminated, then the battery should be replaced. Note: The battery low status LED is illuminated briefly during diagnostics. This is normal.

10.5 (U) Replacing the Battery

Introduction

(U//FOUO) The operator can replace the battery. The lithium battery has an estimated life of two years. Exposure to extreme temperatures will reduce the lifetime. However, the lithium battery will last at least one year over all supported temperature ranges. It is recommended to change the battery every 12 months or when the BATTERY LOW status LED is illuminated.

Important Battery Removal Note

(U//FOUO) The battery may be changed while the device is plugged in or while the device is not plugged in.

(U//FOUO) It is recommended that the battery be changed while the device is plugged in, because when the device is NOT plugged in, there is a 30 second time limit to change the battery. In the unplugged situation, if the battery is not changed within 30 seconds, TACLANE will TAMPER. Therefore, it is important that the operator has the new 3.6 V Lithium battery ready before starting!

(U//FOUO) It is very important that the new battery be placed in correct polarity. If the battery is inserted backwards, there is a risk that the device will be damaged.

(U//FOUO) When changing the battery with the device unpowered, the TACLANE-Micro will illuminate the Battery LED for five seconds upon battery replacement to indicate to the operator the battery is in correctly.

Lithium Battery

(U//FOUO) TACLANE contains a lithium battery.

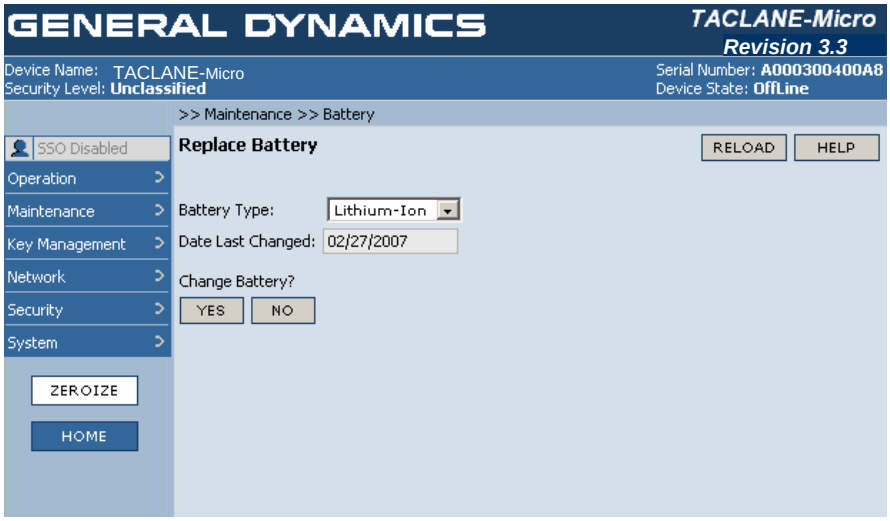
(U) CAUTION: Do not incinerate lithium batteries because of the risk of explosion.

Notes

(U//FOUO) The following notes apply to replacing the battery:

- Replace with a 3.6V AA lithium battery
- Alternative replacement with 1.5V AA alkaline battery.

Procedure (U//FOUO) Follow these steps to replace the battery:

Step	Action
1.	Remove the battery cover (turn counterclockwise).
2.	Install a new battery with negative end first.
3.	Reinsert the battery cover (turn clockwise).
4.	**To update the battery installed date**, from the MAIN MENU select Maintenance -> Battery. Result: The following screen is displayed: 
5.	Select YES to acknowledge battery replacement and return to the MAINTENANCE menu. Note: This sets the battery installed date to the current date.

10.6 (U) Performing Diagnostics

Introduction (U//FOUO) Diagnostics are automatically performed periodically. The operator can initiate diagnostics by restarting the TACLANE.

Procedure (U//FOUO) Follow this step to initiate diagnostics:

Step	Action
1.	Restart the TACLANE (See Section 9.5, "Restarting the TACLANE").

10.7 (U) Troubleshooting General Problems

General Problems

(U//FOUO) The table below describes general TACLANE problems, their causes, and solutions. Also see applicable Release Notes for the TACLANE software version.

Problem	Cause	Solution
TACLANE does not power up	No power	Check power source and connections
TACLANE keeps asking for a valid CIK to be inserted	Invalid CIK	Check that a valid CIK is inserted
	CIK damaged or corrupted by removal during CIK write	A damaged or corrupted CIK cannot be recovered. Another valid CIK copy can be used, if available. If no valid CIK copy is available, the TACLANE needs to be serviced.
Cannot create CIK ("Error reading from CIK. Remove CIK").	CIK device is bad	Try different CIK
Cannot create CIK ("Error writing to CIK. Remove CIK").	CIK device is bad	Try different CIK

10.8 (U) Troubleshooting Filling and Managing Keys

Problems with Filling and Managing Keys

(U//FOUO) The table below describes TACLANE problems with filling and managing keys, their causes, and solutions. Also see applicable Release Notes for the TACLANE software version.

Problem	Cause	Solution
Cannot fill FIREFLY vector set ("Keying material not filled")	The fill process timed out	Check the fill cable connection between the DTD and the TACLANE. Check that the DTD is set to the DS101 protocol.
Cannot fill FIREFLY vector set (TACLANE resets during transfer)	The DTD was set to "issue" the FIREFLY vector set	Check that the DTD is configured to "fill" the FIREFLY vector set rather than "issue" it.
Cannot fill PPK ("Keying material not filled")	The fill process timed out	Check the fill cable connection between the DTD and the TACLANE. Check that the DTD is set to the DS101 protocol.

10.9 (U) Troubleshooting IP/Ethernet

IP/Ethernet Configuration Problems

(U//FOUO) The table below describes TACLANE IP/Ethernet configuration problems, their causes, and solutions. Also see applicable Release Notes for the TACLANE software version.

Problem	Cause	Solution
Cannot ping TACLANE IP addresses	TACLANE not in secure communications mode	Put TACLANE online.
	IP configuration incorrect or incomplete	Check that the IP/Ethernet configuration is complete and correct.
	Ethernet cable/transceiver problem	Check that the Ethernet cables and transceivers (if used) are working properly. If using twisted pair Ethernet cables, check that straight or crossover twisted pair cables are used where needed. Verify that the network speed settings are compatible.

10.10 (U) Troubleshooting Security Associations

Security Association Problems

(U//FOUO) The table below describes TACLANE security association problems, their causes, and solutions. Also, see applicable Release Notes for the TACLANE software version.

Problem	Cause	Solution
Cannot enter secure communications mode ("Configuration error")	IP configuration incorrect or incomplete	Check that the IP configuration is complete and correct.
Cannot secure IP SAs. IP communications fail.	Ethernet cable/transceiver problem	Check that the Ethernet cables and transceivers (if used) are working properly. If using twisted pair Ethernet cables, check that straight or crossover twisted pair cables are used where needed.
	The underlying network is experiencing a failure or is not configured correctly.	Check that the underlying network is configured and operating correctly. If the TACLANE was inserted into an existing IP/Ethernet configuration, flush the ARP caches on hosts and routers. Verify that the network speed settings are compatible.
	Firewall prohibiting SDD, IKE, and/or ESP traffic	Check that any firewalls allow SDD, IKE, and ESP traffic. See the section on "Factory Default Settings and Port Numbers" for the port numbers.
	When using PPKs, TACLANE date/time between communicating TACLANEs is more than 55 minutes apart.	Check that all communicating TACLANEs have their date/time set within 55 minutes of each other to ensure that no communications blackout periods occur when using PPKs.

Continued on next page

(U) Troubleshooting Security Associations, continued

Security Association Problems (continued)

Problem	Cause	Solution
Cannot secure IP SAs. IP communications fail. (continued)	The local and remote TACLANE are at different security levels.	Check that the local and remote TACLANE are at the same security level.
	When using PPKs, the local and remote TACLANE do not have the same PPK filled at the same security level under the same PPK ID.	Check that the local and remote TACLANE have the same PPK filled at the same security level under the same PPK ID.
	When using FIREFLY TEKs, the local or remote FIREFLY vector set is not usable at the current security level.	Check that the local and remote FIREFLY vector sets are valid at the current security level.
	When using FIREFLY TEKs, the local or remote FIREFLY vector set is expired.	Check that the local and remote FIREFLY vector sets are not expired.
	When using FIREFLY TEKs, the local and remote FIREFLY vector sets are identical.	Check that the local and remote FIREFLY vector sets are unique. Each FIREFLY vector set has a unique KMID.
	When using FIREFLY TEKs, the local and remote FIREFLY vector sets are in different partitions or universal editions.	Check that the local and remote FIREFLY vector sets are in the same partition and universal edition.
	PPKs have been expired and automatically deleted.	Automatically deleted PPKs cannot be recovered and must be refilled. Check the entered date/time carefully before confirming to ensure the entered date/time is accurate.
	Access Control Mode is ENABLED at either/both the local/remote TACLANE and the KMID associated with the local/remote FIREFLY vector set is not in the local/remote ACL.	When using Access Control Mode, check that all desired communicating remote TACLANEs have their respective KMIDs entered in the local ACL.

Continued on next page

(U) Troubleshooting Security Associations, continued

Security Association Problems (continued)

Problem	Cause	Solution
Security Associations using PPKs blackout for periods of time.	The underlying network is experiencing periodic temporary failures.	Check that the underlying network is operating correctly.
	TACLANE date/time between communicating TACLANEs is more than 55 minutes apart.	Check that all communicating TACLANEs have their date/time set within 55 minutes of each other to ensure that no communications blackout periods occur.

Appendix A (U) FACTORY DEFAULT SETTINGS

A.1 (U) Factory Default Settings and Port Numbers

TACLANE Factory Default Settings

(U//FOUO) The table below identifies the TACLANE factory default settings for various parameters. The operator may change these parameters.

TACLANE Parameter	Factory Default Setting
IP MTU	1500
MEDIUM	COPPER
ETHERNET COMM MODE	AUTO-NEGOTIATE
MTEK UPDATE	DISABLE
SA HOST ADMINISTRATIVE TIMEOUT	ENABLED
SA HOST ADMINISTRATIVE VALUE	720
FIXED PACKET MODE	ON/FRAGMENT
FIXED PACKET LENGTH	800
PSEQN CHECK	ENABLED
DSCP BYPASS	DISABLED
DF BIT BYPASS	DISABLED
PMTU BYPASS	DISABLED
IGMP/MLD BYPASS	DISABLED
DISCRETIONARY ACCESS CONTROL	OFF
ENABLE SSO PRIVILEGES	DISABLE
SSO PIN	123456789

IKE and ESP Port Numbers

(U//FOUO) Below are the port numbers for SDD, IKE, and ESP. The operator may not change these parameters.

