TACLANE

(U) OPERATOR'S MANUAL

For

TACLANE-E100

Release 3.0v2

15 March 2006

Revision 1.4

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

Not releasable to the Defense Technical Information Center per D.O.D. Instruction 3200.12.

Distribution limited to U.S. Government Agencies only. This document contains NSA information 15 March 2006. Request for this document must be referred to the Director, NSA

Copyright © 2005 General Dynamics C4 Systems, Inc. All rights reserved under the copyrights laws of the United States.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Operator's Manual Revision 1.4

(U) Document Revision History

Document Revision Number	Dated	Description of Revision
-	10-DEC-2004	Initial version of TL-E100 manual
1.0	18-FEB-2005	Incorporate minor edits from the Rel 3.0 testing.
1.1	15-MAR-2005	Incorporate interchange to conform to SRS20867
1.2	4-OCT-2005	Incorporate changes related to R3.0Ev2
1.3	21-DEC-2005	Clarified that backward compatibility was tested w/ R2.x
1.4	15-MAR-2006	Corrected battery changing info

(U) THIS PAGE INTENTIONALLY LEFT BLANK

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U) Table of Contents

Chapte	r 1 . (U) Introduction	1-1
1.1	(U) About the Manual	1-1
1.2	(U) Reference Documents	1-3
1.3	(U) Acronyms and Abbreviations	1-5
1.4	(U) Safety Information	1-9
1.5	(U) Hardware Versions	1-11
1.6	(U) Software Version	1-12
1.7	(U) Customer Support and Contacts	1-13
Chapte	r 2. (U) About the TACLANE	
$2.\bar{1}$	(U) Introduction	2-1
2.2	(U) Concepts	2-3
2.3	(U) Capabilities	2-6
2.4	(U) Connectivity	2-10
2.5	(U) New Features in Release 3.0	2-11
Chapte	r 3. (U) Installing and Operating the TACLANE	
3.1	(U) Unpacking	3-1
3.2	(U) Equipment Checklist	3-2
3.3	(U) Handling and Environmental Conditions	3-4
3.4	(U) Mounting	3-6
3.5	(U) Installing TACLANE Cables	3-7
3.6	(U) Configuring the IP Network	3-12
3.7	(U) Operating the TACLANE	3-14
3.8	(U) HMI Menu Tree	
~		
Chapte	r 4. (U) Filling and Managing Keys	
Chapte 4.1	r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys	4-1 4-1
Chapte 4.1 4.2	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable 	4-1 4-1 4-3
Chapte 4.1 4.2 4.3	 r 4. (U) Filling and Managing Keys	4-1 4-1 4-3 4-4
Chapter 4.1 4.2 4.3 4.4	 r 4. (U) Filling and Managing Keys	4-1 4-1 4-3 4-4 4-7
Chapter 4.1 4.2 4.3 4.4 4.5	 r 4. (U) Filling and Managing Keys	4-1 4-1 4-3 4-4 4-7 4-13
Chapter 4.1 4.2 4.3 4.4 4.5 4.6	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable (U) Filling the FIREFLY Vector Set (U) Filling a PPK (U) Displaying the FIREFLY Vector Set Information (U) Displaying PPK Information 	4-1 4-3 4-4 4-7 4-13 4-14
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable (U) Filling the FIREFLY Vector Set (U) Filling a PPK (U) Displaying the FIREFLY Vector Set Information (U) Displaying PPK Information (U) Deleting the FIREFLY Vector Set 	4-1 4-3 4-4 4-7 4-13 4-14 4-16
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8	 r 4. (U) Filling and Managing Keys	4-1 4-3 4-3 4-4 4-7 4-13 4-14 4-16 4-17
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9	 r 4. (U) Filling and Managing Keys	4-1 4-1 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable (U) Filling the FIREFLY Vector Set (U) Filling a PPK (U) Displaying the FIREFLY Vector Set Information (U) Displaying PPK Information (U) Deleting the FIREFLY Vector Set (U) Deleting a PPK (U) Deleting a Security Level (U) Exiting a Security Level 	4-1 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19 4-20
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter	 r 4. (U) Filling and Managing Keys	4-1 4-3 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19 4-20 5-1
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1	 r 4. (U) Filling and Managing Keys	4-1 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19 4-19 4-20 5-1
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable (U) Filling the FIREFLY Vector Set (U) Filling a PPK (U) Displaying the FIREFLY Vector Set Information (U) Displaying PPK Information (U) Deleting the FIREFLY Vector Set (U) Deleting a PPK (U) Deleting a Security Level (U) Exiting a Security Level (U) Exiting a Security Level (U) Configuring IP/Ethernet (U) Configuring the Ethernet Network Interface Media (U) Configuring the Ethernet Physical Parameters 	4-1 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19 4-20 4-20 5-1 5-3
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2 5.3	 r 4. (U) Filling and Managing Keys	4-1 4-1 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19 4-20 5-1 5-3 5-7
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2 5.3 5.4	 r 4. (U) Filling and Managing Keys	4-1 4-3 4-3 4-3 4-3 4-7 4-13 4-14 4-16 4-16 4-17 4-19 4-20 5-1 5-3 5-7 5-9
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2 5.3 5.4 5.5	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable. (U) Filling the FIREFLY Vector Set (U) Filling a PPK (U) Displaying the FIREFLY Vector Set Information (U) Displaying PPK Information (U) Deleting the FIREFLY Vector Set (U) Deleting a PPK (U) Deleting a Security Level (U) Exiting a Security Level (U) Configuring IP/Ethernet (U) Configuring the Ethernet Network Interface Media (U) Configuring the Ethernet Physical Parameters (U) Auto-Negotiate Setting (U) Displaying Ethernet Speed/Duplex Settingss (U) Entering/Modifying the TACLANE IP Addresses 	4-1 4-3 4-3 4-3 4-3 4-7 4-13 4-14 4-16 4-17 4-19 4-19 4-20 5-1 5-3 5-7 5-9 5-11
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2 5.3 5.4 5.5 5.6	 r 4. (U) Filling and Managing Keys	4-1 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19 4-19 4-20 5-1 5-3 5-7 5-9 5-11 5-13
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2 5.3 5.4 5.5 5.6 5.7	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable (U) Filling the FIREFLY Vector Set (U) Filling a PPK (U) Displaying the FIREFLY Vector Set Information (U) Displaying PPK Information (U) Deleting the FIREFLY Vector Set (U) Deleting a PPK (U) Deleting a Security Level (U) Selecting a Security Level (U) Exiting a Security Level (U) Configuring IP/Ethernet (U) Configuring the Ethernet Network Interface Media (U) Configuring the Ethernet Physical Parameters (U) Auto-Negotiate Setting (U) Displaying Ethernet Speed/Duplex Settings. (U) Entering/Modifying the TACLANE IP Addresses (U) Modifying the TACLANE MTU Size 	4-1 4-3 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19 4-19 4-20 5-1 5-3 5-7 5-9 5-13 5-15
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8	 r 4. (U) Filling and Managing Keys	4-1
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 5.9	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable	
Chapter 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 Chapter 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 5.9 Chapter	 r 4. (U) Filling and Managing Keys (U) Obtaining DTDs and Keys (U) Attaching a Fill Cable (U) Filling the FIREFLY Vector Set (U) Filling a PPK (U) Displaying the FIREFLY Vector Set Information (U) Displaying PPK Information (U) Deleting the FIREFLY Vector Set (U) Deleting a PPK (U) Deleting a Security Level (U) Exiting a Security Level (U) Configuring IP/Ethernet (U) Configuring the Ethernet Network Interface Media (U) Configuring the Ethernet Physical Parameters (U) Displaying Ethernet Speed/Duplex Settings (U) Entering/Modifying the TACLANE IP Addresses (U) Modifying the TACLANE MTU Size (U) Displaying IP Communications Information (U) Turning Ping Support On/Off r 6. (U) Configuring/Managing Secure IP Paths 	4-1 4-3 4-3 4-4 4-7 4-13 4-14 4-16 4-17 4-19 4-19 4-20 5-1 5-1 5-1 5-13 5-15 5-17 5-18 5-18

UNCLASSIFIED//FOUO

6.2	(U) Entering Secure Communications Mode	6-5
6.3	(U) Displaying IP Path Information	6-8
6.4	(U) Deleting FIREFLY-Secured IP Paths	6-11
6.5	(U) Deassigning a PPK from an IP Slot	6-13
6.6	(U) Configuring Remote TACLANE Static Routing	6-15
6.7	(U) Modifying Remote TACLANE Static Routes	6-20
6.8	(U) Deleting Remote TACLANE Static Routes	6-21
6.9	(U) Displaying Remote TACLANE Static Routes	6-23
6.10	(U) Configuring TACLANE EFF Mode	6-24
6.11	(U) Configuring Daily MTEK	6-26
6.12	(U) Displaying the SA Negotiation Information	6-27
Chapte	r 7. (U) Configuring IP Traffic Flow Security Parameters	
7.1	(U) Configuring Fixed Packet Length Parameters	7-1
7.2	(U) Configuring Payload Sequence Number (PSEQN) Checking	7-8
7.3	(U) Configuring DSCP Bypass	7-11
7.4	(U) Configuring Don't Fragment (DF) Bit Bypass	7-15
7.5	(U) Configuring PMTU Bypass	7-18
7.6	(U) Configuring IGMP Bypass	7-22
7.7	(U) Configuring the ICMP Notification Host	7-25
7.8	(U) Displaying IP Traffic Flow Security Information	7-27
Chapte	r 8. (U) Configuring Access Control and the Network Manager	
8.1	(U) Turning Discretionary Access Control On/Off	8-1
8.2	(U) Displaying Discretionary Access Control Mode	
8.3	(U) Creating an ACL Entry	
8.4	(U) Modifying an ACL Entry	8-5
8.5	(U) Deleting an ACL Entry	8-6
8.6	(U) Displaying the ACL	8-7
8.7	(U) Configuring the Network Manager	8-8
8.8	(U) Displaying Network Manager Information	8-16
8.9	(U) Deleting the Network Manager	
Chapte	r 9. (U) Maintaining TACLANE	
9.1	(U) Setting the Date and Time	9-1
9.2	(U) Displaying the Date and Time	
9.3	(U) Displaying CIK Information	9-4
9.4	(U) Copying a CIK	9-5
9.5	(U) Deleting a CIK	9-9
9.6	(U) Restarting the TACLANE	9-11
9.7	(U) Shutting Down the TACLANE	
9.8	(U) Displaying Version Information	9-14
9.9	(U) Displaying Battery Installed Date	9-15
9.10	(U) Performing a Field Software Upgrade	9-16
9.11	(U) Zeroizing the TACLANE	
9.12	(U) Configuring the System Name	
9.13	(U) Display System Information	
9.14	(U) Configuring Backward Compatibility Mode	
9.15	(U) Display Backward Compatibility	
9.16	(U) Configuring Delegate Privileges	
Chapte	r 10. (U) Troubleshooting TACLANE	10-1
10.1	(U) Alarm	

ii UNCLASSIFIED//FOUO

10.0		
10.2	(U) Tamper	
10.3	(U) Performing a Field Tamper Recovery	
10.4	(U) Checking for a Low Battery	10-6
10.5	(U) Replacing the Battery	
10.6	(U) Adjusting Display Contrast	
10.7	(U) Performing Diagnostics	
10.8	(U) Troubleshooting General Problems	
10.9	(U) Troubleshooting Filling and Managing Keys	
10.10	(U) Troubleshooting IP/Ethernet	
10.11	(U) Troubleshooting Secure IP Paths	
Append	ix A . (U) Factory Default Settings	A-1
Ā.1	(U) Factory Default Settings and Port Numbers	A-1
Append	ix B. (U) IP/Ethernet Configuration Tips	B-1
B.1	(U) Introduction	B-1
B.2	(II) Francisca I. Conserve ID Noterior de	
	(U) Example Secure IP Network	B-1
B.3	(U) Example Secure IP Network	B-1 B-3
B.3 B.4	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-8
B.3 B.4 B.5	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-8 B-11
B.3 B.4 B.5 B.6	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-8 B-11 B-14
B.3 B.4 B.5 B.6 B.7	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-8 B-11 B-14 B-19
B.3 B.4 B.5 B.6 B.7 B.8	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-8 B-11 B-14 B-14 B-19 B-24
B.3 B.4 B.5 B.6 B.7 B.8 Append	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-8 B-11 B-14 B-19 B-24 C-1
B.3 B.4 B.5 B.6 B.7 B.8 Append C.1	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-8 B-11 B-14 B-14 B-19 B-24 C-1 C-1
B.3 B.4 B.5 B.6 B.7 B.8 Append C.1 C.2	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-8 B-11 B-14 B-14 B-19 B-24 C-1 C-1 C-1
B.3 B.4 B.5 B.6 B.7 B.8 Append C.1 C.2 C.3	 (U) Example Secure IP Network (U) General IP/Ethernet Configuration Tips	B-1 B-3 B-3 B-11 B-14 B-14 B-19 B-24 C-1 C-1 C-1 C-2

(U) List of Figures

Figure 2.1-1 (U) TACLANE KG-175	2-1
Figure 2.4-1 (U) Network Environment	2-10
Figure 3.5-1 (U) TACLANE-E100 Rear Panel	3-7
Figure 3.6-1 (U) TACLANE-Secured IP/Ethernet Network	3-12
Figure 3.7-1 (U) TACLANE Front Panel	3-14
Figure 3.7-2 (U) TACLANE Screen Format	3-15
Figure B.2-1 (U) TACLANE-Secured IP/Ethernet Network	B-1
Figure B.4-1 (U) TACLANE Configuration	B-8
Figure B.4-2 (U) TACLANE Configuration w/IP Tunnels	B-10
Figure B.5-1 (U) TACLANE Encryption Gateway Connecting Two Networks	B-11
Figure B.5-2 (U) TACLANE Encryption Gateway Connecting Many Subnet Enclaves	B-12
Figure B.6-1 (U) TACLANE Multiple Gateway Configuration Example	B-16
Figure B.6-2 (U) TACLANE Single Gateway Nested Configuration Example	B-17
Figure B.7-1 (U) Multiple CT Default Gateways	B-19
Figure B.7-2 (U) False Subnet Mask Configuration	B-2 1
Figure B.7-3 (U) Added Router Configuration	B-22
Figure B.7-4 (U) Manual PPK Configuration	B-23
Figure B.8-1 (U) Single-Ended TACLANE Redundancy with Router Redundancy	B-25
Figure B.8-2 (U) Single-Ended TACLANE Redundancy without Router Redundancy	B-27
Figure B.8-3 (U) Using Four GRE Tunnels to Provide Double-Ended TACLANE Redundancy	B-29
Figure C.3-1 (U) TACLANE Front View	C-2
Figure C.3-2 (U) TACLANE Bottom View	C-3

Chapter 1. (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-E100 (KG-175) 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 fifth edition of the TACLANE-E100 Operator's Manual. In the past (TACLANE Releases 2.1 and earlier), the TACLANE Operator's Manual was common for both the TACLANE Classic and E100. However, because a significant portion of the information in the manual was not applicable to the E100 (e.g., ATM configuration details), this new version of the Operator's Manual is specific for the Release 3.0v2 TACLANE-E100. The previous TACLANE Operator's Manual has also been broken into three separate versions: 1. TACLANE-E100 Operator's Manual (this manual), which includes IP configuration information for the TACLANE-E100 Release 3.0v2, 2. TACLANE Classic Operator's Manual, which includes IP and ATM configuration information for the TACLANE Classic Release 3.0v2, and 3. TACLANE-MINI and TACLANE-GigE Operator's Manual, which includes IP configuration information for the Release 3.2 TACLANE-GigE and Mini.
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) About the Manual, continued

Chapter	Title	Page
1	Introduction	1-1
2	About the TACLANE	2-1
3	Installing and Operating the TACLANE	3-1
4	Filling and Managing Keys	4-1
5	Configuring IP/Ethernet	5-1
6	Configuring/Managing Secure IP Paths	6-1
7	Configuring IP Traffic Flow Security Parameters	7-1
8	Configuring Access Control and the Network Manager	8-1
9	Maintaining TACLANE	9-1
10	Troubleshooting TACLANE	10-1
Appendix A	Factory Default Settings	A-1
Appendix B	IP/Ethernet Configuration Tips	B-1
Appendix C	Mechanical Drawings for Installation	C-1

(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.