Protocol	Port # or Protocol ID	Description
IKE	UDP port 500	IKE is used to setup FIREFLY TEKs.
ESP	IP Protocol ID 50	ESP is used to send encrypted IP traffic.

Appendix B (U) IP/ETHERNET CONFIGURATION TIPS

B.1 (U) Introduction

Purpose

(U//FOUO) The purpose of this appendix to the TACLANE Operator's Manual is to provide additional information on sample configurations and configuration tips useful to install, operate, and configure the General Dynamics TACLANE-Micro (KG-175D).

(U//FOUO) This appendix serves as a TACLANE "cookbook" by offering tips for effectively using TACLANEs in various configurations that resemble typical user environments. The configurations described here are examples to illustrate the concepts involved. There may be other configurations that are equivalent to those described in this appendix.

B.2 (U) Example Secure IP Network

Example Secure IP Network

(U//FOUO) The diagram below shows an example IP network secured with TACLANEs.

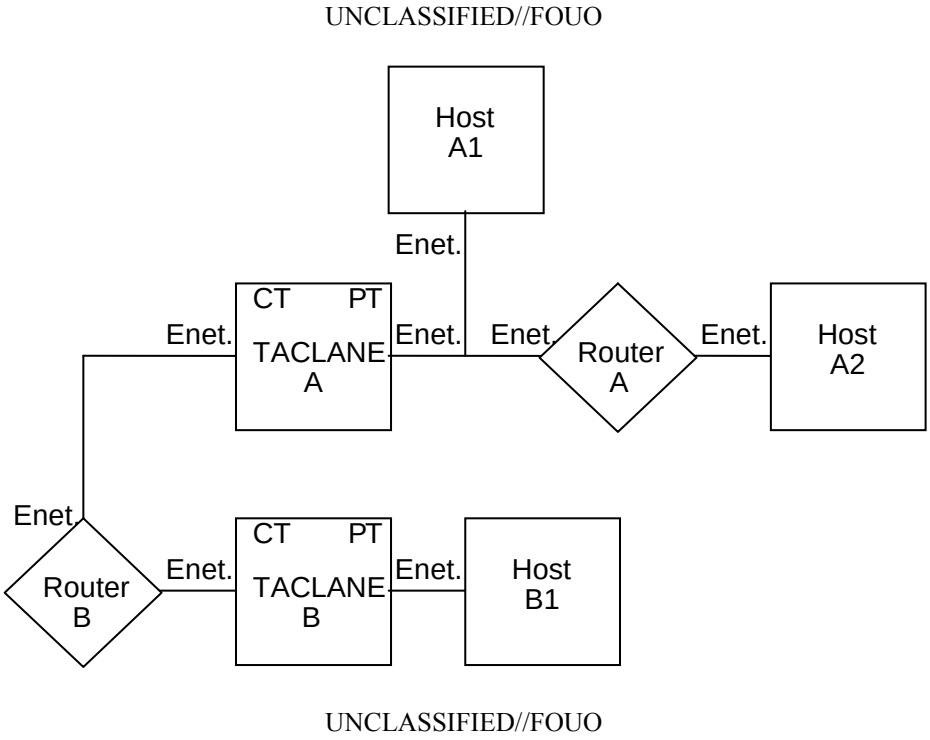


Figure B.2-1 (U) TACLANE-Secured IP/Ethernet Network

Example Secure IP Network (continued)

(U//FOUO) Router B represents the CT IP network. Router A, Host A1, Host A2, and Host B1 represent the protected PT IP network. TACLANE A fronts Host A1, Router A, and Host A2. TACLANE B fronts Host B1.

(U//FOUO) The TACLANEs secure IP datagram traffic traveling between them.

B.3 (U) General IP/Ethernet Configuration Tips

Introduction

(U//FOUO) Listed below are some general TACLANE IP configuration tips.

Single CT Default Gateway

(U//FOUO) Any outgoing CT IP datagrams that have a destination IP address that is off the local IP network/subnetwork are statically routed to the CT default gateway if configured.

(U//FOUO) If the optional CT default gateway is not configured, the TACLANE ARPs for all destination IP addresses for outgoing CT IP datagram traffic. With this configuration, ARP enhancements allow multiple CT gateways – assuming proxy-ARP support on all CT gateways.

Single PT Default Gateway

(U//FOUO) Any outgoing PT IP datagrams that have a destination IP address that is off of the local IP network/subnetwork are statically routed to the PT default gateway if configured.

(U//FOUO) If the optional PT default gateway is not configured, the TACLANE ARPs for all destination IP addresses for outgoing PT IP datagram traffic. With this configuration, ARP enhancements allow multiple PT gateways – assuming proxy-ARP support on all PT gateways.

Optimum PT IP MTU Size

(U//FOUO) For optimum performance, PT-side hosts and routers should reduce their MTU size by 100 bytes for each matched pair of TACLANEs the traffic passes through. This allows for the addition of the AH and ESP headers to each encrypted datagram without causing fragmentation.

(U//FOUO) PT-side hosts and routers fronted by a TACLANE with Fixed Packet Length processing enabled should set their MTU size equal to the fixed packet length of the fronting TACLANE. This improves performance by avoiding fragmentation in the TACLANE prior to encryption and reduces the amount of reassembly required by destination hosts. Note that if the FPL fragment/discard parameter of the fronting TACLANE is set to DISCARD, then PT-side hosts and routers must set their MTU size no greater than the fixed packet length of the TACLANE.

Continued on next page

General IP/Ethernet Configuration Tips, continued

Multicast IP Datagram Support	(U//FOUO) TACLANE allows PPKs to be assigned to Class D addresses in support of IP multicast. (U//FOUO) PT multicast traffic is encrypted and sent to the same multicast address. (U//FOUO) TACLANE does not support the use of the TTL field to limit the scope of multicast IP datagram traffic.
TACLANE Nesting	(U//FOUO) TACLANE nesting, up to three pairs deep, is supported for IP over Ethernet. Nested configurations using three pairs of TACLANEs have been tested, but three is not a hard limit.
Auto-recovery	(U//FOUO) If the TACLANE is turned off, or prime power fails, while processing user traffic, the TACLANE performs autorecovery when power is restored and automatically returns to processing user traffic: • Security associations reestablish automatically without operator intervention.
PPK Takes Precedence Over FIREFLY	(U//FOUO) For security associations, a PPK assignment takes precedence over generating a FIREFLY TEK.
Firewalls Must Pass SDD, IKE, and ESP	(U//FOUO) Any firewalls in the path between communicating TACLANEs must be configured to pass SDD, IKE, and ESP. See the Operator's Manual section on "Factory Default Settings and Port Numbers" for the port numbers for these protocols.
ARP Cache Flushing	(U//FOUO) If the TACLANE was inserted into an existing IP/Ethernet configuration, flush the ARP caches on hosts and routers before putting the TACLANE online. To flush TACLANE's ARP cache, reset the TACLANE.

Continued on next page

General IP/Ethernet Configuration Tips, continued

Automated Peer TACLANE Discovery

(U//FOUO) TACLANEs support automated peer TACLANE discovery for security associations, through the HAIPE IS Secure Dynamic Discovery (SDD) protocol. Once a peer TACLANE is identified, the following occurs:

- PPK assignments are checked for a match based on the remote TACLANE IP address. If a match is found, the corresponding PPK is used to secure the IP traffic.
- Existing security associations using FIREFLY TEKs are checked for a match based on the remote TACLANE IP address. If a match is found, the corresponding existing security association (using a FIREFLY TEK) is used to secure the IP traffic.

(U//FOUO) If there is no matching PPK assignment or security association (using a FIREFLY TEK), and an operational FIREFLY vector set is usable at the current security level, the following occurs:

- A new security association is created and the initiator and responder peer TACLANEs cooperatively generate a FIREFLY TEK using their FIREFLY vector sets.

(U//FOUO) Automated peer TACLANE discovery may be inhibited using PPKs. See the chapter on "Configuring/Managing Security Associations."

(U//FOUO) If automated peer TACLANE discovery is not desirable, remote TACLANE static routes can be defined. (See the section in the Operator's Manual titled "Configuring Remote TACLANE Static Routing.")

PT Proxy-ARP Support

(U//FOUO) TACLANE proxy-ARP replies to an ARP request received by the PT interface when the target address is covered by a static routing table entry. TACLANE will not proxy-ARP reply to a PT host based solely on a default route. The target IP address in the PT ARP request must be covered by a static routing table entry other than the default route.

Continued on next page

General IP/Ethernet Configuration Tips, continued

Remote TACLANE Static Routing Table

(U//FOUO) The operator may define a remote TACLANE routing table to associate destination IP networks/subnetworks with remote TACLANEs:

- Up to 1024 IP network/subnetwork destination entries may be defined. Entries are pooled; a maximum of 1024 entries may be created across all security levels. (The sum total of all entries at all security levels must be less than or equal to 1024).
- Entries consist of a remote TACLANE IP address, destination network ID, and prefix length.
- Routes for the local TACLANE may be included. This allows the same remote TACLANE routing table to be used in every TACLANE. **It is recommended that these routes be included when a CT default route is also defined.**
- Multiple destination IP networks/subnetworks may be associated with the same remote TACLANE IP address.
- One default route TACLANE table entry may be defined by identifying the network ID and prefix length as 0.0.0.0/0.
- Validation checks on table entries include:
  - Prefix length must be valid for the network ID.
  - No duplicate table entries (no two entries with the same network ID and prefix length). (The same network ID may be defined in multiple entries as long as the prefix lengths are different.)
- A "longest match" search of the table based on combination of network ID and prefix length is used to determine the remote TACLANE to which the IP traffic should be sent.
- **GEM X can also configure the routing table. One routing table can be generated by the GEM X and distributed to all the TACLANEs.**

PT Default Gateway or ARP Used to Deliver PT IP Traffic

- (U//FOUO) If the optional PT default gateway IP address is configured, all off-net decrypted PT IP traffic will be delivered to the PT default gateway.
- If the optional PT default gateway is not configured, TACLANE will ARP for all off-net destination IP addresses for decrypted PT IP traffic.
  - Assumes proxy-ARP support in PT routers. Proxy-ARP allows a router to reply to a received ARP request for a host in a network that is in the router's routing table.

CT Default Gateway or ARP Used to Deliver CT IP Traffic

- (U//FOUO) If the optional CT default gateway IP address is configured, all off-net encrypted CT IP traffic will be delivered to the CT default gateway.
- If the optional CT default gateway is not configured, TACLANE will ARP for all off-net destination IP addresses for encrypted CT IP traffic.
  - Assumes proxy-ARP support in CT routers. Proxy-ARP allows a router to reply to a received ARP request for a host in a network that is in the router's routing table.

When a CT default gateway is defined, it is recommended that a route for the local TL-protected network also be included in the static routing table.

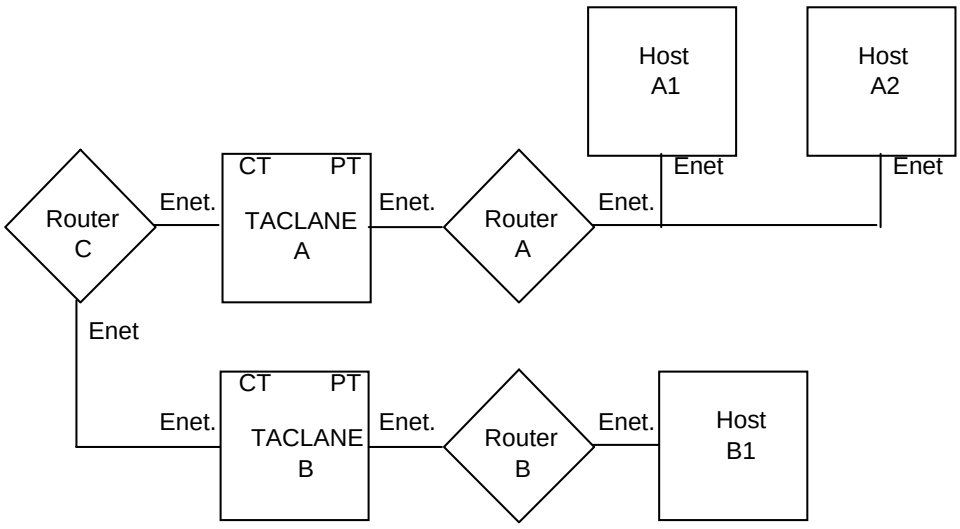
B.4 (U) IP Routing Workarounds

Introduction

(U//FOUO) This example illustrates several workarounds to configuring static IP routes on CT routers. The CT network, represented by Router C, knows about the two directly-connected networks. However, Router C does not know about the networks served by Router A and Router B. The typical solution to this problem is to use static IP routes between PT/CT routers for the networks they serve.

(U//FOUO) Note: Remote TACLANE static routing eliminates the need for static routes to PT networks on CT routers, and vice versa – and also eliminates the need for the IP routing workarounds described in this section.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.4-1 (U) TACLANE Configuration

(U//FOUO) However there are scenarios where this is not desirable:

- User does not control the CT network: e.g., the administrators of Router C may not allow the configuration of Router C to be changed.
- User networks are not routable over the CT network: e.g., the TACLANE user is using a private IP network (such as network 10.0.0.0) and the CT network does not route traffic for private IP networks.
- The number of user networks is large: T he number of user networks makes configuration of static IP routes on Router C cumbersome (e.g., Router B fronts the Internet).

IP Routing Workarounds, continued

Two Example Solutions

(U//FOUO) This section describes two example configurations. The first example uses PPKs and the second uses IP tunnels.

(U//FOUO) Note: Remote TACLANE static routing eliminates the need for static routes to PT networks on CT routers, and vice versa – and also eliminates the need for the IP routing workarounds described in this section.

Manual PPK Configuration

(U//FOUO) One option is to manually configure each TACLANE with IP PPK assignments including each remote host IP address that is reachable behind every other TACLANE. This same solution, but to a different problem, is illustrated in "Multiple Gateways from Network."

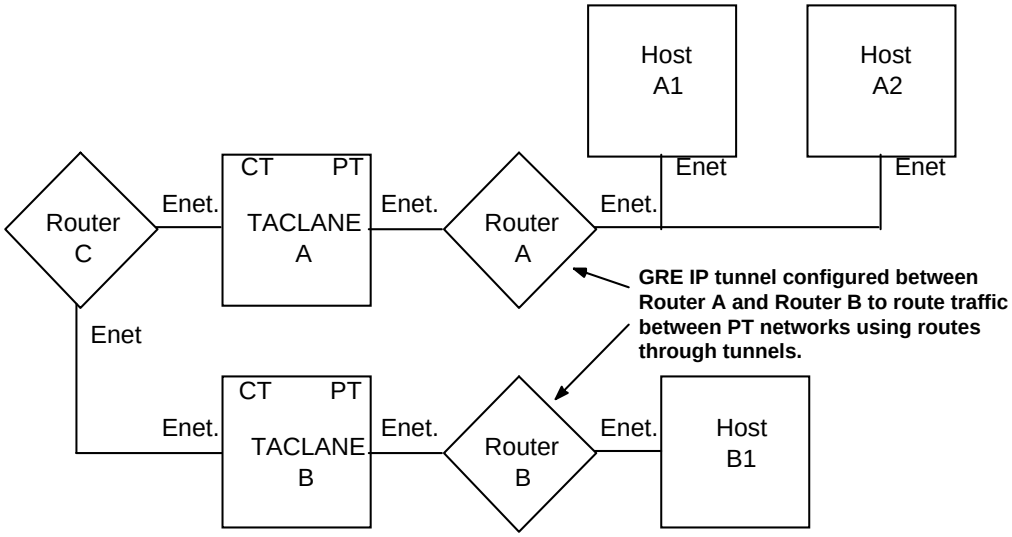
How it Works

(U//FOUO) This lets the source TACLANE know the IP address of the destination TACLANE ahead of time, so the TACLANE does not have to rely on the CT network to route automated peer TACLANE discovery messages to the correct TACLANE.

PT Router IP Tunnels

(U//FOUO) Another option is to configure IP tunnels (e.g., Cisco GRE IP tunnels) between each router. Static routes may be defined to route traffic between hosts (and networks) through the tunnels. This example solution is shown in the figure below.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.4-2 (U) TACLANE Configuration With IP Tunnels

How it Works

(U//FOUO) All IP datagram traffic between PT hosts is encapsulated by the PT routers supporting the GRE IP tunnels, and all resulting encapsulated IP datagrams have the source and destination IP addresses of tunnel endpoints (Router A and Router B). The CT network (Router C) only needs to route between the Router A and Router B IP addresses in the directly-connected networks known to Router C.

(U//FOUO) Note that since the added PT-side routers can communicate with each other (since they are behind TACLANEs), it is possible for these routers to exchange dynamic routing information (e.g., using BGP) to reduce the need for manual configuration.

B.5 (U) Connecting Networks Using a Different IP Encryptor

Introduction

(U//FOUO) In this example, there are users behind TACLANEs and users behind different IP encryptors that need to intercommunicate.

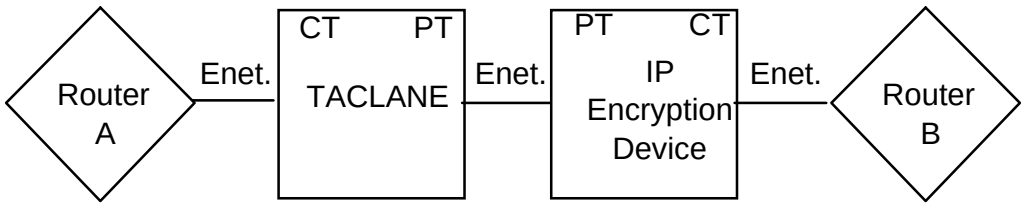
TACLANE Encryption Gateway

(U//FOUO) A solution is to provide a TACLANE encryption gateway. Such a gateway consists of a TACLANE and a different IP encryptor connected either back-to-back directly or back-to-back via a PT-side router. There are two basic scenarios. The first scenario is connecting two networks where one network uses TACLANE and the other network uses a different IP encryptor. The second scenario is connecting many subnet enclaves where some subnets use TACLANE and some subnets use a different IP encryptor.

Connecting Two Networks

(U//FOUO) To directly connect two networks, the TACLANEs are connected back-to-back directly. This solution is shown in the diagram below. Router A and Router B represent the connection between the two networks.

UNCLASSIFIED//FOUO



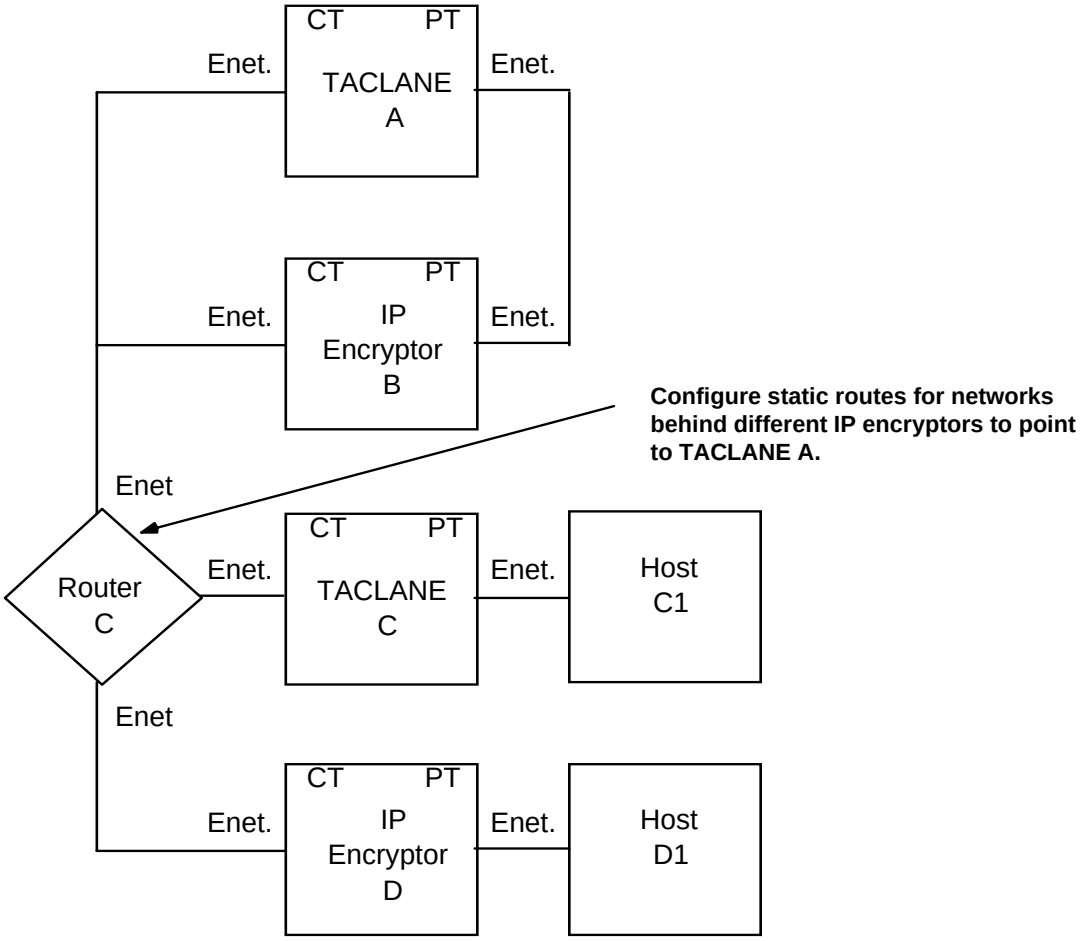
UNCLASSIFIED//FOUO

Figure B.5-1 (U) TACLANE Encryption Gateway Connecting Two Networks

Connecting Many Subnet Enclaves

(U//FOUO) To connect many subnet enclaves where some subnets use TACLANE and some subnets use a different IP encryptor, a TACLANE encryption gateway is needed that can be reached from anywhere in the network. This solution is shown in the figure below. (Note that routers do not need to be configured with static routes if all TACLANEs support static routing.)