1.2 (U) Reference Documents

Related TACLANE Documents

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

Document #	Title	Rev	ADRL or CDRL #	Date	Classif. (U,C,S)
TL-025-05	TACLANE Interface Control Document	6.0	CDRL D003	01-MAR- 2004	U
TL-027-05	TACLANE Key Management Plan	5.0	CDRL N001	27-JUN- 2003	S
TL-080-02	TACLANE Security Features Users Guide	2.0	CDRL S001/ ADRL PM09	30-MAY- 2003	S
TL-121-03	TACLANE Operational Concept Description	3.0	CDRL W001	23-FEB- 2004	U
TL-023-04	TACLANE Reliability Prediction and Documentation of Supporting Data	4.0	CDRL T002	18-JUN- 2001	U
GIG-089-01	TACLANE Quick Start Manual	-	N/A	18-JAN- 2005	U

(U) Reference Documents, continued

Other Referenced Documents

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

Document #	Title	Rev	ADRL or CDRL #	Date	Classif. (U,C,S)
CNSSI No. 3029	Operational Systems Security Doctrine for TACLANE (KG-175)	-	N/A	27-MAR- 2003	U
-	Interoperability Specification for High Assurance Internet Protocol Encryptor (HAIPE) Devices	1.3.5	N/A	11-MAY- 2004	U
-	HAIPIS Traffic Flow Specification	1.3.5	N/A	02-JUN- 2004	S
GEM001	GEM 7.0 and GEM Lite 4.0 Operator's Manual	-	N/A	TBD	U
0N477430	DTD User's Manual	Е	N/A	7-MAR- 1996	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

Acronym/ Abbr.	Definition
AC	Alternating Current
ACL	Access Control List
AH	Authentication Header
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AWG	American Wire Gage
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
СТ	Ciphertext
D	Depth
DAC	Discretionary Access Control
dB	Decibel
dBm	Decibel (referenced to milliwatts)
DC	Direct Current
DF	Don't Fragment
DHCP	Dynamic Host Configuration Protocol
DoD	Department of Defense
DoDAAC	Department of Defense Activity Address Code
DRAM	Dynamic Random Access Memory
DS	Differentiated Services
DS3	Digital Signal Level 3 (44.736 Mbps.)
DSCP	Differentiated Services (DIFFSERV) Code Point

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

(U) Acronyms and Abbreviations, continued

Acronyms and Abbreviations (continued)

Acronym/ Abbr.	Definition
DTD	Data Transfer Device
ECN	Explicit Congestion Notification
EFF	Enhanced FIREFLY
EKMS	Electronic Key Management System
EMI	Electromagnetic Interference
ENET	Ethernet
ESP	Encapsulating Security Payload
F	Fahrenheit
FF	FIREFLY
FPL	Fixed Packet Length
FSU	Field Software Upgrade
ft.	Feet
FTR	Field Tamper Recovery
GBS	Global Broadcast Service
GBSI	GBS Interface
GEM	General Dynamics Encryptor Manager
GND	Ground
Н	Height
HAIPIS	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

(U) Acronyms and Abbreviations, continued

Acronyms and Abbreviations (continued)

Acronym/ Abbr.	Definition
IKE	Internet Key Exchange
in.	Inches
INE	Inline Network Encryptor
IP	Internet Protocol
IPv4	IP version 4
KG	Key Generator
km.	Kilometers
KMID	Key Material ID
KSD	Key Storage Device
LAN	Local Area Network
lbs.	Pounds
LCD	Liquid Crystal Display
LED	Light Emitting Diode
m.	Meters
MAC	Mandatory Access Control
MAC	Medium Access Control
MAX	Maximum
Mbps	Megabits per second
MIB	Management Information Base
mph	Miles per hour
MTBF	Mean Time Between Failures
MTU	Maximum Transmission Unit
μm.	Micrometers
NA	Numerical Aperture
NIC	Network Interface Card
nm.	Nanometers
NSA	National Security Agency
NSN	National Stock Number
OC3	Optical Carrier Level 3 (155.520 Mbps)
PIN	Personal Identification Number
PIN	Positive-Intrinsic-Negative

(U) Acronyms and Abbreviations, continued

Acronyms and Abbreviations (continued)

Acronym/ Abbr.	Definition
PMTU	Path Maximum Transmission Unit
PPK	Preplaced Key
PSEQN	Payload Sequence Number
РТ	Plaintext
RARP	Reverse ARP
RECIPe	Remote Encryptor Configuration Information Protocol
RFC	Request For Comment
SA	Security Association
SAMP	Security Association Management Protocol
SDD	Secure Dynamic Discovery
SDNS	Secure Data Network System
sec.	Seconds
SNMP	Simple Network Management Protocol
SP	Security Processor
SSO	Site Security Officer
STD	Standard
STP	Shielded Twisted Pair
SVN	Secure Virtual Network
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

UNCLASSIFIED//FOUO

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) The unit must be grounded. In the event of a short circuit, grounding reduces the risk of electrical shock by providing a low resistance path for the current. (U//FOUO) <u>TACLANE ground</u> : A ground wire is recommended for all installations. A ground wire is required to meet HEMP for indoor installations, and a ground strap is required to meet HEMP for outdoor installations. Verify that the ground wire/strap 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.
	<u>AC power cord</u> : The AC power cord ends in three-pole grounding plugs. Do <u>not</u> use three-pole to two-pole adapters with these plugs.
	<u>AC outlet</u> : Verify that the AC outlet used is properly installed and grounded. The outlet must comply with applicable National Electric Codes.
DC Power Safety	(U//FOUO) Make sure that the power rating of the power source matches the requirements for the TACLANE.
	<u>DC power cord</u> : The DC power cord ends in three flying lugs. Verify that these lugs, especially the ground, are connected properly at the DC power source.
	DC source: Verify that the DC source used is properly installed and grounded.
	Continued on next page

(U) Safety Information, continued

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 contains a lithium battery. Do not incinerate lithium batteries because of the risk of explosion.

1.5 (U) Hardware Versions

Different TACLANE-E100 Versions	(U//FOUO) There are several versions of the TACLANE-E100 being offered by General Dynamics. The following table identifies the different part numbers and descriptions of these TACLANE-E100 versions.
---------------------------------------	--

(U//FOUO) The TL-E100 AUS, TL-E100 CAN, and TL-E100 NZL all function in the same manner as the TL-E100, and they have the same rear panels as the TL-E100. In this manual, functions listed as applying to the "TL-E100" also apply to the respective AUS, CAN, and NZL models.

Part Number	TACLANE Version & Description
0N649470-5 (AC) 0N649470-6 (DC)	<i>TL-E100 (KG-175)</i> – supports IP/Ethernet (10/100+ Mbps) encryption; rear panel shows MT-RJ and RJ-45 connectors.
0N649470-13 (AC) 0N649470-14 (DC)	<i>TL-E100 AUS (KG-175)</i> – Australian version of the TACLANE-E100.
0N649470-15 (AC) 0N649470-16 (DC)	<i>TL-E100 CAN (KG-175)</i> – Canadian version of the TACLANE-E100.
0N649470-19 (AC) 0N649470-20 (DC)	<i>TL-E100 NZL (KG-175)</i> – New Zealand version of the TACLANE-E100.

Other TACLANE Versions (U//FOUO) The following table identifies the part numbers and descriptions of the other TACLANE versions.

Part Number	TACLANE Version & Description
0N684240-1	<i>TL-GigE (KG-175A)</i> – supports IP/Ethernet (10/100/1000 Mbps) encryption; rear panel shows RJ-45 and LC connectors.
0N649755-1	<i>TL-Mini (KG-175B)</i> – supports IP/Ethernet (10/100+ Mbps) encryption; rear panel shows RJ-45 and MT-RJ connectors.
0N649470-1 (AC) 0N649470-2 (DC)	<i>TL-Classic (KG-175)</i> – supports 10 Mbps 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)	<i>TL-GBSI (KG-175)</i> – supports ATM OC3 encryption (up to 45 Mbps rate); rear panel shows MT-RJ connectors.
0N649470-7 (AC) 0N649470-8 (DC)	TLAUS (KG-175) – Australian version of the TACLANE-Classic.
0N649470-9 (AC) 0N649470-10 (DC)	<i>TL CAN (KG-175)</i> – Canadian version of the TACLANE-Classic.
0N649470-17 (AC) 0N649470-18 (DC)	TL NZL (KG-175) – New Zealand version of the TACLANE-Classic.

1.6 (U) Software Version

Individual Software Components	(U//FOUO) The F software compone • Crypto • Crypto • Networ • Securit	Rel 3 TACLANE-E100 software is comprised of four individual ents: Card Kernel (CC KRL) Card Software (CC SW) rk Interface Card Software (NIC SW) ry Processor Software (SP SW)
Displaying Software Version	(U//FOUO) The o information. The hardware and soft (U//FOUO) Refer how to display the following screen:	operator can display the TACLANE software release version release number by itself uniquely identifies a combination of tware. r to the section on "Displaying Version Information" for details on e TACLANE version information. The output will display the
		DISPLAY VERSION INFO PLATFORM: E100 RELEASE: rx.xvx CC KRL: xx.xxx CC SW: xx.xxx SELECT ACTION:

1

(U//FOUO) The specific values depend on the particular TACLANE software installed. Please refer to the Release Notes file to ensure that the installed TACLANE software matches the latest software defined in the Release Notes file.

DONE | M_MENU

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 TACLANE Help Desk at: Phone: (877) 230-0236 E-mail: <u>infosecsupport@gdc4s.com</u>
TACLANE Sales Support	(U//FOUO) For TACLANE sales support inquiries, please contact the TACLANE Sales Support group at: Phone: (781) 455-2800 E-mail: <u>infosec@gdc4s.com</u>
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 1306 Concourse Drive, Suite 310 Linthicum, MD 21090
	Phone: (410) 487-0220 Fax: (410) 850-5005 E-mail: <u>infosectraining@gdc4s.com</u> Web: <u>www.gdc4s.com/</u>

(U) THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2. (U) About the TACLANE

2.1 (U) Introduction

What is the TACLANE?

(U//FOUO) TACLANE (KG-175) is a low-cost, key-agile, inline-network encryptor for deployment in DoD tactical and strategic networks. However, 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 KG-175

TACLANE Mission (U//FOUO) The TACLANE-E100 is an In-line Network Encryptors (INEs) developed by General Dynamics C4 Systems (GDC4S) to support secure transfers of IP datagram traffic for tactical and strategic network applications. The TACLANE-E100 provides encryption for IP datagram traffic to support a variety of IP network configurations. While the TACLANE Classic supports both IP and ATM encryption, the TACLANE-E100, TACLANE-MINI, and TACLANE-GigE are IP-only encryptors.

(U) Introduction, continued

TACLANE
Mission
(continued)(U//FOUO) The TACLANE-E100 provides high performance (10/100 Mbps) secure
communication over fast IP networks. The E100 hardware consists of two
replacement network interface cards (NICs) that include interfaces for 10 Mbps Half
and Full Duplex 10Base-T, 100 Mbps Half and Full Duplex 100Base-TX, and 100
Mbps Full Duplex 100Base-FX.

UNCLASSIFIED//FOUO

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.)

(U) Concepts, continued

Keying Concepts

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

Concept	Definition
СІК	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 are used to dynamically generate pairwise FIREFLY TEKs between communicating TACLANES. FIREFLY vector sets are generated by the EKMS CF. Each FIREFLY vector set has a unique Key Material ID (KMID) 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.
ТЕК	TEKs are used to encrypt and decrypt IP traffic. TEKs can be dynamically generated FIREFLY TEKs or manually filled PPKs (traditional TEKs).
РРК	 PPKs are manually filled traditional TEKs. PPKs are generated by the EKMS CF. DS-74 PPKs are uniquely identified by the following information: EKMS ID Cryptonet Edition Segment DS-100-1 PPKs are uniquely identified by the following information: Short Title Edition Segment When filled, each PPK is associated with an effective date.
DTD	DTDs 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	Keys are deleted by being zeroized. A selective zeroize deletes a particular key. A panic zeroize deletes all keys.

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

UNCLASSIFIED//FOUO

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.
Secure IP Path	An IP datagram tunnel secured by a TACLANE. There is at most one secure IP path between a given pair of TACLANEs at any time. All user IP datagram traffic passed between a pair of TACLANEs is protected using the same secure IP path.
Initiator	TACLANE at origin of secure IP path.
Responder	TACLANE at destination of secure IP path.
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, the Access Control List (ACL). 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.
	An additional MAC method is the Bad Guy List (BGL), which can be downloaded from the remote manager. The TACLANE cannot set up security associations with any FIREFLY vector set with its KMID on the BGL, with the exception that it is never restricted from communicating with the remote manager. The BGL cannot be displayed at the HMI and it cannot be disabled.
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.

UNCLASSIFIED//FOUO

2.3 (U) Capabilities

IP/Ethernet Encryption at 100 Mbps	(U//FOUO) The TACLANE-E100 supports IP datagram encryption over an Ethernet 10/100Base-TX or 100Base-FX physical interface:
	 100 Mbps throughput with a user traffic MTU size of 1424 octets (per RFC 791), half duplex 100+ Mbps aggregate throughput with a user traffic MTU size of 1424 octets
	(per RFC 791), full duplex
	• HAIPIS v1.3.5 compliant IP encryption
	• 253 secure IP paths supported for user traffic (One secure IP path protects all user traffic between a given pair of TACLANES)
	 Automated peer TACLANE discovery for secure IP paths using Secure Dynamic Discovery (SDD)
	• PPK or dynamically generated FIREFLY TEK for each secure IP path
	• Enhanced FIREFLY (EFF) support
	• Up to eleven changeover PPKs in each PPK chain
	• IP TFS controls: FPL, PSEQN, DSCP bypass, DF Bit bypass, IGMP bypass, and PMTU bypass
	• Auto-Negotiating 10Base-T vs. 100Base-T Ethernet interface
	Static multicast with PPK
	PT-side notification of CT-side Source Quench and Destination Unreachable ICMP messages
	• Domoto TACI ANE static routes
	• Remote TACLAINE static fouries

Operator's Manual Revision 1.4	UNCLASSIFIED//FOUO TL-275-06 15 March 2006
(U) Capabilit	ies, continued
Periods Processing at Multiple Levels	(U//FOUO) TACLANE can communicate at multiple security levels, one level at any given time. The operator selects the security level.
Easy to Use	(U//FOUO) The TACLANE-E100 provides a front panel HMI that provides a simple stand-alone menu interface with minimal keystrokes needed for on-the-spot reconfiguration in the field.
Local Key Management	(U//FOUO) The CIK protects one FIREFLY vector set and up to 48 PPKs, each with up to eleven changeover PPKs. All PPKs are filled using a DTD.
	(U//FOUO) An operator can create up to two user CIKs, for a total of three CIKs (two user CIKs and one SSO CIK). The different user CIKs allow shift operators access to the same key material. An operator can also delete user CIKs. User CIKs are functionally identical to the SSO CIK except that they do not have SSO privileges (e.g., Field Software Upgrade, IP TFS configuration capabilities). The TACLANE cannot go into secure comms with the SSO CIK inserted.
Access Control	(U//FOUO) MAC checks (must be the same for initiator and responder TACLANE) for FIREFLY TEK generation include:Partition code of FIREFLY vector set
	• Current security level (U//FOUO) An additional MAC method is the Bad Guy List (BGL), which can be downloaded from the remote manager. The TACLANE cannot set up security associations with any FIREFLY vector set with its KMID on the BGL, with the exception that it is never restricted from communicating with the remote manager.
	(U//FOUO) DAC checks (operator-selectable option) include an Access Control List (ACL) containing an operator-editable list of KMIDs (FIREFLY TEKs are only generated with remote FIREFLY vector sets having KMIDs on the ACL)
	(U//FOUO) Physical access control is provided by removing the CIK, which locks the TACLANE.

(U) Capabilities, continued			
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 (but never less than UNCLASSIFIED/CCI). When the CIK is removed, the TACLANE is UNCLASSIFIED/CCI and the CIK is UNCLASSIFIED/CCI and the CIK is UNCLASSIFIED/CCI.		
Field Software Upgrade and Field Tamper Recovery	 (U//FOUO) The TACLANE software supports Field Software Upgrade (FSU) and Field Tamper Recovery (FTR) capabilities. FSU allows a Site Security Officer (SSO) to upgrade the software in a TL from an UNCLASSIFIED encrypted image on a CD. FTR enables a SSO to recover a TL from a benign tamper using a classified SECRET FTR CIK. Both features help reduce downtime since units no longer need to be sent to the depot for software upgrades or tamper recoveries. (U//FOUO) The TACLANE must be at Release 2.0 or later in order to perform a Field Software Upgrade. (U//FOUO) Please see the sections on "Performing a Field Software Upgrade" and "Performing a Field Tamper Percovery" 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 HAIPIS 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 CIK is inserted. The IP TFS features include:		
	 Fixed Packet Length (FPL) for outgoing CT encrypted traffic Payload Sequence Number (PSEQN) checking for incoming CT encrypted traffic – <i>note that HAIPIS PSEQN is different from Rel 2.1E PSEQN</i> Differentiated Services Code Point (DSCP) bypass control Don't Fragment (DF) Bit bypass control IGMP bypass control PMTU bypass control 		
	(U//FOUO) Configuration of the ICMP Notification Host IP address is also restricted to the SSO.		
	(U//FOUO) Please see the chapter on "Configuring IP Traffic Flow Security Parameters" for more information.		

(U) Capabili	ties, continued
Secure Remote Management Using SNMP	(U//FOUO) TACLANEs can be managed by GEM using SNMPv1 using the portions of the standard MIBs listed below:
g	• RFC 1213
	• System Group • RFC 1573
	Interfaces Group
	• IP Group (IP address table only)
	(U//FOUO) GEM 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
	• Remote online/offline/restart control
	• Trap management (TACLANE sends audit data full (at 80% full and 100% full) and low battery SNMP traps)
	 Configuring a Bad Guy List (a list of 256 KMIDs with which the TACLANE cannot set up security associations)
	• Switchover to the Backup Manager (for IP TACLANEs)
	· Viewing acting a of ID TEC nonemators

- Changing KMID of configured network manager

(U//FOUO) GEM also provides network management of TACLANE-protected network elements using SNMPv1.

(U//FOUO) TACLANE can be managed from the Plaintext (PT) or Ciphertext (CT) side. CT-side management traffic is encrypted between the TACLANE fronting the GEM 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.

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

UNCLASSIFIED//FOUO

- Viewing settings of IP TFS parameters

2.4 (U) Connectivity

Network Environment

(U//FOUO) The diagram below illustrates TACLANEs deployed in an IP WAN.