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.5-2 (U) TACLANE Encryption Gateway Connecting Many Subnet Enclaves

(U//FOUO) The CT network represented by Router C requires at least a static route for the network behind IP Encryptor D to point to TACLANE A. This is needed to route automated peer discovery messages to the correct TACLANE. The routing configuration may need further modification depending on the nature of the different IP encryptor. Note that this solution can be augmented with the solutions from "IP Routing Workarounds", or static routing capabilities.

How it Works

(U//FOUO) In both scenarios, the TACLANE encryption gateway works by having the different IP encryptor decrypt IP datagram traffic before it is encrypted again by the TACLANE, and vice versa.

B.6 (U) Connecting Networks at Different Security Levels

Introduction

(U//FOUO) In this example, there are two base networks, one Secret and one Unclassified. In order to share network infrastructure and provide flexibility, administrators need to deploy Secret hosts on the Unclassified network, deploy Unclassified hosts on the Secret network, and allow all hosts to communicate with their respective base networks.

(U//FOUO) Note: Remote TACLANE static routing eliminates the need for static routes to PT networks on CT routers, and vice versa – and may greatly simplify the configurations described in this section.

Two Example Configurations

(U//FOUO) This section describes two example configurations of TACLANE-protected gateways between networks at different security levels. The first example uses multiple TACLANEs between two networks, and the second uses a single TACLANE between two networks – making use of nested TACLANEs to obtain the needed isolation.

(U//FOUO) Note that these are only examples to illustrate the concepts involved. There may be other configurations that are equivalent to those discussed here. All of the example IP networks are Class B networks.

(U//FOUO) Note: Remote TACLANE static routing eliminates the need for static routes to PT networks on CT routers, and vice versa – and may greatly simplify the configurations described in this section.

Continued on next page

(U) Connecting Networks at Different Security Levels, continued

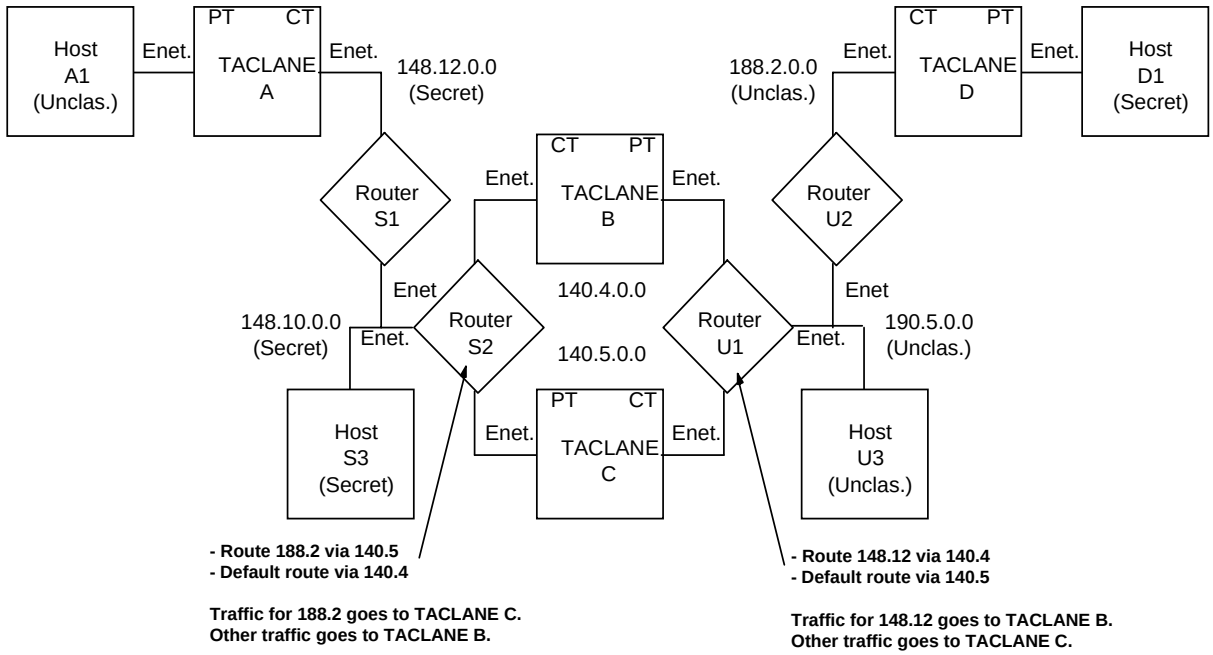
Multiple Gateway Configuration

(U//FOUO) In this example, there is a Secret IP network (148.10) and an Unclassified IP network (190.5). There are Unclassified hosts (Host A1) homed on the Secret network that need to communicate with the Unclassified network, and there are Secret hosts (Host D1) homed on the Unclassified network that need to communicate with the Secret network.

(U//FOUO) To provide the needed connectivity, two TACLANEs are configured between the routers (Router S2 and Router U1), each TACLANE within its own IP network (the Unclassified TACLANE (TACLANE B) is on 140.4.0.0 and the Secret TACLANE (TACLANE C) is on 140.5.0.0). The enclave of Unclassified hosts on the Secret network must be contained within a separate IP network (148.12.0.0). Similarly, the enclave of Secret hosts on the Unclassified network must be contained within a separate IP network (188.2.0.0). Note that the positioning of the TACLANE to the left or to the right of the IP routers serving 148.12.0.0 (Router S1) and 188.2.0.0 (Router U2) does not matter.

(U//FOUO) The IP routers connected to the two TACLANEs are configured to route traffic to the correct TACLANE based on destination IP network. The Secret router (Router S2) is configured to route IP destined for 188.2.0.0 via the 140.5.0.0 network, and to default route to the 140.4.0.0 network. The Unclassified router (Router U1) is configured to route IP destined for 148.12.0.0 via the 140.4.0.0 network, and to default route to the 104.5.0.0 network. Note that all routes between the CT and PT side of any TACLANE are static routes.
(U//FOUO) This example is shown in the figure below:

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.6-1 (U) TACLANE Multiple Gateway Configuration Example

How it Works

(U//FOUO) All IP traffic from the Secret network to the Secret enclave on the Unclassified network is routed through the Secret TACLANE (TACLANE C). All other traffic from the Secret network is routed through the Unclassified TACLANE (TACLANE B). Similarly, all IP traffic from the Unclassified network to the Unclassified enclave on the Secret network is routed through the Unclassified TACLANE (TACLANE B). All other traffic from the Unclassified network is routed through the Secret TACLANE (TACLANE C). Note that this is secure because even if the router routes traffic incorrectly, the traffic is discarded and/or unintelligible if it reaches the wrong TACLANE.

Continued on next page

(U) Connecting Networks at Different Security Levels, continued

Supporting Three or More Levels

(U//FOUO) This example configuration works when two different security levels are involved. To support interconnection of networks where three or more security levels are involved, nested TACLANE configurations (as described below) need to be added to support the additional security levels.

(U//FOUO) Note: TACLANE nesting has been tested in configurations of up to three pairs deep. Due to the encryption overhead imposed by each additional level, it is recommended that nesting be kept to a minimum.

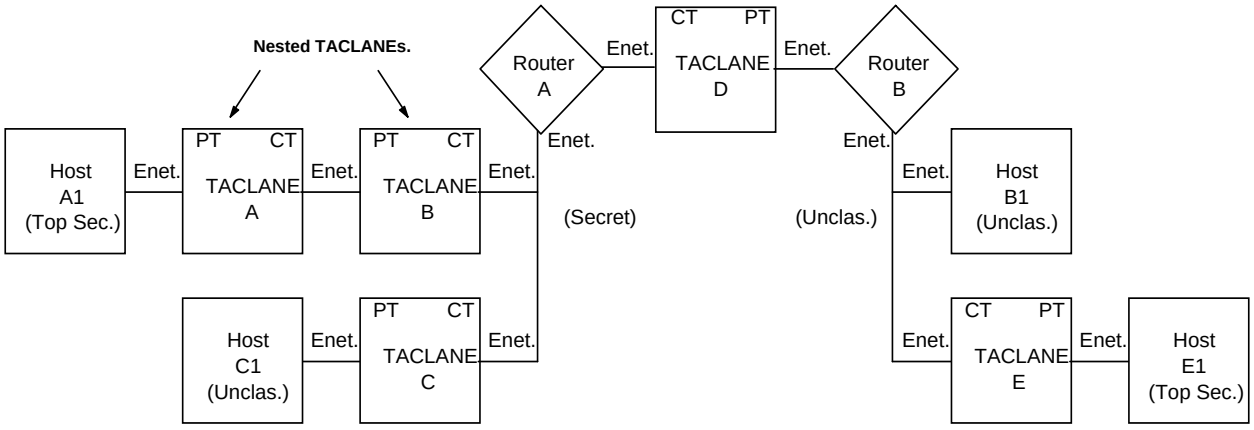
Single Gateway Nested Configuration

(U//FOUO) In this example, there is a Secret IP network and an Unclassified IP network. There are Unclassified hosts homed on the Secret network that need to communicate with the Unclassified network, and there are Top Secret hosts homed on the Secret network that need to communicate with Top Secret hosts homed on the Unclassified network.

(U//FOUO) To provide the needed connectivity, one TACLANE is configured between the routers within its own IP network (TACLANE D). There is no need to isolate enclaves of hosts within separate IP networks. TACLANE A and TACLANE E are set to Top Secret. TACLANE B and TACLANE C are set to Unclassified. TACLANE A and TACLANE B are in a nested TACLANE configuration.