UNCLASSIFIED//FOUO

IP Network GW GW TACLANE Data E-Net TPN,DDN Workstation LAN TACLANE E-Net Data LAN Workstation G٧ 0 TACLANE Data E-Net Workstation LAN

UNCLASSIFIED//FOUO

Figure 2.4-1 (U) Network Environment

2-10 UNCLASSIFIED//FOUO

2.5 (U) New Features in Release 3.0

New features in Release 3.0	(U//FOUO) This section briefly describes those new features that are in the Release 3.0 TACLANE-E100.		
HAIPIS v1.3.5 compliant	 (U//FOUO) TACLANE-E100 is now HAIPIS v1.3.5 compliant. The Rel 3.0 changes include support for: Enhanced FIREFLY (EFF) Secure Dynamic Discovery (SDD) protocol Daily MTEK key updates DS-100-1 PPKs PSEQN IGMP Bypass DF Bit Bypass PMTU Bypass Unique Station IDs 		
Up to 11 Changeover PPKs	(U//FOUO) The Rel 3.0 TACLANE supports up to 11 changeover PPKs for each PPK. Prior to Rel 3.0, there was only one changeover PPK for each PPK.		
SSO Privileges	 (U//FOUO) The SSO can enable a non-SSO TACLANE operator to have access to the TACLANE HMI's 'privileged' commands. Refer to Section 3.8 ("HMI Menu Tree") for the list of HMI commands, with the legend indicating the privilege mode notation of each command in the HMI tree. (U//FOUO) The TACLANE HMI commands can be broken into four sets of varied access control based on the operator type: 		
	 SSO-only commands – those to which only the SSO has access SSO-delegatable commands – those that a non-SSO operator can access only when the Delegate Privileges setting is ON (note: the SSO can also gain access to these commands) Non-privileged commands – those to which any operator (SSO and non-SSO) can gain access Non-SSO commands - those that the non-SSO can access, but the SSO cannot access (there is currently only one command in this category: Secure Comm). 		

(U) New Features in Release 3.0, continued

Backup Remote Manager	(U//FOUO) The Rel 3.0 TACLANE supports both a primary and a backup remote network manager.
Dual KMIDs per remote manager	(U//FOUO) The TACLANE now supports two KMIDs for each remote manager. This second KMID allows the managed TACLANE to automatically switch to the alternate KMID when the vector set in the TACLANE fronting the network manager is replaced.
Configurable system name	(U//FOUO) The TACLANE operator can configure a system name for the TACLANE unit. The system name allows a remote manager to more easily identify the managed TACLANEs.
Bad Guy List (BGL)	(U//FOUO) The TACLANE now supports a Bad Guy List (BGL), which is a list of KMIDs with which the TACLANE is not permitted to establish security associations (SAs).
Auto- Negotiation enhancements	 (U//FOUO) The TACLANE-E100's Ethernet interface Auto-Negotiation feature has been enhanced in Rel 3.0. Specifically, three enhancements were added: Auto-negotiation supports different port speeds (e.g., the CT port can be auto-negotiated to a different port speed than the PT port was auto-negotiated to). The TACLANE operator can configure which rates/duplex settings should be advertised as part of auto-negotiation. The TACLANE now performs auto-negotiation on any detected link state changes. Thus, there is no longer a need to restart the TACLANE unit to force an auto-negotiation.
Backward Compatibility support	(U//FOUO) While being HAIPIS v1.3.5 compliant, the Rel 3.0 TACLANE can also be configured to be backwards compatible with Rel 2.x TACLANE releases (Rel 2.x). This mode allows the Rel 3.0 TACLANE to support features such as: SAMP, DS-74 PPKs, and pre-HAIPIS ESP header.
View TACLANE Unique ID	(U//FOUO) The operator can now view the TACLANE unique ID at the HMI.
View TACLANE Static Routes while Online	(U//FOUO) The operator can now view the TACLANE static routes while the TACLANE is Online (in Secure Comms).

Chapter 3. (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.

(U) Equipment Checklist 3.2

TACLANE units.

(U//FOUO) The following table lists the standard TACLANE equipment.

System	
Components	

Item	Qty	Description
1	1	TACLANE-E100 Ethernet
		(AC power TACLANE model – part number 0N649470-5, or DC power TACLANE model – part number 0N649470-6)
2	2	KSD-1 CIK (SSO CIK) inserted in TL plus a blank spare and two CIK tags)
		Part number: 0N649683-1
3	1	3.6V AA lithium battery (inside battery compartment)
		NSN: 6135-01-301-8776
4	1	Power cable (AC power cable for AC power TACLANE models, DC power cable for DC power TACLANE models)
		AC power cable part number: 0N649533-1
		DC power cable part number: 0N649530-1
5	1	CD with TACLANE documentation (including Operator's Manual, Quick Start Manual, Release Notes, etc)

Suctor

Field Tamper

Recovery CIK

TL-275-06

15 March 2006

benign tamper (a maximum of ten times) without returning it to the depot. The FTR CIK is classified SECRET and must be shipped separately from the TACLANE. (U//FOUO) FTR CIKs are TACLANE unit specific. For customers with more than one TACLANE unit, please make sure to note the serial # of the TACLANE associated with each FTR CIK. Do not attempt to use FTR CIKs in alternate

(U//FOUO) A Field Tamper Recovery (FTR) CIK is included when ordering a

TACLANE. The FTR CIK can be used to recover its associated TACLANE from a
(U) Equipment Checklist, continued

TL-E100 Optional Apcillary Kit	(U//FOUO) The optional ancillary kit for the TACLANE-E100 (part number 0N649471-3) includes:		
	 Transit case: includes space for the TACLANE and its power cable, all items in the ancillary kit, and a TACLANE Operator's Manual, and has a hard plastic shell exterior with a foam-lined interior 2 spare blank CIKs 2 10 ft. lengths of straight through shielded twisted pair Ethernet cable w/RJ-45 connectors 		
	• 2 5 meter MT-RJ to SC duplex multimode fiber optic cables		
Optional Rack	(U//FOUO) The optional rack mount kit (part number 0N649704-1) includes:		
Mount Kit	19 in. EIA rack mounting bracketHardware for securing 2 TACLANEs to the bracket and the bracket to the rack		
	The rack mount bracket is 6.90 in. H x 19.00 in. W x 16.70 in. D and is designed for a 4U (7 in.) vertical space when used with the universal mounting rail hole pattern in a 19 in. rack. Two TLs can be mounted side-by-side with their handles removed. Alternately, a single TL can be mounted in the center with its front handles still attached. The bracket is painted to match the TACLANE.		
Additional Equipment	(U//FOUO) The following items not supplied with the TACLANE are required for filling key:		
Required	 DTD (AN/CYZ-10(V3) NSN: 5810-01-393-1973) Fill cable for DTD 		
Important CIK Note	(U//FOUO) Check that KSD-1 devices used as TACLANE CIKs were manufactured after 1995. KSD-1 devices manufactured before 1995 use slower memory technology and may not work correctly when used as TACLANE CIKs.		

3.3 (U) Handling and Environmental Conditions

Handling and Environmental Specifications

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

Note: For mounting instructions and maximum dimensions, see Appendix C.

Specification	Remarks
Size	4.5 in. H x 8.25 in. W x 16.5 in. D (excluding front panel protrusions and removable front handles)
Weight	14 lbs, 5 oz
Power	 AC power TACLANE: 100-240 VAC, 50/60 Hz auto-ranging DC power TACLANE: 18-36 VDC Dissipation: 40 W max.
Temperature	 Non-operating: -25 °F to +150 °F Operating (no warm-up): Ambient +40 °F to +120 °F Operating (30 min. warm-up): Ambient 0 °F to +120 °F
Humidity	10% to 95% non-condensing
Shock and Vibration	 Vibration operating: Operable in wheeled (XM1097 HHMMWV) and tracked (XM1068) vehicle, with an external isolation system required for tracked vehicles Vibration non-operating: Transportable, inside transit case, in wheeled (XM1097 HHMMWV) and tracked (XM1068) vehicle. Shock non-operating: Withstands 3 drops from 3 ft. on each face with TACLANE inside its transit case and one 30° rotational drop from each bottom edge without its transit case.
Sand and Dust	Withstands exposure to fine sand and dust @20 MPH for 20 min; MIL-STD-810E, Notice I (Method 510.3, Procedure I and II)
Rain	Withstands precipitation blown into shelters
Altitude	 Operating: Sea level to 15,000 ft. max. (w/temperature range) Non-operating: Sea level to 40,000 ft. max. (w/temperature range)
HEMP	MIL-STD-2169B (Proper grounding is required)
TEMPEST	NSTISSAM TEMPEST/1-92 Level 1 (Proper grounding and shielded twisted pair Ethernet cable (when using Ethernet) are required)
HIJACK	KAG-30A/TSEC
EMI	MIL-STD-461D for Army ground platforms (Proper grounding and shielded twisted pair Ethernet cable (when using Ethernet) are required)

(U) Handling and Environmental Conditions, continued

Important Battery Removal Note	(U//FOUO) Always remove and replace the battery with the TACLANE remaining powered on. Battery removal with the TACLANE powered off (or powering off the TACLANE after removing the battery) tampers the TACLANE.	
	(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.	
Failure Rate Summary (based on deployed units)	(U//FOUO) The Mean Time Between Failure (MTBF), based on 30,000+ deployed TACLANE units, is 100,000+ hours. This calculation was derived using the MIL-HDBK-272 approach on the deployed units.	
Failure Rate Summary Estimates (based on prediction models)	(U//FOUO) MTBF estimates have been calculated for the different TACLANE hardware configurations in varying operating environments. The results can be found in the TACLANE Reliability Prediction and Documentation of Supporting Data document. They are also summarized in the table below (all values are MTBF in hours).	
	(U//FOUO) Note that the Ground Fixed and Ground Mobile values are the predicted MTBF using MIL-HDBK-272, while the Ground Benign values are the predicted MTBF using the Bellcore standard.	

	Ground Fixed	Ground Mobile	Ground Benign
TL-E100 (AC)	9,910	3,526	25,400
TL-E100 (DC)	9,676	3,437	24,677

TL-275-06 15 March 2006 **UNCLASSIFIED//FOUO**

3.4 (U) Mounting

Mechanical Drawings for Installation	(U//FOUO) Please refer to Appendix C for mechanical drawings for installation.
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 (See "Handling and Environmental Conditions").
Cable Clearance	(U//FOUO) Make sure there is enough clearance to the rear of the TACLANE so as not to excessively bend and damage the cables. Appendix C shows the bend radii.
Desktop Placement	(U//FOUO) TACLANE has 4 rubber feet for placement on a desktop without damaging the desktop surface.
Rack Mount	(U//FOUO) Two TACLANEs can be rack mounted side-by-side in a standard EIA 19 in. rack. The TACLANE has 4 10/32 in. threaded holes on the bottom cover for mounting to a rack shelf. Spacers must be used to bypass the rubber feet (the rubber feet are not removable). The TACLANE front handles can be removed for rack mounting. An optional rack mount kit (part number 0N649704-1) is available. See Section 3.2, "Equipment Checklist," for more information.
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.
Vehicle Mount	(U//FOUO) Mounting in a tracked vehicle requires an external isolation system (isolation tray) to control vibration (this is not required for mounting in a wheeled vehicle). The TACLANE has 4 10/32 in. threaded holes on the bottom cover for mounting to an isolation tray. Spacers must be used to bypass the rubber feet (the rubber feet are not removable). The TACLANE front handles can also be removed for vehicle mounting.

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-E100 Rear Panel

Warning

(U//FOUO) Proper grounding is required for safety and to meet HEMP, TEMPEST, and EMI requirements:

- Proper grounding through the AC or DC power ground is required.
- A ground wire (AWG18, not longer than 6 ft.) is recommended for all installations. A ground wire (AWG18, not longer than 6 ft.) for indoor installations or a ground strap (U.S. Army SC-B-539494 or equivalent) for outdoor installations is required to meet HEMP.



AC Power Connector Pin Mapping (U//FOUO) Below is the pin mapping for the TACLANE AC power connector:

• Cable connector is MIL-SPEC part number MS27467T13F4S

• TACLANE connector is MIL-SPEC part number MS27505E13F4PN

Pin #	Name	Definition
А	Phase	
В	Neutral	
С	Ground	Chassis ground
D		Not used

(U) Installing TACLANE Cables, continued

Attaching the DC Power Cable	(U//FOU TACLA	O) Follow these steps to install the TACLANE DC power cable (DC power NE models):
	Step	Action
	1.	Make sure that the TACLANE is powered off.
	2.	Make sure that power at the connection to the DC source is off.
		Connect the DC power cable to the power connector on the TACLANE. (Rotate the cable connector against the connector on the TACLANE until the cable connector slides onto the connector on the TACLANE. Rotate the collar on the cable connector clockwise until a click is heard and the connector is locked on.)
		<u>Note</u> : The AC and DC power connectors are keyed differently to prevent an AC TACLANE from being connected to a DC supply, and vice versa.
	3.	Securely connect the 3 flying leads, ground, positive, and negative to the DC source.
	4.	Restore power at the connection to the DC source.

DC Power Connector Pin Mapping

(U//FOUO) Below is the pin mapping for the TACLANE DC power connector:

• Cable connector is MIL-SPEC part number MS27467T13F4SA

• TACLANE connector is MIL-SPEC part number MS27505E13F4PA

Pin #	Name	Definition
А	28 VDC	
В	28 VDC return	
С	Ground	Chassis ground
D		Not used

TL-275-06 15 March 2006	UNCLASSIFIED//FOUO Operator's Manual Revision 1.4				
(U) Installing	g TACL	ANE Cables, continue	ed		
Attaching Fiber Cables	(U//FOU multimo use of m	JO) Follow these steps to attac de fiber distance, based on the nultimode fiber that meets EIA	th the fiber cables. Note that e strength of the TACLANE attenuation limits, is 2 km.	t the maximum transmitter and the	
	Step				
	1.	Make sure that the TACLANE is powered off.			
	2.	Connect the fiber cable origination TACLANE.	inating at the user PT port to	o the PT port on the	
	3.	Connect the fiber cable origin on the TACLANE.	inating at the network CT p	ort to the CT port	
Fiber Interface Characteristics	(U//FOU FX fiber	JO) The following characterist	ics apply to the TACLANE	E-E100 100Base-	
	 Full vers Tran MT- 	compliance with the optical p sion of IEEE 802.3u sceivers can be used with 2 kn -RJ fiber connectors	erformance requirements of m. multimode fiber backbor	f 100Base-FX nes	
	(U//FOUO) The transmitter utilizes a 1300 nm. Surface Emitting InGaAsP LED. Below are the transmitter optical characteristics:				
	Cente	er wavelength:	1270-1380 nm. (1308 nr	n. typical)	
	Outpt (62.5)	ut optical power: /125 μm., NA = 0.275 fiber)	-14.0 dBm average (max -20.0 dBm average (min -15.7 dBm average (typi	kimum) himum) hcal)	
	Outpt (50/1	ut optical power: 25 μm., NA = 0.20 fiber)	-14.0 dBm average (max -23.5 dBm average (min -20.3 dBm average (typi	kimum) imum) ical)	
	Optic	al extinction ratio:	-27 dB (maximum) -33 dB (typical)		
	(U//FOU optical c	JO) The receiver utilizes an In characteristics:	GaAs PIN photodiode. Bel	ow are the receiver	
	Opera	ating wavelength:	1270-1380 nm.		
	Input minir	optical power num at window edge:	-31.0 dBm average (max -33.5 dBm average (typi	kimum) ical)	
	Input minir	optical power num at eye center:	-31.8 dBm average (max -34.5 dBm average (typi	kimum) ical)	
	Input	optical power maximum:	-14.0 dBm average (min -11.8 dBm average (typi	imum) ical)	

(U) Installing TACLANE Cables, continued

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.		
Ethernet Cable Installation for TEMPEST Compliance	(U//FOUO) TEMPEST compliance requires use of shielded twisted pair (STP) system 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 6 inches from the AC power cable. In addition, a ground cable shall be connected between the binding post on the rear of the chassis labeled "GND" and earth ground.		
Straight vs. Crossover Ethernet Cable	(U//FOUO) Each TACLANE Ethernet interface needs a straight or a crossover Ethernet cable depending upon what it is connected to. If the TACLANE Ethernet interface is connected directly to a host, then a crossover Ethernet cable is needed. If the TACLANE Ethernet interface is connected to a hub, then a straight Ethernet cable is needed since the hub typically performs the crossover function internally. (The transmit pin on one end of a crossover cable is "crossed over" to the receive pin on the other end.)		
Attaching a 10Base-T or 100Base-T Ethernet Cable	(U//FOUO) Follow these steps to attach a 10Base-T or 100Base-T Ethernet cable. The TACLANE RJ-45 jacks are covered by rubber boots. When not in use, make sure that the rubber boots completely cover the RJ-45 jacks to protect them from rain, sand, and dust. Note that the IEEE recommended cable distance limit for Category 5 UTP is 328 ft. (100 m.).		
	Step	Action	
	1.	Make sure that the TACLANE is powered off.	
	2.	Connect the 10Base-T Ethernet cable to the PT or CT "10 Base T" jack on the TACLANE, gently folding back the rubber boot to insert the cable RJ-45 plug.	

3.6 (U) Configuring the IP Network

Typical Secure
IP Network(U//FOUO) The diagram below shows a typical IP network secured with
TACLANEs. (See Appendix B, "IP/Ethernet Configuration Tips" for additional
configurations.)



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

(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.

(U) Configuring the IP Network, continued

Static IP Routes	(U//FOUO) Configure IP routers that are separated by a TACLANE with static IP routes. On CT routers, define static IP routes to PT networks across the TACLANE On PT routers, define static IP routes to CT networks (and other destination PT networks) across the TACLANE. This is needed since TACLANE does not bypass IP routing protocols.		
	(U//FOUO) <u>Note</u> : Remote TACLANE static routing eliminates the need for static routes to PT networks on CT routers, and vice versa.		
Firewalls must pass IKE, ESP, SDD, and optionally SAMP	(U//FOUO) Any firewalls in the path between communicating TACLANEs must be configured to pass IKE, ESP, SDD, and SAMP (if backward compatibility is enabled). See Appendix A of this document for the port numbers for these protocols.		
Static Multicast Routes	(U//FOUO) For multicast IP support, configure CT and PT network elements with static multicast routes and/or statically configure each of them as a member of the multicast group.		

3.7 (U) Operating the TACLANE



Component	Description
ON/OFF Switch	Power switch and circuit breaker for the TACLANE. If the circuit
	breaker trips, the power switch moves to the OFF position.
Status LEDs	• POWER: Indicates unit is on and receiving power
	• RUN: Indicates unit is operational, and flashes once per second
	when unit is in secure communications mode (ready to process
	traffic)
	• ALARM: Indicates unit is alarmed, and is illuminated briefly
	during diagnostics
	• BATTERY LOW: Indicates battery voltage is low
Display	Backlit 9 line by 26 character LCD display
Kevpad	• 4 arrow keys: Navigation through menu items
) [• 3 unlabeled function keys: Allow menu-specific functions to be
	invoked. The last line of the display identifies the functions.
CIK Port	Keyceptacle for KSD-1 CIK

(U) Operating the TACLANE, continued

TACLANE HMI (continued)

Component	Description
Key FILL Port	CSESD-11 fill connector
ZEROIZE Buttons	Invokes zeroize function when both ZEROIZE buttons are depressed simultaneously for 5 seconds, whether TACLANE is ON or OFF.
LCD Display Contrast	(Inside battery compartment) Contrast adjustment for LCD display to accommodate various lighting conditions. Adjusted using small flat-head screwdriver.

Screen Format (U//FOUO) Below is a description of the TACLANE screen format.

UNCLASSIFIED//FOUO

	S	CREEN	TIT	LE	
	T 7 7 T		חחמ	TON	
	VAR	LABLE	REG	TON	
	INS	TRUCT	LON	LINE	
FUNC	#1	FINC	#2	FINC	#3
LOINC	π⊥	LONC	π 4	LONC	πJ

UNCLASSIFIED//FOUO

Figure 3.7-2 (U) TACLANE Screen Format

Screen Area	Description		
Screen Title	Identifies the current position in the menu tree (current screen)		
Variable Region	Contents depend on the type of screen displayed. This area consists of either:		
	Menu choices		
	• Item choices within a particular menu		
	• Fields for display and/or edit		
	• Status and error messages		
	If the amount of information to display is large, this region can be scrolled using the up and down arrow keys. If the arrow key is held down, TACLANE will automatically scroll through the field.		
Instruction Line	Identifies action to take for the current screen. Actions include		
	using the arrow and/or function keys to select item choices and/or		
	functions.		

Screen Format (continued)

	Screen Area	Description	
	Function Keys	Actions performed by each of the three function keys depend on the type of screen displayed. A function key is active when a function name appears in one or more of the spaces identified as "FUNC #1," "FUNC #2," or "FUNC #3."	
Important CIK Notes	(U//FOUO) Use care in turning a CIK (KSD-1) when inserting and removing, especially the first few times a CIK is inserted and removed. Tabs on the CIK may break if the CIK is forced.		
	(U//FOUO) If a C	IK is inserted, do not remove the CIK during TACLANE startup.	
	(U//FOUO) Check after 1995. KSD- technology and ma	that KSD-1 devices used as TACLANE CIKs were manufactured 1 devices manufactured before 1995 use slower memory ay not work correctly when used as TACLANE CIKs.	
	(U//FOUO) A spat Dynamics recomm CIK copy. The SS inserted in the TA kept in a safe place for normal TACL	re blank KSD-1 CIK is included with the TACLANE. General nends that the operator use this spare KSD-1 CIK to create a user SO CIK (sometimes referred to as the Master CIK or CIK #1) is CLANE when it arrives from the factory and should be tagged and e. The user CIK copy should then be used instead of the SSO CIK ANE operation.	
Automatic Scrolling	(U//FOUO) Certai visible screen area to scroll to view th key is held.	In TACLANE HMI screens display fields that are larger than the I. TACLANE allows the operator to use the left and right arrows nese entire fields. Scrolling continues automatically when an arrow	
	(U//FOUO) The o numeric fields (e.g TACLANE autom	perator can also use automatic scrolling when entering alpha- g., IP address). When the +DIGIT or –DIGIT function key is held, natically continues to increment or decrement alphanumeric fields.	
Important Data Entry Note	(U//FOUO) Durin entry is interrupted	g data entry, entries (e.g., IP addresses, KMID) are lost if data d by a pop-up TACLANE status message.	
No Dynamic Screen Update	(U//FOUO) TACL displayed as of the change dynamical	LANE HMI screens are not updated dynamically. Information is e time a function is selected – e.g., the date/time screen does not ly.	

UNCLASSIFIED//FOUO (U) Operating the TACLANE, continued

1.	Turn on the TACLANE. <u>Result</u> : The following screens are displayed:
	Result: The following screens are displayed:
	Testing the SP DRAM
	- Checking TL Application-
2.	The TACLANE-E100 will next display the following screens:
	Running Diagnostics

Starting Up the TACLANE (U//FOUO) Follow these steps to startup the TACLANE:

CT NIC Downloading
PT NIC Downloading
Initialization continues the same way for all TACLANE models.
<u>Result</u> : The following screen is displayed:
Initializing
Note: If a different screen is displayed, see "Other Startup Screens."

Starting Up the TACLANE (continued)

Starting Up the TACLANE (continued)

Step	Action			
5.	If a CIK (KSD-1) is not already inserted, the operator is prompted to insert a CIK.			
	Result: The following screen is displayed:			
	Insert and Turn CIK Note: If a different screen is displayed, see "Other Startup Screens."			
	<u>Note</u> : If a CIK is inserted, do not remove the CIK during startup (or restart).			
6.	When a valid CIK (KSD-1) is inserted, the boot sequence continues.			
	<u>Result</u> : The following screen is displayed:			
	Warm Start in Progress Standby			

Starting Up the TACLANE (continued)

Step	Action		
7.	The OFFLINE MAIN MENU is displayed after successful startup:		
	OFFLINE MAIN MENU		
	>OPERATION CONFIG DISPLAY KEY MGMT MAINT		
	SELECT ITEM:		
	SELECT		
	Note: It is recommended to insert/turn the CIK before turning on the TACLANE.		
	<u>Note</u> : If a CIK is inserted, do not remove the CIK during startup (or restart).		
	<u>Note</u> : Do not power down the TACLANE during the power-up sequence, or the inserted CIK may be made invalid.		
	Note: If a different screen is displayed, see "Other Startup Screens."		
	<u>Note</u> : Specific version information is displayed in the space denoted by " x "s.		
	Note: Specific version information is displayed in the space denoted by "x"s.		

Other Startup Screens	(U//FOUO) The table below describes other startup screens that may appear.		
	Screen	Description	
	Auto-recovery in progress	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 processing user traffic.	
	TACLANE zeroized	Alerts the operator that a panic zeroize previously occurred. After the operator presses any key to continue, the message does not appear again until the next panic zeroize occurs.	
	Tamper detected	See the chapter on "Maintaining TACLANE."	
	or		
	Depot tamper recovery in progress		
	Alarm	See the chapter on "Maintaining TACLANE."	
Shutting Down the TACLANE	(U//FOUO) For d on "Maintaining 7	irections on shutting TACLANE down, please refer to the chapter FACLANE."	
Autorecovery	(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 processing user traffic:		
	• Secure IP path intervention.	hs re-establish themselves automatically without operator	
Clock Drift	(U//FOUO) Nomi date and time sho	inal TACLANE clock drift is maximum 2 min./month. TACLANE uld be checked for accuracy at least once every 6 months and	

TL-275-06

15 March 2006

Operator's Manual

Revision 1.4

3.8 (U) HMI Menu Tree

Menu Tree for TL-E100 (U//FOUO) Shown below is the TACLANE Human Machine Interface (HMI) menu tree for the Release 3.0 TL-E100. The Main Menu choices appear in bold across the top. Menu items available only in a specific mode (or modes) are noted by superscript letters (refer to the Legend).

OPERATION	CONFIG	CONFIG	KEY MGMT	MAINT
RESTART ^R	NETWORK	SECURITY	FILL [#]	SEC ADMIN
ZEROIZE ^R	• IP COMM ^{N L}	• ACCESS MODE ^{NL*}	• OPERATE ^N	• DEL PRIV ^{N^*}
SHUTDOWN [#]	• IP ADDRESSES ^R	• ACL^{NL*}	• PPK^{LS}	• B/W COMP ^{N *}
SECURE COMM L^	• MTU	• CREATE	DELETE [#]	SYSTEM NAME
EXIT LVL ^{L # R}	SUBNET MASK	MODIFY	• OPERATE ^N	BATTERY
SELECT LVL ^{N#}	IP OPTIONS	DELETE	• PPK ^L	DATE/TIME # R
OFFLINE ^S	• E-NET COMM ^{LNR}	• CIK COPY ^{N#}		SW UPGRADE N*R
CALL INFO ^{LS}	MEDIUM	• CIK DELETE ^{N#}		
• SUMMARY	PHYSICAL	• NET. MGR ^{LR*}	DISPLAY	
• IP PATHS	AUTO NEG	CONFIGURE	ACCESS MODE	
DETAILED		PRIMARY	ACL	
• IP PATHS		BACKUP	BACK COMPAT	
		• DELETE	BATTERY	LEGEND
		PRIMARY	CIK INFO	Traffic Modes:
		BACKUP	DATE/TIME	^N No Security Level
		• BOTH	E-NET COMM	^L In Security Level
		 PPK ASSIGN[#] 	FF VS INFO	^s Secure Comms
		IP SLOT ^L	IP COMM	
		• STATIC RTE ^L	IP TFS	Privilege Modes:
		CREATE	NET MGR ^{LS}	[#] SSO Delegate
		MODIFY	PPK INFO ^{LS}	* SSO Only
		DELETE	SA NEGOTIATE	^ Non-SSO Only
		DELETE ALL	STATIC RTE ^{LS}	
		• IP TFS ^{* R N}	SYSTEM INFO	Restart:
		 FIXED PKT 	VERSION	^R Restart Required
		 MODE 		
		 LENGTH 		
		PSEQN CHECK		
		BYPASS		
		• PMTU		
		• IGMP		
		DSCP		
		DF BIT		
		ICMP HOST		
		• SA NEGOTIATE ^{*N}		
		• EFF		
		DAILY MTEK		

Chapter 4. (U) Filling and Managing Keys

4.1 (U) Obtaining DTDs and Keys

סדס	(U/FOUO) The Data Transfer Device (DTD) (AN/CVZ 10(V3)) is the only fill			
	device used at this time to fill TACLANEs with FIREFLY vector sets and PPKs.			
	Note: Only the AN/CYZ-10(V3) should be ordered or used.			
Obtaining DTDs	(U//FOUO) Obtaining DTDs through military supply:			
Military Supply	Only available to DoD.National Stock Number (NSN) 5810-01-393-1973			
	<u>Note</u> : US Army personnel must order the AN/CYZ-10(V3) through the Army Item Manager only. Call DSN 879-8176 or commercial (520) 538-8176 for additional information.			
Obtaining DTDs	(U//FOUO) Obtaining DTDs through CUP:			
COMSEC Utility Program (CUP)	 Available to DoD, civil agencies, and foreign allies. POC: Rose Bechtold or Susan Carter, NSA POC Phone Number: (410) 854-6154 			
Obtaining DTDs From	(U//FOUO) Obtaining DTD from Sypris Electronics LLC (formerly GroupTech), Tampa, FL:			
Manufacturer	Available to all, including contractors.POC: Melissa Pruss			
	• POC Phone Number: (813) 972-6234			
Obtaining FIREFLY Vector Sets	 (U//FOUO) Obtaining FIREFLY vector sets: Coordinate with Controlling Authority for closed partitions (if needed). Coordinate with COMSEC Account(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 Basic or Enhanced 			

(U) Obtaining DTDs and Keys, continued

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:
Whether order is for TACLANE/FASTLANE-type or HAIPIS-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//FOU FIREFL informat	O) A DTD, connected using a fill cable, is used to fill the TACLANE with a Y vector set and/or PPKs. See the DTD User's Manual for more ion on DTD operation.
Note	(U//FOU applies v connecto	IO) The fill cable is only needed when filling key. The same procedure whether attaching the fill cable to the TACLANE or the DTD – the cable ors at each end are the same.
Procedure	(U//FOU	O) 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.
		<u>Note</u> : 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.	Release the fill cable connector.
		<u>Result</u> : The fill cable is locked onto the fill port.
Procedure	(U//FOU	O) Follow these steps to remove the fill cable:
	Step	Action
	1.	Apply firm pressure to the cable connector, then slightly rotate the cable

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

4.3 (U) Filling the FIREFLY Vector Set

Introduction	(U//FOU FIREFL be dynan	JO) The operator can fill TACLANE, using a DTD, with one operational Y vector set. The FIREFLY vector set allows pairwise FIREFLY TEKs to mically set up between an initiator and responder TACLANE.
Enhanced FIREFLY and Basic FIREFLY	(U//FOU the Basic	JO) The TACLANE supports both the Enhanced FIREFLY (EFF) as well as c FIREFLY.
Notes	(U//FOU	JO) The following notes apply to filling the FIREFLY vector set:
Procedure	 TACL Level" Only th Privile The op FIREF If the H Mode' (U//FOU 	ANE must be offline with no security level selected (See "Exiting a Security ') in order to fill the FIREFLY vector set. he SSO or a privileged user (see Section 9.16 "Configuring Delegate eges") can access this command perator must delete any existing FIREFLY vector set before filling a new FLY vector set (See "Deleting the FIREFLY Vector Set"). EFF-only switch is set to EFF-only (See "Configuring TACLANE EFF "), TACLANE will not allow fill of a Basic vector set.
	Step	Action
	1.	From the OFFLINE MAIN MENU, select KEY MGMT.
	2.	From the KEY MANAGEMENT menu, select FILL.
		Result: The KEY FILL menu is displayed:
		KEY FILL
		>OPERATE
		SELECT ITEM:

Continued on next page

SELECT |

DONE | M_MENU

(U) Filling the FIREFLY Vector Set, continued

Procedure (continued)

Step	Action		
3.	From the KEY FILL menu, select OPERATE.		
	Result: The following screen is displayed:		
	FILL FIREFLY VS		
	Connect fill device to fill port		
	SELECT ACTION:		
	CANCEL READY		
4.	Using a fill cable, connect a DTD to the TACLANE fill port.		
5.	Configure the DTD to transmit the operational FIREFLY vector set.		
	<u>Note</u> : The DTD must be configured to "fill" the FIREFLY vector set rather than "issue" it.		
6.	Select READY on the TACLANE.		
	Result: The following screen is displayed:		
	FILL FIREFLY VS		
	Initiate fill device operation or abort		
	SELECT ACTION:		
	ABORT		
	Note: ABORT cancels a fill operation in progress and returns to the KEY FILL menu.		

(U) Filling the FIREFLY Vector Set, continued

Procedure (continued)

Step	Action
7.	Transmit the operational FIREFLY vector set from the DTD.
	<u>Result</u> : The following screen appears if the fill operation was successful:
	FIREFLY VS FILL
	< <expired ind="">></expired>
	KMID: 00000001204825
	CLASS: U,C,S,T
	CAPABILITY: FF/EFF
	<down for="" more=""></down>
	TYPE: >OPERATIONAL
	USER ID: DOD/SMITH/PAT/>
	UNIV ID: 1234
	UNIV ED: 01
	NEXT ED:
	CURR EXPIRE: 2005/07/01
	NEXT EXPIRE: 2005/08/01
	TEST KEY: N
	SELECT ACTION:
	DONE
	When the USER ID is selected, the operator can view the entire USER ID
	by scrolling with the right and left arrow keys.
	Note: Specific values depend on the particular FIREFLY vector set.
8.	Select DONE to return to the KEY FILL menu.
9.	Disconnect the fill cable from the TACLANE fill port.

4.4 (U) Filling a PPK

Introduction	(U//FOUO) The operator can fill a TACLANE, using a DTD, with up to 48 active PPKs. PPKs are used to secure IP paths between an initiator and responder TACLANE.
Notes	(U//FOUO) The following notes apply to filling PPKs:
	 TACLANE must have a security level selected (See Section 4.9, "Selecting a Security Level") in order to fill a PPK. Only the SSO or a privileged user (see Section 9.16 "Configuring Delegate Privileges") can access this command A total of 48 PPK chains may be filled in a TACLANE. A PPK chain consists of the one active PPK and up to 11 changeover PPKs. Assuming each PPK has a 1-month duration, 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 – 48, and are available at each of the security levels. All 48 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 48 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 01 at the SECRET level. There are two types of PPKs: User PPKs and the Secure Dynamic Discovery (SDD) PPK. The User PPKs secure user traffic while the SDD PPK is used to encrypt the SDD messages. There is only one SDD PPK. When filling a PPK, the operator is prompted to enter the Effective Date of the PPK and the Type of PPK (User vs. SDD). 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 type is not prompted for in filling the changeover PPK since these parameters are derived from the slot's active PPK. For secure IP paths using PPKs, all communicating TACLANEs must have the same PPK filled at the same security level and with the same effective date. In Backward Compatibility mode (see "Configuring Backward Compatibility Mode"), for pre-HAIPIS SAs, the PPKs being used must also be in the same slot at all communicating TACLANEs.
PPK formats supported	(U//FOUO) The TACLANE-E100 supports DS-100-1 PPK formats. If the Backward Compatibility mode is ON, then the TACLANE will also support the DS-74 PPK format. DS-100-1 PPKs can only be used for HAIPIS SAs.

TL-275-06	
15 March 2006	

PPK Changeover	(U//FOUO) TACLANE PPK changeover (PPK changeover occurs on the effective date of a changeover PPK) 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 secure IP path, 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.
	(U//FOUO) These windows are the same for DS-74 PPK and DS-100-1 PPK.
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 secure IP path, 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. After 31 updates, a PPK is automatically deleted at 1:05 AM on the following day. The 31 PPK updates, however, are superseded by a changeover key, if one is assigned and the changeover occurs prior to the 31 updates. These windows are the same for DS-74 PPK and DS-100-1 PPK.