(U//FOUO) The IP routers connected to the TACLANE are configured to default static route traffic to the opposite router.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.6-2 (U) TACLANE Single Gateway Nested Configuration Example

(U) Connecting Networks at Different Security Levels, continued

How it Works

(U//FOUO) All IP traffic between the Unclassified network and the Unclassified enclaves on the Secret network travels through a pair of Unclassified TACLANEs (TACLANE B and TACLANE D, or TACLANE C and TACLANE D). Host C1 communicates with Host B1 through TACLANE C and TACLANE D. Top Secret traffic between Host A1 and Host E1 is handled by the nested TACLANE configuration. TACLANE A and TACLANE E are peer Top Secret TACLANEs, and TACLANE B and TACLANE D are peer Unclassified TACLANEs. The nested TACLANE configuration overlays the protected Top Secret traffic over the Unclassified traffic in order for it to be able to use the same TACLANE-protected network. This is secure because of the TACLANE nesting. The Unclassified TACLANEs isolate Unclassified traffic from the Secret network, and the Top Secret TACLANEs isolate traffic from the Unclassified network.

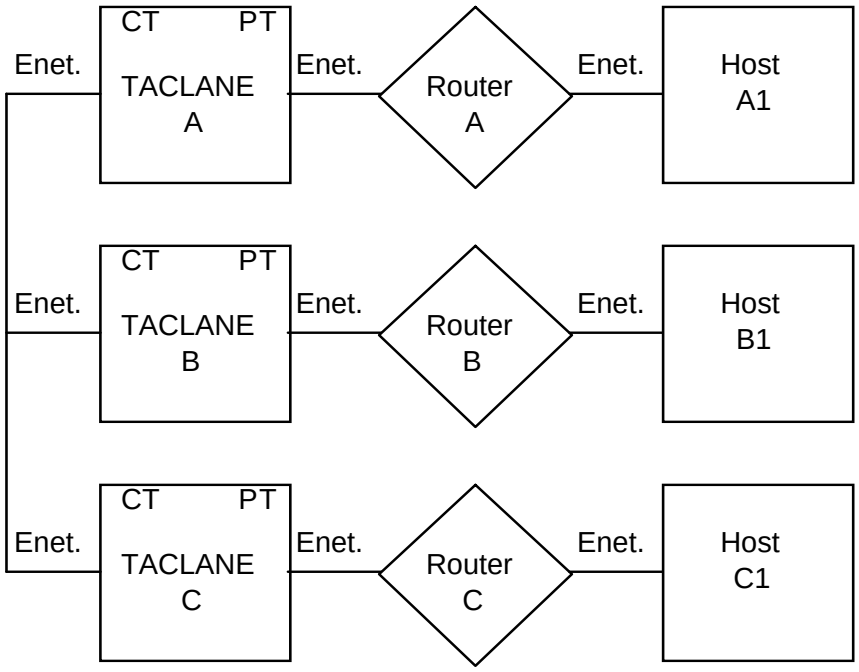
B.7 (U) Multiple Gateways from Network

Introduction

(U//FOUO) In this example, there is one backbone network and three TACLANE-protected networks off of the backbone network. Each TACLANE-protected network is at the same security level. This configuration is illustrated in the figure below.

(U//FOUO) Note: Remote TACLANE static routing ARP enhancements allow multiple PT or CT gateways to be supported with the only requirement that these multiple gateways support proxy-ARP. TACLANEs ARP for off-net destinations when the PT or CT default gateway is not defined.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.7-1 (U) Multiple CT Default Gateways

Continued on next page

(U) Multiple Gateways from Network, continued

Introduction (continued)

(U//FOUO) Each TACLANE in this configuration has two possible CT Default Gateways for which to send off-net CT datagrams. For example, TACLANE A could send off-net CT datagrams to Router B or Router C. Since Router A, Router B, and Router C can communicate with each other (since all are behind TACLANEs) they can exchange routing protocol information and learn where off-net datagram traffic needs to be routed. Although the router knows where it wants to forward the off-net datagram, the TACLANE cannot benefit from the router's decision, and must make the decision again. Since the TACLANE only supports a single CT Default Gateway, the TACLANE sends all off-net CT datagrams to that single CT Default Gateway – whether or not it is really the correct router.

(U//FOUO) It is possible to make this configuration work if each TACLANE points to a different router as its single CT Default Gateway. Since the purpose of a router is to route, a router attempts to forward an errant datagram to its proper destination. Thus, off-net datagrams may need to bounce off one incorrect router, and pass through pairs of TACLANEs twice, before arriving at the proper destination.

Four Example Configurations

(U//FOUO) This section details three possible solutions that allow this configuration to work more efficiently. A fourth option is also mentioned. Note that these are only examples to illustrate the concepts involved. There may be other configurations that are equivalent to those discussed here.

(U//FOUO) Note: Remote TACLANE static routing ARP enhancements allow multiple PT or CT gateways to be supported with the only requirement that these multiple gateways support proxy-ARP. TACLANEs ARP for off-net destinations when the PT or CT default gateway is not defined.

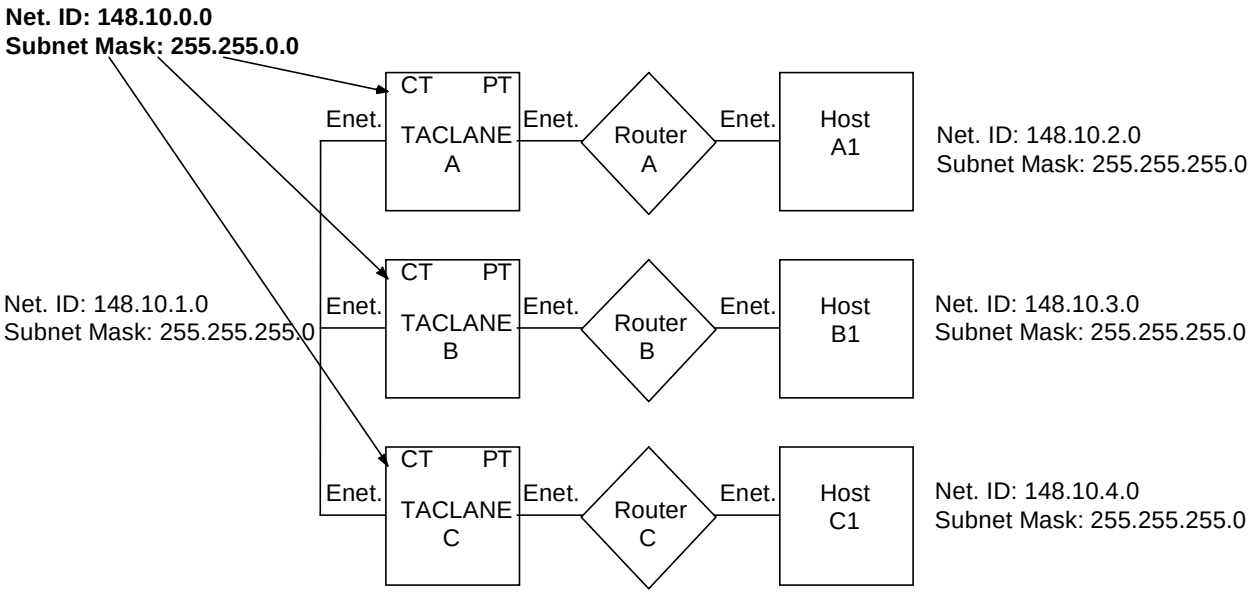
False Subnet Mask Configuration

(U//FOUO) One option is to use a false subnet mask in the TACLANEs. To make this work:

- The configuration must consist of subnetworks that all fit within a higher level network or subnet.
- Router A, Router B, and Router C must be configured to support proxy-ARP for the networks they serve.

(U//FOUO) This example solution is shown in the figure below.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.7-2 (U) False Subnet Mask Configuration

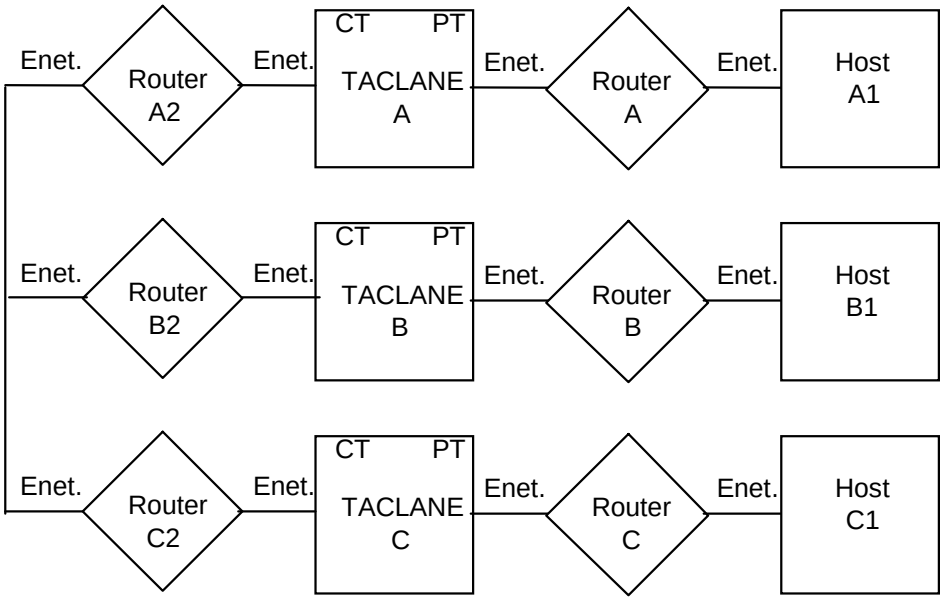
How it Works

(U//FOUO) In this example, the backbone network and the networks served by Router A, Router B, and Router C all fit with the Class B network 148.10.0.0. Although every other component in the network is configured to use the proper 24-bit subnet mask, the TACLANEs are configured with the standard Class B mask. This solution "fools" the TACLANEs into thinking everything is on the same network. When a TACLANE relays an ARP from the CT to PT side, the router proxy-ARP replies if the IP address is located behind it.