Operator's Manual
Revision 1.4

(U) Filling a PPK, continued

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

Step	Action
1.	From the MAIN MENU, select KEY MGMT.
2.	From the KEY MANAGEMENT menu, select FILL.
	Result: The KEY FILL menu is displayed:
	KEY FILL
	>PPK
	SELECT ITEM:
	SELECT DONE M_MENU
3.	From the KEY FILL menu, select PPK.
	Result: The FILL PREPLACED KEY menu is displayed:
	FILL PREPLACED KEY
	<unclassified>></unclassified>
	02/USR/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	<up down="" for="" more=""></up>
	11/ EMPLY
	SELECT ITEM:
	SELECT DONE M_MENU

Bicp	Action	
4.	Use the arrow keys to navigate up and down to a particular PPK slot and	
	then press SELECT.	
	Result: The specific PPK screen is displayed:	
	FILL PREPLACED KEY	
	< <unclassified>></unclassified>	
	EFFECTIVE: 2004/07/01	
	TYPE: USR	
	ENTER PPK INFORMATION:	
	+DIGIT -DIGIT DONE	
	Note: If this is a changeover PPK (i.e., PPK filled in an active PPK slot),	
	then only the EFFECTIVE prompt appears.	
5.	Use the arrow keys to navigate up and down to a particular entry. Use the +DIGIT and -DIGIT function keys to increment or decrement each digit	
	The EEECTIVE (affective date) defaults to the first day of the surrout	
	• The EFFECTIVE (effective date) defaults to the first day of the current month but this can be modified up to one month past the previous PPK	
	effective date.	
	• The type choices are USR or SDD.	
6.	Select DONE when finished; then select YES to confirm the PPK information.	
	Result: The following screen is displayed:	
	FILL PREPLACED KEY	
	Connect fill device	
	to	
	fill port	
	SELECT ACTION:	

Procedure (continued)

Operator's Manual

Revision 1.4

Step	Action
7.	Using a fill cable, connect a DTD to the TACLANE fill port.
8.	Configure the DTD to transmit the PPK.
	Note: The DTD must be configured to "fill" the PPK rather than "issue" it.
9.	Select READY on the TACLANE.
	Result: The following screen is displayed:
	FILL PREPLACED KEY
	Initiate fill device operation or abort
	SELECT ACTION:
	ABORT
	Note: ABORT cancels a fill operation in progress and returns to the KEY
	FILL menu.

Procedure (continued)

Step	Action				
10.	Transmit the PPK from the DTD.				
	Result: If the particular PPK was of the <u>DS-100-1 format</u> , the following				
	screen appears if the fill operation was successful:				
	FILL PREPLACED KEY				
	< <unclassified>></unclassified>				
	PPK ID: UI				
	TYPE: USP				
	<pre><down for="" more=""></down></pre>				
	TITLE: XXXXXXXXXXXX				
	EDITION: XXXXXX				
	SEGMENT: 001				
	EFFECTIVE: 2004/07/01				
	SEC. LEVEL: UNCLASSIFIED				
	FORMAT: DS-100-1				
	SELECT ACTION:				
	DONE				
	Note: Specific values depend on the particular PPK.				
	Result: If the particular PPK was of the DS-74 format, the following				
	screen appears if the fill operation was successful:				
	FILL PREPLACED KEY				
	< <unclassified>></unclassified>				
	PPK ID: 01				
	CHAIN: XX				
	TYPE: USR				
	EKMS ID: 812345				
	EDITION: XXXXXX				
	SEGMENT: 001				
	EFFECTIVE: 2004/07/01				
	SEC. LEVEL: UNCLASSIFIED				
	ALGORITHM: BATON				
	SELECT ACTION:				
	DONE				
	Note: Specific values depend on the particular PPK.				
11.	Select DONE to return to the KEY FILL menu.				
12.	Disconnect the fill cable from the TACLANE fill port.				

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 From the MAIN MENU, select DISPLAY. 1. 2. From the DISPLAY INFORMATION menu, select FF VS INFO. 3. From the DISPLAY FF VS INFO menu, select OPER (the only choice on this menu). Result: The following screen is displayed: ----FIREFLY VS INFO-----<<EXPIRATION IND>> KMID: 00000001204825 CLASS: U,C,S,T CAPABILITY: FF/EFF <down for more> TYPE: >OPERATIONAL USER ID: DOD/SMITH/PAT/> UNIV ID: 1234 UNIV ED: 01 NEXT ED: CURR EXPIRE: 2005/07/01 NEXT EXPIRE: 2006/07/01 TEST KEY: Ν SELECT ACTION: DONE When the USER ID is selected, the operator can view the entire USER ID by scrolling with the right and left arrow keys. Note: Specific values depend on the particular FIREFLY vector set. 4. Select DONE twice to return to the DISPLAY INFORMATION menu.

4.6 (U) Displaying PPK Information

Introduction	(U//FOU	O) The operator can display the information associated with a PPK.
Note	(U//FOU "Selectin	O) TACLANE must have a security level selected (See Section 4.9, ag a Security Level") in order to display PPK information.
Procedure	(U//FOU	O) Follow these steps to display PPK information:
	Step	Action
	1.	From the MAIN MENU, select DISPLAY.
	2.	From the DISPLAY INFORMATION menu, select PPK INFO.
		Result: The following screen is displayed:
		DISPLAY PPK INFO
		>01/USR/0000005123812345 02/USR/0000005456812345 03/USR/0000005789812345
		SELECI ACIION·
		INFO DONE M_MENU
		Note: Specific values depend on the particular PPK.
		<u>Note</u> : The operator can view the full PPK ID/EDITION/SEGMENT by scrolling with the right and left arrow keys.
	3.	Use the up and down arrow keys to navigate to a particular PPK.

(U) Displaying PPK Information, continued

Procedure (continued)

Step	Action				
4.	Select INFO.				
	Result: If the PPK is a DS-74 key, the following screen is displayed:				
	PPK ID: 01				
	CHAIN: XX				
	<pre>down for more></pre>				
	CRYPTONET: 0000005123				
	EKMS ID: 812345				
	EDITION: G				
	SEGMENT: 001				
	EFF DATE: 2004/07/01				
	SEC. LEVEL: UNCLASSIFIED				
	FORMAT: DS-74				
	UPDATE CNT: XXXXX				
	SELECT ACTION:				
	DONE				
	Note: Specific values depend on the particular PPK.				
	Note: Initial PPK update count is displayed as 0. The update count is				
	displayed as 1 at 2:56 AM on the effective date of the PPK, and so on.				
	Result: If the PPK is a DS-100-1 key, the following screen is displayed:				
	PPK ID: 01				
	CHAIN: XX				
	TYPE: USR				
	<down for="" more=""></down>				
	EDITION: XXXXXX				
	SEGMENT: 001				
	EFF DATE: 2004/07/01				
	SEC. LEVEL: UNCLASSIFIED				
	ALGORITHM: BATON				
	FORMAT: DS-100-1				
	OPDATE CNT: XXXXX				
	SELECT ACTION:				
	DONE				
	Note: Specific values depend on the particular PPK.				
	Note: Initial PPK update count is displayed as 0. The update count is				
	displayed as 1 at 2:56 AM on the effective date of the PPK, and so on.				
5.	Select DONE twice to return to the DISPLAY INFORMATION menu.				

4.7 (U) Deleting the FIREFLY Vector Set

Introduction	(U//FOUO) The operator can delete the operational FIREFLY vector set.				
Note	(U//FOU • TAC Secu • Only acce	O) The following notes apply to deleting the FIREFLY vector set: CLANE must be offline with no security level selected (see "Exiting a writy Level") in order to delete the FIREFLY vector set. The SSO or a privileged user (see "Configuring Delegate Privileges") can ss this command			
Procedure	(U//FOU	O) Follow these steps to delete the FIREFLY vector set:			
	Step	Action			
	1.	From the OFFLINE MAIN MENU, select KEY MGMT.			
	2.	From the KEY MGMT menu, select DELETE.			
	3.	From the KEY DELETE menu, select OPERATE			
		Result: The following screen is displayed:			
		DELETE FIREFLY VS < <expired ind="">> KMID: 00000001204825 CLASS: T CAPABILITY: >FF/EFF <down for="" more=""> TYPE: OPERATIONAL USER ID: DOD/SMITH/PAT/> UNIV ID: 1234 UNIV ED: 01 NEXT ED: CURR EXPIRE: 2005/07/01 NEXT EXPIRE: 2005/08/01 TEST KEY: N DELETE KEY? </down></expired>			
		by scrolling with the right and left arrow keys.			
	4	<u>Note</u> . Specific values depend on the particular FIKEFLT vector set.			
	4.	Select YES to delete the FIREFLY vector set (or select NO to cancel).			
	5.	Select DONE to return to the KEY DELETE menu.			
4.8 (U) Deleting a PPK

Introduction	(U//FOUO) The operator can delete a PPK.	
Note	(U//FOU	O) The following notes apply to deleting a PPK:
	• (FACLANE must be offline with a security level selected (See Section 4.9, 'Selecting a Security Level'') in order to delete a PPK Only the SSO or a privileged user (see "Configuring Delegate Privileges") can access this command
Procedure	(U//FOU	O) Follow these steps to delete a PPK:
	Step	Action
	1.	From the MAIN MENU, select KEY MGMT.
	2.	From the KEY MANAGEMENT menu, select DELETE.
	3.	From the KEY DELETE menu, select PPK.
		Result: The following screen is displayed:
		>01/USR/0000005123/812345 02/USR/0000005456/812345 03/USR/00000005789/812345 <up down="" for="" more=""> SELECT ACTION:</up>
		SELECT DONE M MENU
		Note: Specific values depend on the particular PPK
		<u>Note</u> : The operator can view the entire PPK ID/CRYPTONET/EKMS ID/EDITION/SEGMENT by scrolling with the right and left arrow keys.
	4.	Use the up and down arrow keys to navigate to a particular PPK.

(U) Deleting a PPK, continued

Step	Action		
5.	Select SELECT.		
	Result: The following screen is displayed:		
	PPK INFO		
	PPK ID: 01 CRYPTONET: 0000005123 EKMS ID: 812345 <down for="" more=""> EDITION: G SEGMENT: 001 EFF DATE: 2004/07/01 CHANGEOVER: N SEC. LEVEL: UNCLASSIFIED</down>		
	DELETE PPK?		
	YES NO		
	Note: Specific values depend on the particular PPK.		
6.	Select YES to delete the PPK (or select NO to cancel).		
7.	Select DONE to return to the KEY DELETE menu.		

4.9 (U) Selecting a Security Level

Introduction	(U//FOUO) The operator can select a security level for the TACLANE to operate. Certain menu choices, such as filling PPKs and 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: TACLANE must be offline with no security level selected (See "Exiting a Security Level") in order to select a security level. Only the SSO or a privileged user (see "Configuring Delegate Privileges") 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 security levels allowed by the FIREFLY vector set. PPKs may only be used at the security level at which they were filled. 	
Procedure	(U//FOU	O) Follow these steps to select a security level:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select OPERATION.
	2.	From the OPERATIONS menu, select SELECT LVL.
		Result: The following screen is displayed: ENTER SECURITY LEVEL >UNCLASSIFIED CONFIDENTIAL SECRET TOP SECRET SELECT ITEM: SELECT DONE M_MENU
	3.	Select the desired security level.
		Result: The OFFLINE MAIN MENU is displayed: OFFLINE MAIN MENU <unclassified>> >OPERATION CONFIG DISPLAY KEY MGMT MAINT SELECT SELECT</unclassified>

4.10 (U) Exiting a Security Level

Introduction (U//FOUO) The operator can exit the current security level, returning to "no security level." Certain menu choices, such as filling the FIREFLY vector set, are only available when the TACLANE is not in a security level. Note (U//FOUO) The following notes apply to exiting a security level: • The TACLANE must be offline with a security level selected (See Section 4.9, "Selecting a Security Level") in order to exit a security level. • Only the SSO or a privileged user (see "Configuring Delegate Privileges") can access this command. • The TACLANE will restart after this command is executed. • The Shutdown command (see "Shutting Down the TACLANE") will also exit the security level automatically. Procedure (U//FOUO) Follow these steps to exit a security level: Step Action 1. From the OFFLINE MAIN MENU, select OPERATION. 2. From the OPERATIONS menu, select EXIT LVL. Result: The following screen is displayed: ----EXIT SECURITY LEVEL---<<UNCLASSIFIED>> TACLANE will restart and all calls will be lost EXIT SECURITY LEVEL? _____ YES NO Note: This warning is displayed because there may be secure IP paths to a network manager even though the user has no secure IP paths (See the chapter on "Configuring Access Control and the Network Manager"). 3. Select YES to exit the current security level. Result: The TACLANE restarts and the OFFLINE MAIN MENU is displayed: ----OFFLINE MAIN MENU---->OPERATION CONFIG DISPLAY KEY MGMT MAINT SELECT ITEM: _____ SELECT

4-20 UNCLASSIFIED//FOUO

Chapter 5. (U) Configuring IP/Ethernet

5.1 (U) Configuring the Ethernet Network Interface Media

Introduction	(U//FOU multimoo CT and F independ	O) The TACLANE-E100 can each be configured to work with either de fiber (FX) or copper (TX) Ethernet network interface media on both the PT interfaces. The network medium for each interface can be set ently (e.g., one interface can use copper, and the other can use fiber).
Notes	(U//FOU media: • The ' • The ' • A ch the T	O) The following notes apply to configuring the Ethernet network interface TACLANE must be offline in order to configure Ethernet network interface ia. default medium for both the CT and PT interfaces is copper. ange in the Ethernet communications parameters does not take effect until TACLANE has been restarted.
Procedure	(U//FOU	O) Follow these steps to configure the Ethernet network interface media:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select NETWORK.
	3.	From the CONFIGURE NETWORK menu, select E-NET COMM.
		Result: The following screen is displayed:
		E-NET COMMUNICATIONS
		>MEDIUM PHYSICAL AUTO-NEG
		SELECT ITEM:
		SELECT SAVE CANCEL

(U) Configuring the Ethernet Network Interface Media, continued

Step	Action
4.	Select MEDIUM.
	Result: The following screen is displayed:
	E-NET BASEBAND MEDIUM
	>CT: FIBER PT: COPPER
	SELECT ACTION:
	CHANGE DONE
5.	Select the interface you wish to change (CT or PT), and after selecting CHANGE, the medium will change to either COPPER or FIBER.
6.	Once the changes are completed, select DONE.
	Result: The following screen is displayed:
	E-NET COMMUNICATIONS
	>MEDIUM PHYSICAL AUTO-NEG
	SELECT ITEM:
	SELECT SAVE CANCEL
7.	If there are no other Ethernet communications changes, select SAVE.
8.	Select YES to the CHANGE E-NET PARAMETERS? prompt. After the TACLANE is restarted, return to the OFFLINE MAIN MENU.

5.2 (U) Configuring the Ethernet Physical Parameters

Introduction	(U//FOUO) The TACLANE-E100's PT and CT physical interface parameters are configurable by the operator. Specifically, the Ethernet interface speed and duplex can be configured to accommodate the characteristics of the networks to which a TACLANE-E100 is connected.		
	(U//FOUO) The TACLANE supports both an auto-negotiation interface as well as several constant bandwidths (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.		
Supported E100 physical settings	 (U//FOUO) The E100 supports the following user-configurable Ethernet physical settings. Configuring the physical medium (copper vs. fiber) is described in Section 5.1 ("Configuring the Ethernet Network Interface Media"). (Note: H is half-duplex, F is full-duplex): <u>E100 with a copper interface</u>: 		
	 Auto-Negotiate 		
	• 100/F		
	• 100/H		
	• 10/F		
	• 10/H		
	E100 with a fiber interface:		
	• 100/F		
	(U//FOUO) The default setting for an E100 with a copper interface is: Auto-Negotiate.		
	(U//FOUO) The default, and only possible setting for an E100 with a fiber interface is $100/F$.		

(U) Configuring the Ethernet Physical Parameters, continued

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 (refer to Section 5.3). Then, the E100 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). 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 while the duplex defaults to Half. Parallel detection is only used for 10/100BASE-T equipment.
Notes	 (U//FOUO) The following additional notes apply to configuring the Ethernet physical parameters: The TACLANE must be offline to configure the Ethernet physical parameter. The PT and CT physical interface settings are independent. For example, it is possible to have an E100 configured with its CT interface be 100/Full and its PT interface be Auto-Negotiate. An E100 with a fiber interface will have its physical interface automatically set to 100/Full since the fiber interface can only operate at 100/Full. A manual interface speed setting should be used if the TACLANE interfaces with network equipment that doesn't support auto-negotiation. A change in the Ethernet communications parameters does not take effect until the TACLANE has been restarted.

Procedure

(U) Configuring the Ethernet Physical Parameters, continued

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

Step	Action		
1.	From the OFFLINE MAIN MENU, select CONFIG.		
2.	From the CONFIGURATION menu, select NETWORK.		
3.	From the CONFIGURE NETWORK menu, select E-NET COMM.		
	Result: The following screen is displayed:		
	E-NET COMMUNICATIONS		
	MEDIUM >PHYSICAL AUTO-NEG		
	SELECT ITEM:		
	SELECI SAVE CANCEL		
4.	Select PHYSICAL.		
	Result: The following screen is displayed:		
	E-NET PHYSICAL		
	CT:>100/F PT: AUTO-NEG		
	SELECT ACTION:		
	CHANGE DONE		

(U) Configuring the Ethernet Physical Parameters, continued

Step	Action
5.	Select the desired CT and PT physical parameters. The first number represents the speed in Mbps. An "H" following the slash denotes half duplex, and an "F" denotes full duplex. Choosing AUTO-NEG will cause the TACLANE to auto-negotiate the speed and duplex upon restart. After the desired changes have been made, select DONE.
	Result: The following screen is displayed:
	E-NET COMMUNICATIONS
	MEDIUM >PHYSICAL AUTO-NEG
	SELECT ITEM:
	SELECT SAVE CANCEL
6.	If there are no other Ethernet communications changes, select SAVE.
7.	Select YES to the CHANGE E-NET PARAMETERS? prompt. After the TACLANE is restarted, return to the OFFLINE MAIN MENU.