Added Router Configuration

(U//FOUO) Another option is to place extra routers on the CT side of each TACLANE, placing each TACLANE in its own IP subnet. This example solution is shown in the figure below.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.7-3 (U) Added Router Configuration

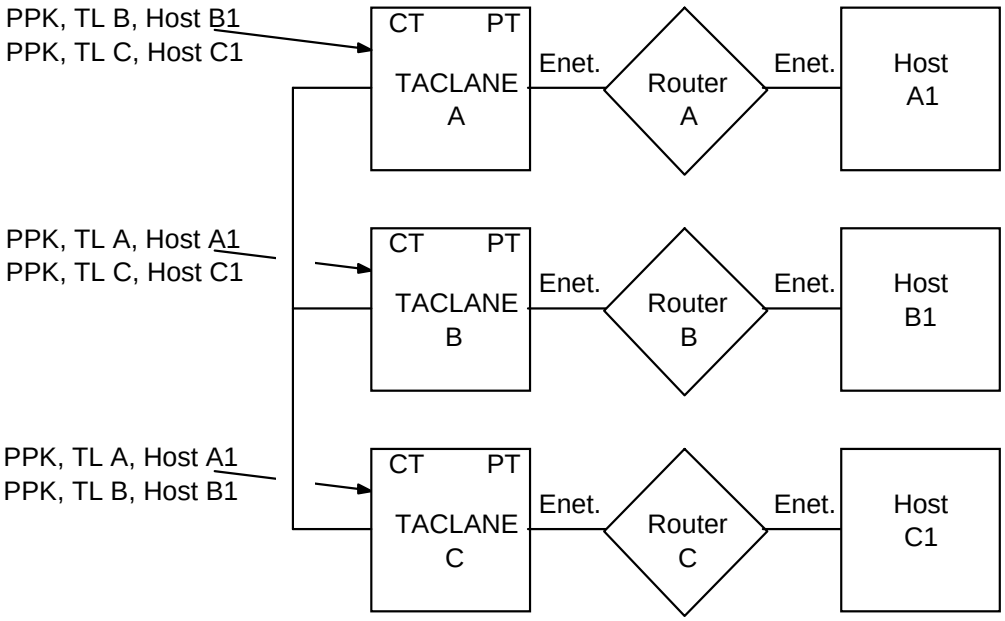
How it Works

(U//FOUO) This solution provides one destination IP address for each TACLANE to forward off-net CT datagrams to. Each added router becomes a CT Default Gateway for each respective TACLANE. The added routers take care of routing datagrams to the proper destination.

Manual PPK Configuration

(U//FOUO) Another option is to manually configure each TACLANE with IP PPK assignments including each remote host IP address that is reachable behind every other TACLANE. This example solution is shown in the figure below.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.7-4 (U) Manual PPK Configuration

How it Works

(U//FOUO) This lets the source TACLANE know the IP address of the destination TACLANE ahead of time, so it does not have to rely on the CT Default Gateway or automated peer TACLANE discovery messages to find the correct destination TACLANE.

IP Tunnel Configuration

(U//FOUO) Another option is to configure Router A, Router B, and Router C to use IP tunnels to encapsulate IP datagram traffic traveling between them. See "IP Routing Workarounds" for a description.

How it Works

(U//FOUO) To the TACLANEs, this option makes all IP datagram traffic appear to be destined for on-net destinations (the routers).

B.8 (U) Redundancy Configurations

Introduction

(U//FOUO) Several user communities require TACLANE redundancy. Usually the requirement is for failover redundancy at a single high value TACLANE-protected enclave (e.g., WAN gateway or server farm), but redundancy can be implemented at any number of enclaves in a community. The case where the high value enclave is protected by two or more TACLANEs and client enclaves are each protected by a single TACLANE is referred to as single-ended redundancy. The case where every enclave is protected by two or more TACLANEs is referred to as double-ended redundancy.

(U//FOUO) The level of TACLANE redundancy that is required at a TACLANE-protected enclave is typically two TACLANEs. Some user communities have a requirement to protect a high value enclave with as many as six TACLANEs. The configuration will also incorporate router redundancy if the redundancy requirement extends beyond TACLANE to the router on the Plaintext (PT) side. The redundancy requirement usually includes the capability to load balance between the redundant TACLANEs that protect an enclave when more than one TACLANE is operational.

(U//FOUO) Currently, TACLANE does not have an internal redundancy function. The TL operator must rely on routing protocols to implement TACLANE redundancy. The examples in this section are limited to the configuration of Cisco Systems' Generic Routing Encapsulation (GRE) tunnels and a routing protocol running on PT routers as a means to provide TACLANE redundancy. Other TACLANE redundancy configurations may be possible (e.g., using the Virtual Redundant Router Protocol (VRRP) or Cisco Systems' Hot Standby Routing Protocol (HSRP)), but they have not yet been tested by General Dynamics.

(U//FOUO) Note: Each of the redundancy configurations described in this section can be implemented with either PrePlaced Key (PPK) or FIREFLY vector sets.

Single-Ended Redundancy

(U//FOUO) Two examples of single-ended redundancy configurations are presented here, each showing encrypted SIPRNET traffic tunneled through the NIPRNET. The first example provides router redundancy as well as TACLANE redundancy; the second example provides only TACLANE redundancy. FIREFLY or PrePlaced Key Security Associations can be used between TACLANEs in either example.

(U//FOUO) The TACLANE operator must choose how to configure the TLs. One option is to assign the CT and PT IP addresses to a single black (NIPRNET) subnet. In this case, the red (SIPRNET) and black (NIPRNET) address spaces are separated at the router on the PT side of each TACLANE. Another option is to assign each TL a black (NIPRNET) CT IP address and a red (SIPRNET) PT IP address and configure each TL with static routes.

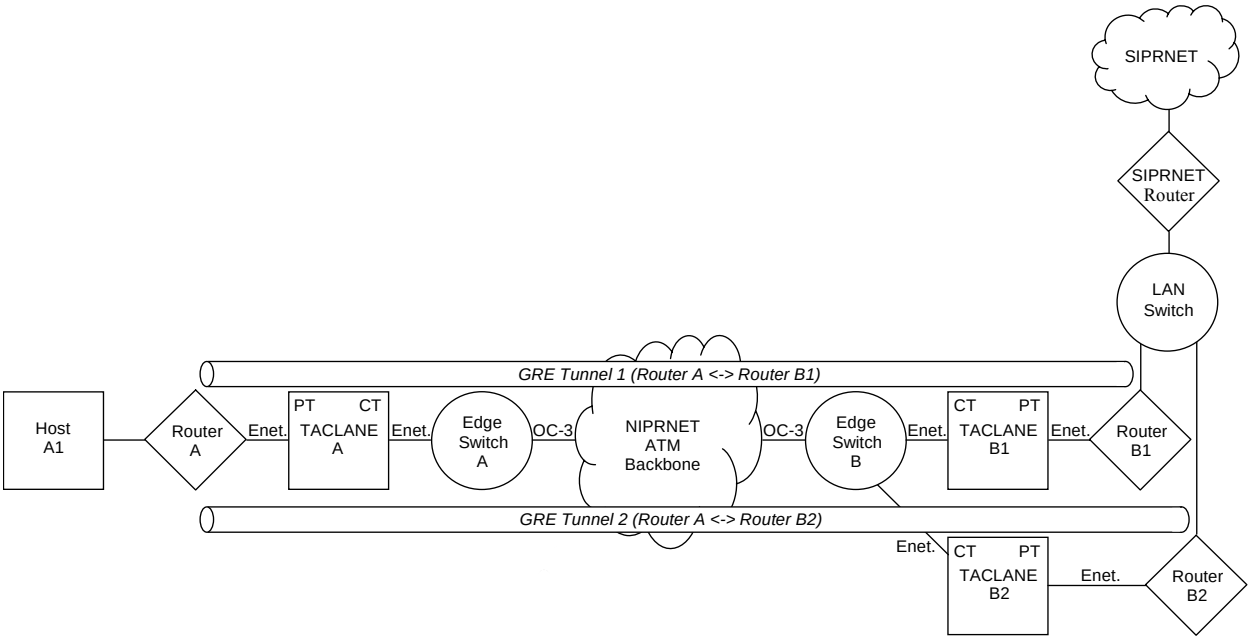
Single-Ended Redundancy with Router Redundancy

(U//FOUO) The figure below is a two-enclave illustration of a base network where TACLANE redundancy is configured only at a gateway enclave, in this case a gateway to the global SIPRNET. Up to 253 SIPRNET enclaves on the base network, represented by the enclave on the left, can be full-time clients of the gateway enclave. An unlimited number of enclaves can be part-time clients. The SIPRNET hosts in a client enclave are able to access the global SIPRNET through either of the two TACLANE/router pairs at the gateway enclave.

(U//FOUO) Failover redundancy is provided by configuring:

- two GRE tunnel interfaces (Tunnel 1 and Tunnel 2) at the client router (Router A)
- a GRE tunnel interface at Router B1 terminating Tunnel 1
- a GRE tunnel interface at Router B2 terminating Tunnel 2
- the same routing protocol (e.g., BGP, EIGRP, OSPF, or RIP) at the client router (Router A) and gateway routers (Router B1 and Router B2), to advertise routes to SIPRNET subnets via the GRE tunnels.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.8-1 (U) Single-Ended TACLANE Redundancy with Router Redundancy

Continued on next page

(U) Redundancy Configurations, continued

How it Works

(U//FOUO) Each GRE tunnel connects the client red router (Router A) and TACLANE with a different red router and TACLANE at the gateway enclave. The routing protocol running on the red routers periodically sends keep-alives (or Hellos) through the GRE tunnels to the routers on the other end. A router will detect that a GRE tunnel is down when it ceases to receive routing protocol keep-alives from the router at the other end of the tunnel. The failure/unavailability of a gateway TACLANE disables one GRE tunnel and causes the client red router to route packets for the gateway enclave or off-base SIPRNET subnets through the other GRE tunnel (gateway TACLANE/router pair) until the disabled GRE tunnel is again available. The SIPRNET Router exchanges routing information with the gateway red routers and will route all packets for the client SIPRNET subnet to the gateway red router that continues to report a route (GRE tunnel path) to the subnet when the other gateway red router or its connected TACLANE fails or becomes unavailable.

(U//FOUO) Note: The interval between keep-alives and the amount of time that the routing protocol will wait for a keep-alive before declaring a tunnel down can be set so that failover occurs in a few seconds.

Load-Balancing

(U//FOUO) The client router (Router A) and the SIPRNET Router automatically balance the load of packets they send to the two GRE tunnels (gateway TACLANE/router pairs), when the cost of the two GRE tunnels is equal and both tunnels are up. The routers will load-balance either on a per-packet basis or on a per-destination basis, depending on whether fast switching is enabled at the tunnel interfaces.