5.3 (U) Auto-Negotiate Setting

Introduction	(U//FOU speed/du where th	O) The TACLANE operator can specify which Ethernet bandwidths (i.e., plex combinations) should be advertised to an interfacing device, in the case e TACLANE interface (copper) is set for auto-negotiation (see Section 5.2).
Notes	(U//FOU • The • Auto set t nego • The • Whe set to • If au until • A ch the T	 O) The following notes apply for configuring the auto-negotiate setting: FACLANE must be offline to configure the auto-negotiate setting. negotiation only occurs if the physical interface setting (see Section 5.2) is b "AUTO-NEG". Only a copper interface (not fiber) can be set for auto- tiate. default is that all items are available (i.e., set as "Y") for auto-negotiation. n an interface is set to auto-negotiate, it will only advertise the bandwidths b "Y". to-negotiation fails, the TACLANE will continue to try auto-negotiation a response is received. ange in the Ethernet communications parameters does not take effect until "ACLANE has been restarted.
Procedure	(U//FOU advertise	O) Follow these steps to specify which Ethernet bandwidths should be d for auto-negotiation:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select NETWORK.
	3.	From the CONFIGURE NETWORK menu, select E-NET COMM.
		Result: The following screen is displayed:
		E-NET COMMUNICATIONS
		MEDIUM >PHYSICAL AUTO-NEG
		SELECT ITEM:
		SELECT SAVE CANCEL

(U) Auto-Negotiate Setting, continued

Step	Action
4.	Select AUTO-NEG.
	Result: The following screen is displayed:
	AUTO-NEG SETTING
	Copper 100/H: Y Copper 100/F: Y Copper 10/H: Y Copper 10/F: Y
	SELECT ACTION:
	CHANGE DONE
5.	Note: "Y" denotes Yes it is advertised, "N" denotes No it is not advertisedSelect the interfaces you wish to advertise by setting them to "Y" and then selecting DONE.
	Result: The following screen is displayed:
	E-NET COMMUNICATIONS
	MEDIUM >PHYSICAL AUTO-NEG
	SELECT ITEM:
	SELECT SAVE CANCEL
6.	If there are no other Ethernet communications changes, select SAVE.
7.	Select YES to the CHANGE E-NET PARAMETERS? prompt. After the TACLANE is restarted, return to the OFFLINE MAIN MENU.

5.4 (U) Displaying Ethernet Speed/Duplex Settings

Introduction	(U//FOUO) The operator may display Ethernet speed/duplex settings in both secure communications and offline modes.
Notes	 (U//FOUO) The following parameter values are displayed in the Ethernet Comm display: <i>CT & PT Speed</i> – displays the interface's current speed (in Mbps) and (F)ull-duplex vs. (H)alf-duplex setting. <i>CT & PT Medium</i> – Copper vs. Fiber <i>CT & PT Operator Speed</i> – indicates the operator-selected speed for the interface. If auto-negotiation was configured, then the CT/PT OPR SPEED is displayed as AUTO-NEG and the CT/PT SPEED displays the actual negotiated interface speed. <i>CT & PT Remote Capability</i> – displays the supported capabilities of the remote INE's Ethernet interface. An "N/R" value indicates "No Response" and this is expected if the interface is "Fiber" or if Autonegotiation is not used.
	 CT & PT Elocal Capability – displays the set of capabilities that the interface will negotiate if Auto-negotiate is turned on. CT & PT Ethernet – displays the Ethernet address of the interface.
	Continued on next page

(U) Displaying Ethernet Speed/Duplex Settings, continued

Procedure

(U//FOUO) Follow these steps to display Ethernet speed/duplex settings:

Step	Action
1.	From the MAIN MENU, select DISPLAY.
2.	From the DISPLAY INFORMATION menu, select E-NET COMMs.
	Result: The following screen is displayed:
	DISPLAY E-NET COMM
	CT SPEED: 100/F
	PT SPEED: 100/F
	CT MEDIUM: COPPER
	<pre><down for="" more=""></down></pre>
	PT MEDIUM: COPPER
	DT OPR SPEED: AUTO-NEG
	CT RMT CAP: 100/F/H
	PT RMT CAP: 100/F
	CT LOCAL CAP: 100/F
	PT LOCAL CAP: 100/F
	CT E-NET: 00:A0:21:00:
	PT E-NET: 00:A0:21:00:
	SELECT ACTION:
	DONE M_MENU
	Note 1: The last two bytes of each Ethernet address are not visible, but the
	arrow keys can be used to scroll left and right
	Note 2: When the operator selected speed/duplex (OPR SPEED) is set to a
	constant bandwidth (rather than AUTO-NEG), the speed/duplex values
	displayed for CT RMT CAPABLE and PT RMT CAPABLE may not be
	accurate, due to limitations of the Auto-Negotiation protocol.
3.	Select DONE to return to the DISPLAY INFORMATION menu.

5.5 (U) Entering/Modifying the TACLANE IP Addresses

Introduction	(U//FOU address. gateway	O) TACLANE requires two IP addresses: a CT IP address and a PT IP To route off-network IP traffic, TACLANE also supports one CT default and one PT default gateway.
Notes	 (U//FOU addresse: TAC addr The or in The (e.g.) Whe IP ad auto (*ba) Whe 	 O) The following notes apply to entering/modifying the TACLANE IP S: CLANE must be offline in order to enter or modify the TACLANE IP esses. TACLANE can be configured with its CT and PT IP addresses in the same different subnets. CT and PT IP addresses must be unique such that no host or remote device , another TACLANE) uses these IP addresses. n any of the IP addresses (CT IP address, PT IP address, CT default gateway iddress, PT default gateway IP address) are entered/modified, the TACLANE matically sets the CT and PT subnet masks to the default* value. sed on whether the IP address is of Class A, B, or C) n this command is completed, the TACLANE will restart
Procedure	(U//FOU	O) Follow these steps to enter or modify the TACLANE IP addresses:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select NETWORK.
	3.	From the CONFIGURE NETWORK menu, select IP COMM.
		Result: The IP COMMUNICATIONS menu is displayed:
		IP COMMUNICATIONS
		>IP ADDRESSES MTU SUBNET MASK IP OPTIONS
		SELECT ITEM:
		SELECT DONE M_MENU

(U) Entering/Modifying the TACLANE IP Addresses, continued

Step	Action
4.	From the IP COMMUNICATIONS menu, select IP ADDRESSES.
	Result: The following screen is displayed:
	IP ADDRESSES
	TL CT IP: 000.000.000.000 TL PT IP: 000.000.000 GWY CT IP: 000.000.000.000 GWY PT IP: 000.000.000.000 SELECT ACTION:
	+DIGIT -DIGIT DONE
5.	Use the arrow keys to navigate to a particular digit of an IP address. Use the +DIGIT and –DIGIT function keys to increment or decrement each digit. Leave leading zeros. For example, an IP address of 148.10.127.55 is entered as "148.010.127.055."
	Note: All IP addresses must be unique.
	<u>Note</u> : The CT and PT IP addresses may be in the same or in separate networks (or subnetworks).
	For more information on setting subnet masks, see Section 5.6, "Entering/Modifying the TACLANE IP Subnet Mask(s)."
6.	Select DONE when finished.
7.	Select YES to "Save Changes?" prompt. The TACLANE restarts and returns to the OFFLINE MAIN MENU.

5.6 (U) Entering/Modifying the TACLANE IP Subnet Mask(s)

Introduction	(U//FOUO) The TACLANE automatically generates the default CT and PT IP subnet masks based on the respective CT and PT IP addresses (Class A, B, or C). However, the operator can also manually modify the default IP subnet masks (e.g., in a case where network is further subnetted).
Restart after setting Subnet Masks	(U//FOUO) Restart the TACLANE after changing subnet masks when configuring a unit intended for static routing operation. Note that configuring static routes after setting subnet masks may cause the TACLANE to automatically restart. Also, setting subnet masks after configuring static routes (or downloading them from GEM) may cause a restart. When changes to the subnet masks do not cause the unit to automatically restart, the operator should manually restart the TACLANE (See Section 9.6, "Restarting the TACLANE").
Notes	 (U//FOUO) The following notes apply to entering/modifying a TACLANE subnet mask: TACLANE must be offline in order to modify a subnet mask. The PT and CT subnet masks are independent of each other (e.g., PT subnet mask could be 255.255.255.0 while the CT subnet mask could be 255.255.255.0.0). Enter TACLANE IP addresses <i>before</i> the subnet mask. When any of the IP addresses (CT IP address, PT IP address, CT default gateway IP address, PT default gateway IP address) are entered/modified, the TACLANE automatically sets the CT and PT subnet masks to the default* value. (*based on whether the IP address is of Class A, B, or C)

TL-275-06 15 March 2006

(U) Entering/Modifying the TACLANE IP Subnet Mask(s), continued

Procedure (U//FOUO) Follow these steps to modify the TACLANE subnet mask(s):

Step	Action
1.	From the OFFLINE MAIN MENU, select CONFIG.
2.	From the CONFIGURATION menu, select NETWORK.
3.	From the CONFIGURE NETWORK menu, select IP COMM.
4.	From the IP COMMUNICATIONS menu, select SUBNET MASK.
	Result: The following screen is displayed:
	IP SUBNET MASK
	CT MASK: 255.000.000.000 PT MASK: 255.255.000.000
	SELECT ACTION:
	+DIGIT -DIGIT DONE
	Note: The default masks for the TACLANE IP addresses are displayed.
5.	Use the arrow keys to navigate to a particular digit of the subnet mask. Use the +DIGIT and –DIGIT function keys to increment or decrement each digit.
	<u>Note</u> : The subnet mask must be consistent with the TACLANE IP addresses entered.
6.	Select DONE when finished.
7.	Select YES to "Save Changes?" prompt and return to the IP COMMUNICATIONS menu.

5.7 (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) When Fixed Packet Length (FPL) processing is enabled, the TACLANE MTU should be set to a value that is at least 60 bytes greater than the configured fixed packet length. This allows for the addition of the AH and ESP headers to each datagram without requiring fragmentation prior to transmission on the CT network. Note that if only pre-HAIPIS security associations (SAs) are used, the MTU can be set to a value that is at least 56 bytes greater than the configured packet length. (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 must be offline in order to modify the MTU size.TACLANE defaults the MTU size to 1500 bytes.

TL-275-06 15 March 2006 UNCLASSIFIED//FOUO

(U) Modifying the TACLANE MTU Size, continued

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

Step	Action
1.	From the OFFLINE MAIN MENU, select CONFIG.
2.	From the CONFIGURATION menu, select NETWORK.
3.	From the CONFIGURE NETWORK menu, select IP COMM.
4.	From the IP COMMUNICATIONS menu, select MTU.
	Result: The following screen is displayed:
	IP MTU
	SIZE (BYTES): 1500
	SELECT ACTION:
	+DIGIT -DIGIT DONE
5.	Use the arrow keys to navigate to a particular digit of the MTU size. Use the +DIGIT and –DIGIT function keys to increment or decrement each digit.
	Note: The MTU size must not be greater than 1500 bytes.
6.	Select DONE when finished.
7.	Select YES to save and return to the IP COMMUNICATIONS menu.

5.8 (U) Displaying IP Communications Information

Introduction	(U//FOU commun	O) The operator can display the information associated with the current IP ications configuration.
Procedure	(U//FOU informat	O) Follow these steps to display the IP communications configuration ion:
	Step	Action
	1.	From the MAIN MENU, select DISPLAY.
	2.	From the DISPLAY INFORMATION menu, select IP COMM.
		<u>Result</u> : The following screen is displayed for a TL with both interfaces on the same subnet:
		DISPLAY IP COMMS
		PROTOCOL: ETHERNET TL CT IP: 148.010.125.089 TL PT IP: 148.010.124.089
		Note: Specific values depend on the particular IP communications
		configuration.
	3.	Select DONE to return to the DISPLAY INFORMATION menu.

5.9 (U) Turning Ping Support On/Off

Introduction	(U//FOU Echo Re	O) TACLANE can be configured to enable or disable responses to ICMP quest (ping) messages sent to either of the TACLANE's two IP addresses.
Notes	(U//FOU • TAC • By d • Whe CT t ping ping • TAC addr	 ¹O) The following notes apply to enabling or disabling ping support: ¹CLANE must be offline in order to enable or disable ping support. ¹Lefault, ping support is ON. ¹In ping support is ON and TACLANE is in secure communications mode, network elements can ping the CT IP address, and PT network elements can g the PT IP address. Note that each side of the TACLANE only responds to gs for its own IP address (PT or CT). ¹CLANE does not respond to encrypted pings sent to either the CT or PT IP resses.
Procedure	(U//FOU	JO) Follow these steps to enable or disable ping support:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select NETWORK.
	3.	From the CONFIGURE NETWORK menu, select IP COMM.
	4.	From the IP COMM menu, select IP OPTIONS.
		Result: The following screen is displayed:
		CONFIGURE IP OPTIONS
		PING: ON
		PING: ON SELECT ACTION:
		PING: ON SELECT ACTION: CHANGE SAVE DONE
	5.	PING: ON SELECT ACTION: CHANGE SAVE DONE Select CHANGE to toggle ping support between ON and OFF.

Chapter 6. (U) Configuring/Managing Secure IP Paths

6.1 (U) Assigning a PPK to an IP Slot

Introduction	(U//FOUO) PPKs can be used to secure IP paths. The operator can assign a PPK to an IP slot by associating a PPK with a remote TACLANE IP address.(U//FOUO) When a remote TACLANE IP address is assigned to a PPK, all secure IP traffic passing through 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 to secure the IP traffic.
Multicast PPK Assignment	(U//FOUO) When configuring a PPK assignment, a multicast (Class D) address may be entered instead of a remote TACLANE IP address.
	(U//FOUO) When an SDD PPK is assigned, 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 Slot, continued

Notes	(U//FOUO) The following notes apply to assigning a PPK to an IP slot:
	• TACLANE must be offline, with a security level selected, in order to assign a PPK to an IP slot.
	 Only the SSO or a privileged user (see "Configuring Delegate Privileges") can access this command.
	• Up to 16 remote TACLANE or multicast IP addresses can be assigned to each PPK.
	• The number of remote TACLANE-to-PPK assignments is limited to 400. As an example, if all 48 PPK slots were used and each PPK was assigned to 8 remote TACLANEs, 384 of the 400 possible assignments would be used.
	• For pre-HAIPIS SAs using PPKs, 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, as well as at the same security level and with the same effective date.
	 For DS-100-1 key assignments, the CT and PT IP addresses must be entered. For DS-100-1 key assignments, if one of the IP addresses is unicast, then both IP addresses must be unicast.
	 For DS-74 keys, the PT IP address is not an option. For PPK configuration tips, see Appendix B, "IP/Ethernet Configuration Tips."

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

Procedure (U//FOUO) Follow these steps to assign a PPK to an IP slot:

Step	Action
1.	From the OFFLINE MAIN MENU, select CONFIG.
2.	From the CONFIGURATION menu, select SECURITY.
3.	From the CONFIGURE SECURITY menu, select PPK ASSIGN.
	Result: The PPK ASSIGNMENTS menu is displayed:
	PPK ASSIGNMENTS
	< <unclassified>></unclassified>
	>IP SLOT
	SELECT ITEM:
	SELECT DONE M MENU
4.	From the PPK ASSIGNMENTS menu, select IP SLOT.
	Result: The following screen is displayed:
	<unclassified>></unclassified>
	>01/SDD/USEVD 0000000120
	02/USR/USEVD 0000000121
	03/USR/0000005789/812345
	SELECT ACTION:
	SELECT DONE M_MENU
	<u>Note</u> : For DS-100-1 PPKs, the PPK ID, TYPE, TITLE, EDITION, and
	CRYPTONET EKMS ID EDITION and SEGMENT are displayed. The
	operator can list the entire list of information for each PPK by scrolling
	with the right and left arrow keys.
5.	Use the up and down arrow keys to navigate to a particular PPK.

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

Step	Action		
6.	Select SELECT.		
	Result: The following screen is displayed:		
	REMOTE INE		
	PPK ID: xx		
	02:		
	03:		
	<up down="" for="" more=""></up>		
	SELECT ACTION:		
	ASSIGN CANCEL		
	Note: The remote TACLANE IP address is the CT-side IP address of the		
	remote TACLANE. The order in which remote TACLANE IP addresses		
	appear does not matter.		
7.	Select ASSIGN.		
	Result: The following screen is displayed:		
	ASSIGN RMT INE		
	RMT PT: 000.000.000		
	SELECT ACTION.		
	+DIGIT -DIGIT DONE		
	Note: The above screen appears for a DS-100-1 PPK. For a DS-74 PPK,		
	there is no RMT PT prompt.		
8.	Use the arrow keys to navigate to a particular digit of the IP address. Use		
	the +DIGIT and –DIGIT function keys to increment or decrement each		
	digit. Leave leading zeros. For example, an IP address of 148.10.127.55		
	Is effected as 146.010.127.033.		
9.	Select DONE when finished.		
10.	Select YES to save changes.		
11.	Select DONE two times to return to the CONFIGURE SECURITY menu.		