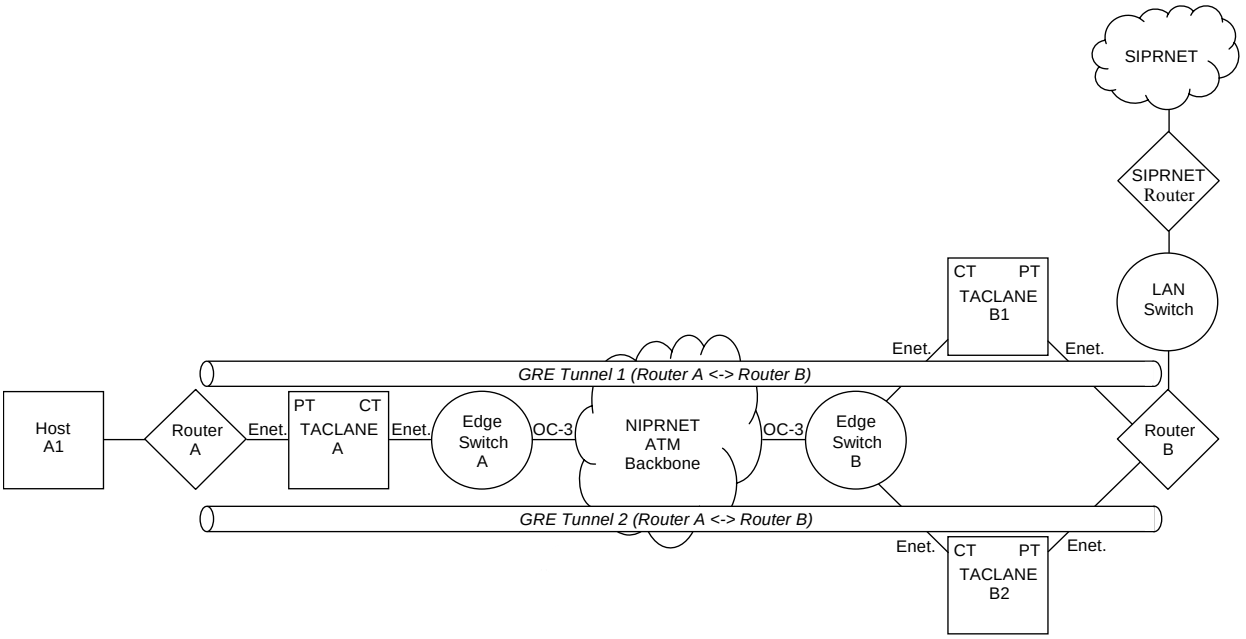
Note on Multicast Routing Protocol Packets

(U//FOUO) Depending on the routing protocol, the protocol can be configured with or without the GRE tunnel interface of the other red router as a protocol neighbor. The GRE tunnels will support the multicast routing protocol messages (e.g., "all OSPF routers") that routers exchange when neighbors are not configured. A GRE tunnel interface will encapsulate a multicast routing protocol packet with a unicast IP header, addressed to the other tunnel end.

Single-Ended Redundancy without Router Redundancy

(U//FOUO) The figure below is another two-enclave example of a base network where TACLANE redundancy is configured only at a gateway enclave. The number of gateway red routers has been reduced to one, making this configuration applicable when the redundancy requirement does not extend beyond the TACLANE. Note that the failure/unavailability of the gateway red router (Router B) will disable both GRE tunnels and the use of both TACLANEs at the gateway.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.8-2 (U) Single-Ended TACLANE Redundancy without Router Redundancy

Continued on next page

(U) Redundancy Configurations, continued

Single-Ended Redundancy without Router Redundancy (continued)

(U//FOUO) Failover redundancy is provided by configuring:

- a secondary IP address assigned to the TACLANE interface of the client red router (Router A)
- two GRE tunnel interfaces (Tunnel 1 and Tunnel 2) at Router A (one using the primary address, and the other using the secondary address)
- two GRE tunnel interfaces at Router B terminating Tunnel 1 and Tunnel 2, the same routing protocol (e.g., BGP, EIGRP, OSPF, or RIP) at the client router (Router A) and gateway router (Router B), to advertise routes to SIPRNET subnets via the GRE tunnels.

How it Works

(U//FOUO) The secondary address at the client red router (Router A) allows the gateway red router (Router B) to distinguish between the client ends of the two GRE tunnels, to forward packets for the client end of GRE Tunnel 1 to TACLANE B1, and to forward packets for the client end of GRE Tunnel 2 to TACLANE B2. A secondary IP address is not required for Router B, since it uses a separate physical interface (with a unique IP address) for each GRE tunnel (gateway TACLANE).

(U//FOUO) The two PT interfaces of TACLANE B1 and TACLANE B2 could be connected to a single interface of Router B (through a hub or switch) by assigning a secondary address to the router interface, assigning TACLANE B1 to the primary subnet of the interface, and assigning TACLANE B2 to the secondary subnet of the interface. This causes the client TL (TACLANE A) to discover that TACLANE B1 fronts the gateway end of GRE Tunnel 1 and that TACLANE B2 fronts the gateway end of GRE tunnel 2.

(U//FOUO) Failover redundancy functions in this example as it was described in the previous example, except that the gateway red router selects the GRE tunnel (gateway TACLANE) that carries a packet to the client SIPRNET subnet. Recall that it was the SIPRNET Router that selected the GRE tunnel in the first example, by forwarding the packet to one of the gateway red routers.

Double-Ended Redundancy

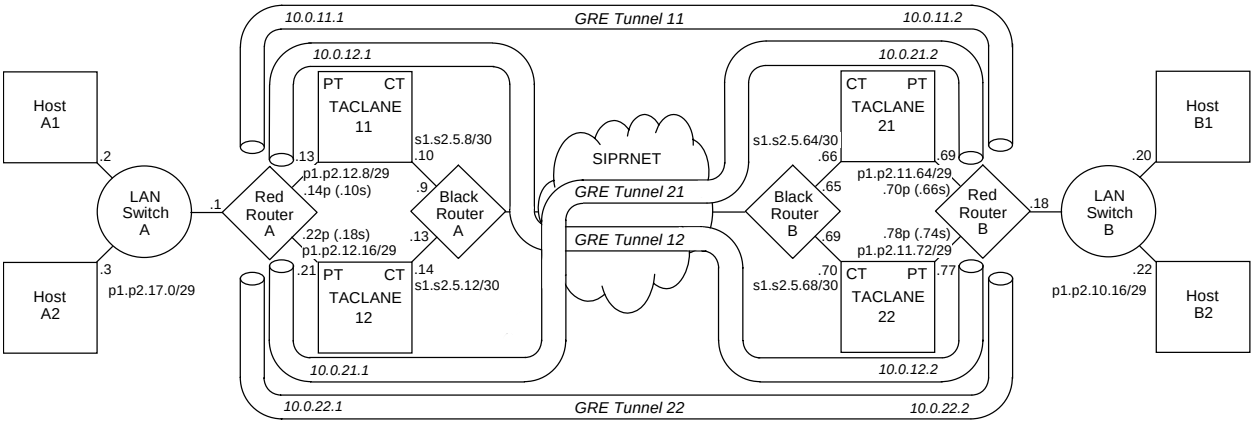
(U//FOUO) As the name implies, double-ended redundancy provides redundancy at both ends of a connection between two high value enclaves. Double-ended redundancy between two TACLANE-protected enclaves can be implemented by configuring either two or four GRE tunnels between the red routers of the enclaves. Only the four tunnel case is illustrated here, as the two tunnel case is a subset of the four tunnel case.

(U//FOUO) Double-ended redundancy can be implemented by configuring all the TACLANEs for static routing or by configuring all the TACLANEs for same subnet operation using dynamic discovery. As with single-ended redundancy, either FIREFLY or PrePlaced Key Security Associations can be used between the TACLANEs. Also, TACLANEs can be used in any combination.

Double-Ended Redundancy with Four GRE Tunnels

(U//FOUO) The figure below depicts a two-enclave network where failover redundancy is provided at both enclaves by configuring four GRE tunnels and a routing protocol between the red routers at the two enclaves. Remote TACLANE static routing is used in this example; the red (private) and black (SIPRNET) address spaces are separated at each TACLANE. Subnets beginning with "p1.p2" are private, and subnets beginning with "s1.s2" are SIPRNET subnets.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Figure B.8-3 (U) Using Four GRE Tunnels to Provide Double-Ended TACLANE Redundancy without Router Redundancy

---

Partial Device Configurations

(U//FOUO) The following table contains partial configurations for devices in this example:

TACLANE 11 Static Routes			TACLANE 21 Static Routes		
Net ID	Net Mask	TL CT IP	Net ID	Net Mask	TL CT IP
p1.p2.11.68	255.255.255.252	s1.s2.5.66	p1.p2.12.12	255.255.255.252	s1.s2.5.10
p1.p2.11.76	255.255.255.252	s1.s2.5.70	p1.p2.12.16	255.255.255.252	s1.s2.5.14
TACLANE 12 Static Routes			**TACLANE 22 Static Routes**		
Net ID	Net Mask	TL CT IP	Net ID	Net Mask	TL CT IP
p1.p2.11.64	255.255.255.252	s1.s2.5.66	p1.p2.12.10	255.255.255.252	s1.s2.5.10
p1.p2.11.72	255.255.255.252	s1.s2.5.70	p1.p2.12.18	255.255.255.252	s1.s2.5.14
Hosts A1 and A2			**Hosts B1 and B2**		
Default gateway: p1.p2.17.1			Default gateway: p1.p2.10.18		

Partial Device Configurations (continued)

(U//FOUO) The partial configurations listed below have been tested with Cisco routers that support BGP and GRE tunnel configuration.

Red Router A	Red Router B
interface tunnel 11	interface tunnel 11
ip address 10.0.11.1 255.255.255.0	ip address 10.0.11.2 255.255.255.0
tunnel source p1.p2.12.14	tunnel source p1.p2.11.70
tunnel destination p1.p2.11.70	tunnel destination p1.p2.12.14
interface tunnel 12	interface tunnel 12
ip address 10.0.12.1 255.255.255.0	ip address 10.0.12.2 255.255.255.0
tunnel source p1.p2.12.10	tunnel source p1.p2.11.78
tunnel destination p1.p2.11.78	tunnel destination p1.p2.12.10
interface tunnel 21	interface tunnel 21
ip address 10.0.21.1 255.255.255.0	ip address 10.0.21.2 255.255.255.0
tunnel source p1.p2.12.18	tunnel source p1.p2.11.66
tunnel destination p1.p2.11.66	tunnel destination p1.p2.12.18
interface tunnel 22	interface tunnel 22
ip address 10.0.22.1 255.255.255.0	ip address 10.0.22.2 255.255.255.0
tunnel source p1.p2.12.22	tunnel source p1.p2.11.74
tunnel destination p1.p2.11.74	tunnel destination p1.p2.12.22
router bgp 1	router bgp 2
maximum-paths 4	maximum-paths 4
timers bgp 5 15	timers bgp 5 15
neighbor 10.0.11.2 remote-as 2	neighbor 10.0.11.1 remote-as 1
neighbor 10.0.12.2 remote-as 2	neighbor 10.0.12.1 remote-as 1
neighbor 10.0.21.2 remote-as 2	neighbor 10.0.21.1 remote-as 1
neighbor 10.0.22.2 remote-as 2	neighbor 10.0.22.1 remote-as 1
network p1.p2.17.0 255.255.255.248	network p1.p2.10.16 255.255.255.248
ip route p1.p2.11.64 255.255.255.252 p1.p2.12.21	ip route p1.p2.12.8 255.255.255.252 p1.p2.11.77
ip route p1.p2.11.68 255.255.255.252 p1.p2.12.13	ip route p1.p2.12.12 255.255.255.252 p1.p2.11.69
ip route p1.p2.11.72 255.255.255.252 p1.p2.12.21	ip route p1.p2.12.16 255.255.255.252 p1.p2.11.69
ip route p1.p2.11.76 255.255.255.252 p1.p2.12.13	ip route p1.p2.12.20 255.255.255.252 p1.p2.11.77

How it Works

(U//FOUO) A unique IP address is provided for each GRE tunnel endpoint by assigning both a primary and a secondary address to each TACLANE-connected red router interface. The unique tunnel endpoint addresses allow a red router to route the packets for the destination ends of two tunnels to one connected TACLANE and to route the packets for the destination ends of the other two tunnels to the second connected TACLANE. The unique addresses also allow a TACLANE to route encrypted packets to different TACLANEs at the other enclave depending on the destination (tunnel endpoint) address. Accordingly, four static routes are configured at each red router and two static routes are configured at each TACLANE. The result is that the path of each GRE tunnel passes through a different combination of TACLANEs, one from each enclave.