6.2 (U) Entering Secure Communications Mode

Introduction	(U//FOUO) The operator may enter secure communications mode to secure IP paths.		
User CIK required for Secure Comm	(U//FOUO) A Rel 3.0 TACLANE with the SSO CIK inserted is not capable of entering the Secure Communications state. Instead, a User CIK must be inserted into the TACLANE for the unit to enter the Secure Communications state.		
	(U//FOUO) For instructions on how to create a User CIK, refer to the section titled "Copying a CIK".		
PPK takes precedence over FIREFLY	(U//FOUO) For secure IP paths, a PPK assignment takes precedence over generating a FIREFLY TEK.		
Automated Peer TACLANE Discovery	(U//FOUO) TACLANEs support automated peer TACLANE discovery for secure IP paths, through the HAIPIS Secure Dynamic Discovery (SDD) protocol, as described in HAIPIS 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 used to secure the IP traffic. Existing secure IP paths using FIREFLY TEKs are checked for a match based on the remote TACLANE IP address. If a match is found, the corresponding existing secure IP path (using a FIREFLY TEK) is used to secure the IP traffic. 		
	(U//FOUO) If there is no matching PPK assignment or secure IP path (using a FIREFLY TEK), and an operational FIREFLY vector set is usable at the current security level, the following occurs: a new secure IP path 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.		

(U) Entering Secure Communications Mode, continued

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. Multicast IP datagram traffic is not supported for FIREFLY.
Notes	 (U//FOUO) The following notes apply to securing IP paths: TACLANE must be offline, with a security level selected, in order to enter secure communications mode. A User CIK, and not the SSO CIK, must be inserted into the TACLANE 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. For pre-HAIPIS SAs using PPKs, all communicating TACLANEs must have valid PPK assignments with the same PPK filled at the same security level, with the same effective date, under the same PPK ID.

(U) Entering Secure Communications Mode, continued

Procedure

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

Step	Action	
1.	From the OFFLINE MAIN MENU, select OPERATION.	
2.	From the OPERATIONS menu, select SECURE COMM.	
	Result: The SECURE COMM MAIN MENU is displayed.	
	Note: The TACLANE is now in secure communications mode. The RUN status LED flashes, indicating that the TACLANE is ready to process traffic.	
3.	To exit secure communications mode , from the OPERATIONS menu, select OFFLINE.	
	Result: The following screen is displayed:	
	GO OFFLINE	
	< <unclassified>></unclassified>	
	All calls will be lost	
	GO OFFLINE?	
	YES NO	
4.	Select YES to exit secure communications mode and return to the OFFLINE MAIN MENU.	

6.3 (U) Displaying IP Path Information

ote	(U//FOU "Selectin	JO) The TACLANE must have a security level selected (See Section 4.9, ng a Security Level") in order to display IP path information.
ocedure	(U//FOU	JO) Follow these steps to display IP path information:
	Step	Action
	1.	From the MAIN MENU, select OPERATION.
	2.	From the OPERATIONS menu, select CALL INFO.
		<u>Result</u> : The following screen is displayed:
		CALL INFORMATION
		>SUMMARY DETAILED
		SELECT ITEM:
		SELECT DONE M_MENU
	3.	To display summary call information, select SUMMARY.
		<u>Result</u> : The following screen is displayed:
		SUMMARY CALL INFO
		TOTAL IP PATH: >0025 IP FF PATH: 0020 IP PPK PATH: 0005
		SELECT ACTION:
		DONE M_MENU

(U) Displaying IP Path Information, continued

Procedure (continued)

Step	Action		
5.	To display detailed call information, select DETAILED.		
	Result: The following screen is displayed:		
	DISPLAY DETAILED CALL		
	>IP PATHs		
	SELECT ITEM:		
	SELECT DONE M_MENU		
6.	Select SELECT.		
	Result: The following screen is displayed:		
	IP PATH INFO		
	00001:>125.095.053.101/197 00002: 131.108.001.003 00003: 200.012.105.033/148 <up down="" for="" more=""> SELECT RMT INE:</up>		
	MORE DONE M_MENU		
7.	Use the up and down arrow keys to navigate to a particular remote TACLANE's IP address(es).		
	Note: This is the remote TACLANE IP address associated with the secure IP path.		

(U) Displaying IP Path Information, continued

Step	Action
8.	Select MORE.
	<u>Result</u> : For secure IP paths using a FIREFLY TEK, the following screen is
	displayed (assumes HAIPIS security association):
	DETAILED IP PATH INFO
	RMT CT: >155.095.053.101 RMT PT: 192.133.039.048 FF/PPK: ENHANCED FF
	PT PMTU: xxxx SELECT ACTION:
	MORE DONE DELETE
	<u>Result</u> : For secure IP paths using a DS-101 PPK, the following screen is displayed:
	DETAILED IP PATH INFO
	RMT CT: >155.095.053.101 RMT PT: 192.133.039.048 FF/PPK: PPK <down for="" more=""> PPK ID: 01 TITLE: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</down>
	EDITION: G SEGMENT: 001 PT PMTU: xxxx SELECT ACTION:
	MORE DONE
	<u>Note</u> : The output display for a DS-74 PPK will contain a CRYPTONET and an EKMS ID value, but won't include a TITLE and a RMT PT value.
9.	Select DONE five times to return to the OPERATIONS menu.

6.4 (U) Deleting FIREFLY-Secured IP Paths

Introduction	(U//FOUO) The operator can delete a FIREFLY-secured IP path.		
Notes	(U//FOU	O) The following notes apply to deleting a FIREFLY-secured IP path:	
	 TAC Secu Dele route For a secu TAC Slot. 	"LANE must have a security level selected (See Section 4.9, "Selecting a nrity Level") in order to delete a FIREFLY-secured IP path. ting FIREFLY-secured IP paths does not affect remote TACLANE static es. a secure IP path using a PPK, the DELETE option is not available. (A re IP path using a PPK may be deleted by deassigning the remote CLANE IP address from the PPK. See "Deassigning a PPK from an IP .")	
Procedure	(U//FOU	O) Follow these steps to delete a FIREFLY-secured IP path:	
	Step	Action	
	1.	From the MAIN MENU, select OPERATION.	
	2.	From the OPERATIONS menu, select CALL INFO.	
		Result: The following screen is displayed:	
		CALL INFORMATION	
		SUMMARY >DETAILED	
		SELECT ITEM:	
		SELECT DONE M_MENU	
	3.	From the CALL INFORMATION menu. select DETAILED.	
	4	Select IP PATHs	

<u>Result</u>: The following screen is displayed:

IP PATH INFO 00001: >155.095.053.101 00002: 131.108.001.003 00003: 200.012.105.033 00004: 178.068.005.115 SELECT RMT INE: MORE DONE M_MENU	8 13
00001: >155.095.053.101 00002: 131.108.001.003 00003: 200.012.105.033 00004: 178.068.005.115 SELECT RMT INE: MORE DONE M_MENU	IP PATH INFO
00002: 131.108.001.003 00003: 200.012.105.033 00004: 178.068.005.115 SELECT RMT INE: MORE DONE M_MENU	00001: >155.095.053.101
00003: 200.012.105.033 00004: 178.068.005.115 SELECT RMT INE: MORE DONE M_MENU	00002: 131.108.001.003
00004: 178.068.005.115 SELECT RMT INE: MORE DONE M_MENU	00003: 200.012.105.033
SELECT RMT INE: MORE DONE M_MENU	00004: 178.068.005.115
MORE DONE M_MENU	SELECT RMT INE:
MORE DONE M_MENU	
·	MORE DONE M_MENU

(U) Deleting FIREFLY-Secured IP Paths, continued

Step	Action	
5.	Use the up and down arrow keys to navigate to a particular remote TACLANE IP address.	
	Note: This is the remote TACLANE IP address associated with the secure IP path.	
6.	Select MORE.	
	<u>Result</u> : For secure IP paths using a FIREFLY TEK, the following screen is displayed:	
	DETAILED IP PATH INFO	
	RMT INE: >155.095.053.101 EFF/FF/PPK: ENHANCED FF KMID: 00000002123456 PT PMTU: xxxx	
	SELECT ACTION:	
	MORE DONE DELETE	
7.	To delete the entire FIREFLY-secured IP path, select DELETE.	
8.	Select YES to confirm deletion of the FIREFLY-secured IP path.	
9.	Select DONE three times to return to the OPERATIONS menu.	

6.5 (U) Deassigning a PPK from an IP Slot

Introduction (U//FOUO) The operator can deassign a PPK from an IP slot. This in deassigning an assigned remote TACLANE IP address.		O) The operator can deassign a PPK from an IP slot. This involves ing an assigned remote TACLANE IP address.
Notes	(U//FOU • TAC PPK • Only acce	O) The following notes apply to deassigning a PPK from an IP slot: CLANE must be offline, with a security level selected, in order to deassign a from an IP slot. the SSO or a privileged user (see "Configuring Delegate Privileges") can ess this command.
Procedure	(U//FOU	O) Follow these steps to deassign a PPK from an IP slot:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select SECURITY.
	3.	From the CONFIGURE SECURITY menu, select PPK ASSIGN.
	4.	From the PPK ASSIGNMENTS menu, select IP SLOT.
		Result: The following screen is displayed:
		< <unclassified>></unclassified>
		>01/USR/0000005123/812345
		03/USR/0000005789/812345
		SELECT ITEM:
		Note: The operator can view the entire PPK ID/CRYPTONET/EKMS
		ID/EDITION/SEGMENT by scrolling with the right and left arrow keys.
	5.	Use the up and down arrow keys to navigate to a particular PPK.
	L	

(U) Deassigning a PPK from an IP Slot, continued

Step	Action		
6.	Select SELECT.		
	Result: The following screen is displayed:		
	PPK ID: xx 01: xxx.xxx.xxx 02: xxx.xxx.xxx 03: xxx.xxx.xxx <down for="" more=""> SELECT ACTION:</down>		
	ASGN/MOD DELETE CANCEL		
	<u>Note</u> : The remote TACLANE IP address is the CT-side IP address of the remote TACLANE. The order in which remote TACLANE IP addresses appear does not matter.		
7.	Use the up and down arrow keys to navigate to a particular remote TACLANE IP address.		
8.	Select DELETE.		
	Result: The following screen is displayed:		
	DELETE RMT INE ASSIGN		
	RMT CT: 155.095.053.101 RMT PT: 155.095.104.088		
	DELETE REMOTE INE?		
	CANCEL YES NO		
	<u>Note</u> : The above screen appears for a DS-100-1 PPK. For a DS-74 PPK, there is no RMT PT prompt.		
9.	Select YES to save changes.		
10.	Select DONE three times to return to the CONFIGURE SECURITY menu.		
6.6 (U) Configuring Remote TACLANE Static Routing

Introduction	(U//FOUO) The TACLANE operator can define static routes which associate destination IP networks/subnetworks with remote TACLANEs.
	(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/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 CT IP address, remote TACLANE PT IP address, destination network ID, and subnet mask. 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. Validation checks on table entries include: Subnet mask must be valid for the network ID. 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 combination of network ID and subnet mask is used to determine the remote TACLANE to which the IP traffic should be sent. GEM can also configure the routing table. One routing table can be generated at the GEM 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 subnet mask to $0.0.0.0$. This default static route entry will be used when no other entry in the table produces a match.
	(U//FOUO) When a default static route is defined, the TACLANE will never try to use Secure Dynamic Discovery (SDD).
	Continued on next page

(U) Configuring Remote TACLANE Static Routing, continued

Static Routing	(U//FOUO) Remote TACLANE static routing:
Features	 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 Secure Dynamic Discovery (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: check for specific static route in remote TACLANE static routing table if static route not found, use the default static route, if it is defined 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 perform SDD, then a default static route must not be configured.
Interoperability with Rel 2.x TACLANEs	(U//FOUO) If a Rel 3.0 TACLANE is to be interoperable with a Rel 2.x TACLANE, then the TACLANE static routes must be used. Rel 2.x TACLANEs do not support SDD. Also, the TACLANE backward compatibility must be ON in order that SAMP is supported in the 3.0 TACLANE. Note also that DS-74 PPKs or FIREFLY must be used with Rel 2.x TACLANEs. (U//FOUO) For an interoperability example, see Section B.9 in Appendix B.
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.

(U) Configuring Remote TACLANE Static Routing, continued

 PT Default Gateway or ARP Used to Deliver PT IP Iraffic (U//FOUO) If the optional PT default gateway IP address is configured, all o decrypted PT IP traffic will be delivered to the PT default gateway. (U//FOUO) If the optional PT default gateway is not configured, TACLANE 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 t to a received ARP request for a host in a network that is in the router's rou table. 		
CT Default Gateway or	(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.	
Deliver CT IP Traffic	(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.	
Subnet Masks and Static Routing	(U//FOUO) Restart the TACLANE after changing subnet masks when configuring a unit intended for static routing operation. Note that configuring static routes after setting subnet masks may cause the TACLANE to automatically restart. Also, setting subnet masks after configuring static routes (or downloading them from GEM) may cause a restart. When changes to the subnet masks do not cause the unit to automatically restart, the operator should manually restart the TACLANE (See Section 9.6, "Restarting the TACLANE").	
Notes	(U//FOUO) The following notes apply to configuring remote TACLANE static routes:	
	• TACLANE must be offline and in a security level in order to configure remote TACLANE static routes.	
	Continued on next page	

TL-275-06 15 March 2006

(U) Configuring Remote TACLANE Static Routing, continued

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

Step		Act	tion	
1.	From the OFFLINE N	AIN MENU, s	elect CONFIG.	
2.	From the CONFIGUE	RATION menu,	select SECURIT	Y.
3.	From the CONFIGUE	RE SECURITY	menu select STA	TIC RTE.
	Result: The STATIC	ROUTE GENE	RATION menu is	s displayed:
	S	TATIC ROUTE	GENERATION-	
		< <unclass< th=""><th>IFIED>></th><th></th></unclass<>	IFIED>>	
	>CF	EATE	MODIFY	
	DE	LETE	DELETE ALL	
	SEI	ECT ITEM:		
	SE	LECT DON	e m_menu	

(U) Configuring Remote TACLANE Static Routing, continued

Procedure (continued)

Step	Action			
4.	Select CREATE.			
	Result: The CREATE STATIC ROUTE screen is displayed:			
	CREATE STATIC ROUTE			
	NET MASK: 255.000.000.000			
	RMT CT: 148.010.000.011			
	<pre><down for="" more=""></down></pre>			
	RMT PT: 148.093.220.047			
	SELECT ACTION:			
	+DIGIT -DIGIT DONE			
	<u>Note</u> : The routing table entry with longest matching network ID and subnet mask combination will be determined to select the remote TACLANE to send the IP traffic to.			
	<u>Note</u> : One default route TACLANE table entry can be defined by setting the NET ID and NET MASK to 0.0.0.0.			
	Example static routing table entries:			
	Entry 1: Net ID: 0.0.0.0 Net Mask: 0.0.0.0 TL CT IP: 148.10.2.1 (default route) Entry 2: Net ID: 200.12.0.0 Net Mask: 255.255.0.0 TL CT IP: 148.10.4.11 Entry 3: Net ID: 200.12.3.0 Net Mask: 255.255.255.0 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.			
5.	Select DONE when finished, and YES to save changes.			

6.7 (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.			
Note	(U//FOUO) TACLANE must be offline and in a security level in order to modify remote TACLANE static routes.			
Procedure	(U//FOU	JO) Follow these steps to modify remote TACLANE static routes:		
	Step	Action		
	1.	From the OFFLINE MAIN MENU, select CONFIG.		
	2.	From the CONFIGURATION menu, select SECURITY.		
	3.	From the CONFIGURE SECURITY menu, select STATIC RTE.		
		Result: The STATIC ROUTE GENERATION menu is displayed:		
		STATIC ROUTE GENERATION- < <unclassified>> CREATE >MODIFY DELETE DELETE ALL</unclassified>		
		SELECT ITEM: SELECT DONE M_MENU		
	4.	Select MODIFY.		
		Result: The MODIFY STATIC ROUTE screen is displayed: MODIFY STATIC ROUTE 0001: 010.000.000/255. 0002: 100.001.000.000/255. 0003: 190.000.005.000/255. <down for="" more=""> SELECT ACTION: SELECT DONE M_MENU</down>		
	5.	Select the route to modify and make changes. Select DONE when finished, and YES to save changes.		

6.8 (U) Deleting Remote TACLANE Static Routes

Introduction	(U//FOUO) The operator can delete a remote TACLANE routing table entry or the entire routing table. See the section "Configuring Remote TACLANE Static Routing" for more information.			
Note	(U//FOU remote T	(U//FOUO) TACLANE must be offline and in a security level in order to delete remote TACLANE static routes.		
Procedure	(U//FOU	O) Follow these steps to delete remote TACLANE static routes:		
	Step	Action		
	1.	From the OFFLINE MAIN MENU, select CONFIG.		
	2.	From the CONFIGURATION menu, select SECURITY.		
	3.	From the CONFIGURE SECURITY menu, select STATIC RTE.		
		Result: The STATIC ROUTE GENERATION menu is displayed: STATIC ROUTE GENERATION- <unclassified>> CREATE MODIFY >DELETE DELETE ALL SELECT ITEM: </unclassified>		
	4.	To delete a single static route, select DELETE. <u>Result</u> : The DELETE STATIC ROUTE screen is displayed: DELETE STATIC ROUTE 0001: 010.000.000/255. 0002: 100.001.000.000/255. 0003: 190.000.005.000/255. <pre></pre>		
	5.	Select the route to delete. Select DONE when finished, and YES to delete the route and return to the STATIC ROUTE GENERATION menu.		