(U//FOUO) The same routing protocol (BGP-4 in this example) is enabled at each red router and configured to advertise the private host subnet of its enclave via each of the four GRE tunnels. The red routers will detect that a GRE tunnel is down when they cease to receive routing protocol keep-alives from the red router at the other enclave through the tunnel. The failure/unavailability of a TACLANE at one enclave will disable two GRE tunnel paths and cause each red router to route all the packets for the private host subnet of the other enclave through the two remaining GRE tunnels. The overlapping failure/unavailability of a TACLANE at the opposite enclave will disable a third GRE tunnel path and cause each red router to route all the packets for the private host subnet of the other enclave through the one remaining GRE tunnel. The BGP-4 router configurations shown will failover in 15 seconds.

(U//FOUO) In the figure, the PT interface of each TACLANE connects to a different interface of the red router at each enclave. The PT interfaces of the two TACLANEs could connect to a single red router interface at an enclave if a total of four IP addresses (one primary plus three secondary) were assigned to the router interface. This would reduce the number of static routes required at the other red router from four to two.

Analysis

(U//FOUO) The four GRE tunnel configuration is more robust that a two GRE tunnel configuration. With only two tunnels, the probability is 0.5 that the overlapping failure/unavailability of one TACLANE at each enclave will disable communications between the private subnets of the two enclaves. This can be seen by visualizing that only GRE Tunnel 11 and GRE Tunnel 22 are configured. The failure of TACLANE 21 will disable GRE Tunnel 11 and remove TACLANE 11 from service. The overlapping failure of TACLANE 12 will then disable GRE Tunnel 22 so that no path remains between the two red routers. In the four tunnel configuration, the failure of TACLANE 21 does not disable GRE Tunnel 12 or remove TACLANE 11 from service, so an overlapping failure of TACLANE 12 still leaves the path through GRE Tunnel 12 intact.

(U//FOUO) A four tunnel configuration may be more robust than is necessary in a network where the number of TACLANE-protected enclaves is very large. The probability that one TL will fail at each enclave at the same time decreases as the number of enclaves increases. If the redundancy design must assure that all n enclaves remain connected when one TL is unavailable at each of the n enclaves, then a four tunnel configuration is needed. If all n enclaves must remain connected when one TL is unavailable at each of n-1 (or fewer) enclaves, then a two tunnel configuration may be sufficient, but enclave-to-enclave latency could increase. If enclave-to-enclave latency must not increase when one TL fails at two or more enclaves, then a four tunnel configuration will be necessary. The number of GRE tunnels can be reduced by half in some networks where the redundancy and latency requirements and the number of enclaves allow failover to a partial mesh of enclave tunnels, where some enclave pairs can only be connected through the red router of a third enclave.

Appendix C (U) STATUS MESSAGES

C.1 (U) Status Messages

TACLANE Status Messages

(U//FOUO) The table below identifies TACLANE-Micro status messages and actions to be taken when the status message is received.

	Status Message	Action
	General Messages:	
	The device was unable to process the operation because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device encountered an internal error and was unable to process the request. Please try again.	Reload page.
	The browser was unable to perform a request to dynamically refresh the display. This is typically caused in Internet Explorer by having ActiveX disabled. Please manually refresh the page using the RELOAD button on the page or the REFRESH button on the tool bar to update the display. If that is unsuccessful, ensure that the device is currently powered on.	Check the LEDs on the TACLANE. The TACLANE may be restarting. Check browser settings to verify that ActiveX is enabled.
	The browser was unable to perform a request to dynamically refresh the display. Please manually refresh the page using the RELOAD button on the page or the REFRESH button on the tool bar to update the display. If that is unsuccessful, ensure that the device is currently powered on.	Check the LEDs on the TACLANE. The TACLANE may be restarting.
	System Level Messages:	
	The device must have a security level selected to access this functionality.	Define a security level through the Operation menu before attempting this function.
	The device was unable to access the battery configuration.	Resubmit the desired changes.

	The device was unable to update the battery configuration because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	CIK Management Messages:	
	Leaving this page before CIK creation is complete will prevent the display of the resulting creation status.	Resulting status message will be missed.
	Unable to access CIK data.	Resubmit the desired changes.
	The selected CIK could not be created.	Resubmit the desired changes.
	It is not possible to abort CIK creation at this time.	Complete CIK creation. CIK can be deleted after creation.
	A valid CIK has been inserted. Please insert a blank KSD.	A CIK that is valid for this TACLANE has been inserted.
	An error occurred during CIK creation.	An invalid CIK was entered. Remove CIK and insert a valid CIK.
	The selected CIK could not be deleted.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	Tamper Recovery Messages:	
	Recovery data download failed. DTR failed.	Verify the TFTP server is running and that the correct Recovery IP address and filename are entered.
	Error creating CIK. Cannot overwrite current Recovery CIK! Tamper Recovery failed.	Remove Recovery CIK. Perform Tamper Recovery. Do not use the Recovery CIK when prompted to insert a CIK.
	Error creating CIK. Tamper Recovery failed.	An invalid CIK was entered. Restart the TACLANE-Micro and perform Tamper Recovery with a valid CIK.

	Tamper Recovery failed.	Retry Tamper Recovery Process.
	Recovery CIK update failed.	The TACLANE-Micro was able to read but not write to the CIK
	Recovery CIK creation failed. Tamper Recovery failed.	An invalid Recovery CIK was inserted while performing Depot Tamper Recovery
	Recovery CIK creation failed. Tamper Recovery continuing.	Read of CIK is successful, write fails during the creation of the Recovery CIK during Field Tamper Recovery.
	Field Software Upgrade Messages:	
	The device was unable to configure the Download Servers because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The Download Server entry could not be deleted because a download is in process.	Wait for the download to complete before deleting the download server.
	The device was unable to update the selected Download Server entry.	Resubmit the desired changes.
	The device was unable to update the selected Download Server entry because a download is in process.	Wait for the download to complete before deleting the download server.
	The selected Download Server is not configured.	Select a download server that is configured before performing the operation.
	The device was unable to modify the Download Servers because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to configure the TFTP settings because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.

	The device was unable to initiate the Download because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to start the installation because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to discard the download because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to perform the selected action because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The FSU Command failed.	Resubmit the desired changes.
	IP Error Messages:	
	The system was unable to update the IPv4 Addresses because another manager was updating the system at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to process the operation because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The provided Router Options can not be set.	Resubmit the desired changes.
	The device was unable to change the MTU because another manager was updating the system at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.

	The device was unable to change the Ethernet Comm settings because another manager was updating the system at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	FFVS and PPK Messages:	
	Timeout occurred during FIREFLY Vector Set fill.	The DTD must be connected to the fill port and the fill must be initiated from the DTD within five minutes.
	Error occurred during FIREFLY Vector Set fill.	Check the Audit Log for the FFVS Fill Failed entry. Note that if the reason = Invalid Key Material, verify that a fill of a PrePlaced Key was not attempted.
	The device was unable to initiate the fill operation because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	Timeout occurred during PrePlaced Key fill.	The DTD must be connected to the fill port and the fill must be initiated from the DTD within five minutes.
	Error occurred during PrePlaced Key fill.	Check the Audit Log for the PPK Fill Failed entry. Note that if the reason = DS-100-1 Parity Error, check the fill cable and verify that a fill of an FFVS was not attempted.
	The device was unable to initiate the fill operation because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	Audit and Event Log Messages:	

	The device was unable to delete the Audit Log because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to update the configuration for the Audit Log Warning Threshold data because another manager was configuring the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	PPK Assignments Messages:	
	The PrePlaced Key Assignment could not be enabled, because a Security Association for this address may already exist.	Verify that a FIREFLY vector set does not already exist to the same remote INE or that the same PPK SA is not in the process of being disabled while trying to enable the same PPK assignment.
	The PrePlaced Key Assignment could not be added.	Verify that the assignment does not already exist or the CT address does not match an existing entry.
	The device was unable to configure SDD PrePlaced Key Assignment information because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to configure User PrePlaced Key Assignment information because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	Secure Dynamic Discovery configuration data was not saved.	Resubmit the desired changes.
	The device was unable to process Secure Dynamic Discovery configuration because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.

	SA Messages:	
	The device was unable to delete the Static Route because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	No Static Routes to display starting from the specified address.	Select different address range to view possible static routes.
	The device was unable to process the operation because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to delete all of the Static Routes.	Resubmit the desired changes.
	The device was unable to update the Security Association Configuration settings because another manager was modifying the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The Security Association Configuration settings were not updated.	Resubmit the desired changes.
	The device was unable to delete the Security Association because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to delete the selected host because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	Access Control setting is not updated.	Resubmit the desired changes.
	The device was unable to update the Access Control List because another manager was updating the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.

	The KMID cannot be deleted from the Access Control List.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The device was unable to add this KMID to the Access Control KMID list.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	TFS Messages:	
	The device was unable to update the TFS Bypass Configuration settings because another manager was modifying the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The provided TFS Bypass Options cannot be set.	Resubmit the desired changes.
	The device was unable to update the TFS PSEQN Configuration settings because another manager was modifying the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The provided TFS PSEQN Options cannot be set.	Resubmit the desired changes.
	The device was unable to update the TFS Fixed Packet Configuration settings because another manager was modifying the device at the same time.	Another manager has updated the device. Check the data for possible updates. Resubmit the desired changes.
	The provided TFS Fixed Packet Options cannot be set.	Resubmit the desired changes.