(U) Deleting Remote TACLANE Static Routes, continued

Procedure (continued)

Step	Action		
6.	To delete all static routes at the current security level , select DELETE ALL from the STATIC ROUTE GENERATION menu.		
	Result: The DELETE ALL STATIC ROUTES screen is displayed:		
	-DELETE ALL STATIC ROUTES-		
	Delete all Static route(s)		
	DELETE ALL STATIC ROUTES?		
	YES NO		
7.	Select YES to delete all static routes at the current security level.		
L			

6.9 (U) Displaying Remote TACLANE Static Routes

Introduction	(U//FOU	JO) The operator can display the remote TACLANE static routes.
Notes	(U//FOU "Selectin	JO) TACLANE must have a security level selected (See Section 4.9, ng a Security Level") in order to display static routes.
Procedure	(U//FOU	JO) Follow these steps to display static route information:
	Step	Action
	1.	From the MAIN MENU, select DISPLAY.
	2.	From the DISPLAY INFORMATION menu, select STATIC RTE.
		Result: The following screen is displayed:
		DISPLAY STATIC ROUTE
		0001. xxx xxx xxx xxx/xxx
		0001: xxx.xxx.xxx/xxx
		0003: xxx.xxx.xxx/xxx
		SELECT ACTION:
		Note: Specific values depend on the particular static routes.
	3.	Use the up and down arrow keys to navigate to a particular PPK.
	4	Select INFO
		Result: The following screen is displayed:
		DISPLAY STATIC ROUTE
		NET ID: XXX.XXX.XXX
		RMT CT: XXX XXX XXX
		RMT PT: XXX.XXX.XXX
		CELECT ACTION.
		SELECI ACITON.
		DONE
	5.	Select DONE twice to return to the DISPLAY INFORMATION menu.

6.10 (U) Configuring TACLANE EFF Mode

Introduction	 (U//FOUO) The TACLANE can establish security associations (SAs) using either Enhanced FIREFLY (EFF) or Basic FIREFLY. The operator can configure the TACLANE unit to be in one of two EFF modes: 1) <i>EFF-ONLY</i> – in this mode the TACLANE will only establish security associations with a FFVS using EFF. If EFF is not possible (e.g., the other INE has a vector set which doesn't support EFF), Basic FF is <u>not</u> tried. 2) <i>NEGOTIATE</i> – in this mode the TACLANE will try to establish security associations with a FFVS using EFF. If EFF is not possible, Basic FF is tried. 			
	 (U//FOUO) In order for a Rel 3.0 TACLANE to establish an SA using EFF, both of the following must be true: the filled FFVS must support EFF the remote INE and its FFVS must support EFF 			
What is EFF?	(U//FOUO) Enhanced FIREFLY (EFF) is a key management technique that makes use of existing FIREFLY technology to implement Elliptic Curve cryptography (specifically, a form of the MAYFLY Elliptic Curve technology). TACLANE is able to use MAYFLY with other enhanced-capable TACLANEs. TACLANE can also negotiate down, if necessary, to Basic FF for TACLANEs that have not been upgraded to support EFF. Enhanced FIREFLY therefore serves as a bridge between the existing FIREFLY infrastructure and the move to a solely Elliptic Curve solution.			
Notes	 (U//FOUO) The following notes apply to configuring the TACLANE EFF mode: The TACLANE must be offline with no security level selected (See "Exiting a Security Level") in order to configure the EFF setting. Only the SSO has the privilege to configure the EFF setting The default EFF value is NEGOTIATE. 			

(U) Configuring TACLANE EFF Mode, continued

Procedure (U//FOUO) Follow these steps to configure the TACLANE's EFF setting:

Step	Action
1.	From the MAIN MENU, select CONFIG.
2.	From the CONFIGURATION menu, select SECURITY.
3.	From the CONFIGURE SECURITY menu, select SA NEGOTIATE.
	Result: The following screen is displayed:
	-SA NEGOTIATION CONFIGURE-
	>EFF: NEGOTIATE DAILY MTEK: ENABLE SELECT ITEM:
4.	Set the EFF value to the desired value (NEGOTIATE or EFF-ONLY) and then select SAVE.
5.	Select DONE when finished.
6.	Select YES to confirm the information.

6.11 (U) Configuring Daily MTEK

Introduction	(U//FOU FIREFL updated performi (U//FOU paramete	 (O) The TACLANE operator can configure the method in which the Y TEKs are automatically updated every 24 hours. FIREFLY TEKs can be either deterministically, using the ACCORDION algorithm, or by ng a new IKE exchange and generating a new TEK (MTEK/MTEK update). (O) Specifically, the TACLANE operator configures the DAILY MTEK er to one of the following two values: (I) <i>ENABLE</i> – when enabled, MTEK/MTEK (IKE exchange) is the method used for the daily FIREFLY key update. (I) <i>DISABLE</i> (the default value) – when disabled, local ACCORDION update s the method used for the daily FIREFLY key update.
Notes	 (U//FOUO) The following notes apply to configuring the MTEK Update mode: The TACLANE must be offline with no security level selected (See "Exiting a Security Level") in order to configure the Daily MTEK setting. Only the SSO has the privilege to configure the Daily MTEK setting The default Daily MTEK value is DISABLE. 	
Procedure	(U//FOU	O) Follow these steps to configure the MTEK update setting:
	Step	Action
	1.	From the MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select SECURITY.
	3.	From the CONFIGURE SECURITY menu, select SA NEGOTIATE.
		Result: The following screen is displayed:
		-SA NEGOTIATION CONFIGURE-
		EFF: NEGOTIATE >DAILY MTEK: DISABLE
		SELECT ITEM:
		CHANGE SAVE DONE
	4.	Set the DAILY MTEK value to the desired value (DISABLE or ENABLE) and then select SAVE.
	5.	Select DONE when finished.
	6.	Select YES to confirm the information.

6.12 (U) Displaying the SA Negotiation Information

Introduction	(U//FOUO) The operator can display the SA Negotiation information, which includes the TACLANE's EFF setting and the MTEK Update setting.		
Procedure	(U//FOUO) Follow these steps to display the SA Negotiation information:		
	Step	Action	
	1.	From the MAIN MENU, select DISPLAY.	
	2.	From the DISPLAY INFORMATION menu, select SA NEGOTIATE.	
		Result: The following screen is displayed:	
		DISPLAY SA NEGOTIATION	
		EFF: NEGOTIATE	
		DAILY MTEK: DISABLE	
		SELECT ACTION:	
		DONE M_MENU	
	3.	Select DONE twice to return to the DISPLAY INFORMATION menu.	

(U) THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 7. (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 HAIPIS Traffic Flow 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.

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.

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.
	 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 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. For HAIPIS security associations, the resulting CT encrypted IP packets will be 60 bytes longer due to the addition of the AH and ESP headers (this assumes no fragmentation due to the TACLANE MTU size). For pre-HAIPIS security associations, the resulting CT encrypted IP packets will be 56 bytes longer (no ESP header).

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 if the Don't Fragment (DF) bit in the packet is set to "0". In this case, all fragments will be equal to the fixed packet length, with fragments being padded if necessary. (See the SFUG for more details on fragmentation.) Incoming PT IP user data packets longer than the fixed packet length are dropped if the DF bit in the packet is set to "1". 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 (regardless of data packet's DF bit value). Incoming PT IP user data packets shorter than the fixed packet length are padded to the fixed packet length. A destination unreachable message is sent to the originator if packets with DF bit set to "1" are discarded.
	(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.
	(U//FOUO) <u>Note</u> : Fixed Packet Length processing applies to all ESP IP datagrams, including IP multicast datagrams. Control messages such as SAMP and ARP are not affected by FPL processing.

Caveats	 (U//FOUO) The following caveats apply to Fixed Packet Length parameters: When the fixed packet mode is set to ON/DISCARD, incoming user data packets larger than the fixed packet length will be discarded. The MTU settings of PT-side hosts and routers may require modification in order to ensure that user data packets are not discarded. See Section B.3 in Appendix B for more information. The fixed packet mode should be set to ON/FRAGMENT when PT-side host and router MTU settings cannot be modified. When using TACLANEs in a nested configuration, the fixed packet mode of the inner TLs must <u>not</u> 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. (U//FOUO) FPL processing interacts with PMTU and DF bit bypass processing. If they are set in an incompatible way, performance will be greatly degraded. See Appendix B.3 for details.
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 as a result 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 5.7, "Modifying the TACLANE MTU Size."

(U) Configuring Fixed Packet Length Parameters, continued

Configuration	(U//FOU is selected Selecting paramete	(U//FOUO) IP TFS parameters must be saved once they are modified. When SAVE is selected from the IP TFS menu, all modifications to IP TFS parameters are saved. Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.		
Notes	(U//FOUO) The following notes apply to configuring Fixed Packet Length parameters:			
	 TACLANE must be offline with no security level selected in order to configure FPL parameters. Only the SSO has the privilege to configure FPL parameters. Audit log entries are generated when FPL parameters are modified. A change in the IP TFS parameters does not take effect until the TACLANE has been restarted. To minimize the number of restarts, all IP TFS parameters may be configured from the IP TFS menu prior to selecting SAVE. When SAVE is selected, all modifications to IP TFS parameters are saved. 			
Procedure	(U//FOU	IO) Follow these steps to configure the Fixed Packet Length parameters:		
Procedure	(U//FOU	IO) Follow these steps to configure the Fixed Packet Length parameters: Action		
Procedure	(U//FOU Step 1.	IO) Follow these steps to configure the Fixed Packet Length parameters: Action From the OFFLINE MAIN MENU, select CONFIG.		
Procedure	(U//FOU Step 1. 2.	IO) Follow these steps to configure the Fixed Packet Length parameters: Action From the OFFLINE MAIN MENU, select CONFIG. From the CONFIGURATION menu, select SECURITY.		
Procedure	(U//FOU Step 1. 2. 3.	O) Follow these steps to configure the Fixed Packet Length parameters: Action From the OFFLINE MAIN MENU, select CONFIG. From the CONFIGURATION menu, select SECURITY. From the CONFIGURE SECURITY menu, select IP TFS.		
Procedure	(U//FOU Step 1. 2. 3.	IO) Follow these steps to configure the Fixed Packet Length parameters: Action From the OFFLINE MAIN MENU, select CONFIG. From the CONFIGURATION menu, select SECURITY. From the CONFIGURE SECURITY menu, select IP TFS. Result: The Traffic Flow Security menu is displayed:		

Procedure (continued)

Step	Action
4.	Select FIXED PKT.
	Result: The FIXED PACKET menu is displayed:
	FIXED PACKET
	SELECT ITEM:
	SELECT DONE
5.	To configure the fixed packet mode, select MODE.
	Result: The FIXED PACKET MODE screen is displayed:
	FIXED PACKET MODE
	(Current: ON/FRAGMENT)
	>ON/FRAGMENT ON/DISCARD
	OFF
	SELECT ITEM:
	SELECT DONE
6.	Use the left and right arrow keys to navigate to the ON/FRAGMENT,
	ON/DISCARD, or OFF options. Select SELECT to change the current setting
7	Select DONE to return to the EIXED PACKET menu
7. 8	To modify the fixed packet length select LENGTH
0.	Result: The FIXED PACKET I FNGTH screen is displayed:
	FIXED PACKET LENGTH
	LENGTH (bytes): >0800
	SELECT ACTION.
	+48 -48 DONE

Procedure (continued)

Step	Action
9.	Use the +48 and -48 function keys to increment or decrement the fixed packet length by 48 bytes at a time. The minimum value is 176, the maximum value is 1424, and the default is 800.
10.	Select DONE when finished.
11.	Select YES to confirm the displayed fixed packet length and return to the FIXED PACKET menu.
	<u>Note</u> : Selecting NO will permit further modification of the length. Selecting ABORT will discard any change to the length and return to the IP TFS menu.
12.	Select DONE to return to the IP TFS menu.
	<u>Note</u> : Changes to IP TFS parameters must still be saved. However, other IP TFS parameters may be configured before selecting SAVE. When SAVE is selected, all IP TFS configuration changes will be saved at once. See the other sections in this chapter for instructions on configuring the other IP TFS parameters.
13.	To save the IP TFS configuration, select SAVE.
	<u>Note</u> : Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
14.	Select YES to restart the TACLANE and return to the OFFLINE MAIN MENU.

7.2 (U) Configuring Payload Sequence Number (PSEQN) Checking

Introduction (U//FOUO) The purpose of payload sequence numbers (PSEQNs) 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.

PSEQN Processing(U//FOUO) TACLANE-E100 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) When PSEQN checking is ON, the TACLANE only checks datagrams for valid PSEQN if they're received from HAIPIS SAs, but skips checking datagrams for valid PSEQN if they're received from pre-HAIPIS SAs. As an example, if a Rel 3.0 TACLANE with PSEQN checking set to ON has HAIPIS SAs established (with other Rel 3.0 TACLANEs) as well as pre-HAIPIS SAs established (with Rel 2.x TACLANEs, with Backward Compatibility = ON), the TACLANE performs PSEQN checks only for the HAIPIS SAs. The Release 2.1 TACLANE-E100s generated PSEQNs, however, the calculation of the PSEQN for the Release 2.1 TACLANEs was different than for HAIPIS (TACLANE Rel 3.0), so PSEQN processing is not compatible between the two releases.

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

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

Operator's Manual Revision 1.4 UNCLASSIFIED//FOUO

(U) Configuring Payload Sequence Number (PSEQN) Checking, continued

PSEQN Check Parameter	(U//FOUO) The PSEQN check parameter can only be configured by the SSO. It can be set to either ON or OFF. By default, this parameter is set to ON.
	(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 set to ON, packets received undergo PSEQN checking and only valid (non-replayed) traffic will be accepted.
	(U//FOUO) When the PSEQN check parameter is set to OFF, no PSEQN checking is done. In this case, all ESP datagrams are considered valid regardless of PSEQN value.
IP TFS Configuration	(U//FOUO) IP TFS parameters must be saved once they are modified. When SAVE is selected from the IP TFS menu, all modifications to IP TFS parameters are saved. Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
Notes	(U//FOUO) The following notes apply to configuring PSEQN checking:
	 TACLANE must be offline with no security level selected in order to configure PSEQN checking. Only the SSO has the privilege to configure the PSEQN checking An audit log entry is generated when the PSEQN check parameter is modified. A change in the PSEQN parameter does not take effect until the TACLANE has been restarted. To minimize the number of restarts, all IP TFS parameters may be configured from the IP TFS menu prior to selecting SAVE. When SAVE is selected, all modifications to IP TFS parameters are saved.

Procedure

(U) Configuring Payload Sequence Number (PSEQN) Checking, continued

Step	Action		
1.	From the OFFLINE MAIN MENU, select CONFIG.		
2.	From the CONFIGURATION menu, select SECURITY.		
3.	From the CONFIGURE SECURITY menu, select IP TFS.		
	Result: The IP TFS menu is displayed:		
	IP TFS		
	FIXED PKT >PSEON CHECK		
	BYPASS ICMP HOST		
	SELECT ACTION:		
	SELECI SAVE CANCEL		
4.	Select PSEON CHECK.		
	Result: The PSEON CHECK screen is displayed:		
	PSEQN CHECK		
	(Current: ON)		
	SELECT ITEM:		
	SELECI DONE		
5.	Use the arrow keys to navigate to the desired PSEQN check option.		
6.	Select SELECT to change the current setting.		
7.	Select DONE to return to the IP TFS menu.		
	Note: Changes to IP TFS parameters must still be saved. However, o		
	IP TFS parameters may be configured before selecting SAVE. When		
	SAVE is selected, all IP TFS configuration changes will be saved at o		
8.	To save the IP TFS configuration, select SAVE.		
	Note: Selecting CANCEL from the IP TFS menu will cause any unsa		
0	Changes to 1FS parameter settings to be lost.		

7.3 (U) Configuring DSCP Bypass

Introduction	 (U//FOUO) The DSCP bypass parameter can only be configured by the SSO. The 8-bit TOS field in the IP header has been superceded by 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 codepoint and referred to as the Differentiated Services Code Point (DSCP). The DSCP bypass parameter only applies to PT-to-CT traffic and provides the TACLANE SSO the following three options: "ON" – bypasses all 8 bits of the former TOS field (the 6-bit DSCP field as well as the 2-bit ECN field) "LIMITED" – restricts the bypass to only when the DSCP value is one of 21 standard values (see table on next page) "OFF" – no bypass of any of the 8 bits of the former TOS field
DSCP Bypass Parameter and Processing	(U//FOUO) The DSCP bypass parameter can be configured as either: ON, LIMITED, or OFF. The default setting for this parameter is OFF.
	(U//FOUO) When DSCP bypass is set to ON, the DSCP value and the ECN value is copied (i.e., bypassed) to the corresponding 8-bits of the CT IP header. Note that the bypass is from PT to CT, but not in the opposite direction.
	(U//FOUO) When DSCP bypass is set to LIMITED, the DSCP value from each PT IP header is compared to the list of 21 standard values (see table on next page). If it is one of the 21 standard DSCP values, then it is copied to the CT IP header. If the DSCP value is not one of the standard values, the codepoint in the CT IP header is set to all zeros. The two least significant bits of the DS field in the CT IP header are set to zero regardless of the DSCP value. Note that the bypass is from PT to CT, but not in the opposite direction.
	(U//FOUO) When DSCP bypass is set to OFF, all eight bits of the DS field in each CT IP header are set to zero.

(U) Configuring DSCP Bypass, continued

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

Table of DSCP
Bypass Values(U//FOUO) The following table lists the 21 standard DSCP values that will be
bypassed when DSCP bypass is set to LIMITED (and also bypassed when set to
ON):

IP TFS Configuration

(U//FOUO) IP TFS parameters must be saved once they are modified. When SAVE is selected from the IP TFS menu, all modifications to IP TFS parameters are saved. Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.

(U) Configuring DSCP Bypass, continued

Notes (U//FOUO) The following notes apply to configuring the DSCP bypass parameter: • TACLANE must be offline with no security level selected in order to configure the DSCP bypass parameter. • Only the SSO has the privilege to configure the DSCP bypass parameter. • An audit log entry is generated when the DSCP bypass parameter is modified. • A change in the IP TFS parameters does not take effect until the TACLANE has been restarted. To minimize the number of restarts, all IP TFS parameters may be configured from the IP TFS menu prior to selecting SAVE. When SAVE is selected, all modifications to IP TFS parameters are saved. Procedure (U//FOUO) Follow these steps to configure the DSCP bypass parameter: Step Action 1. From the OFFLINE MAIN MENU, select CONFIG. 2. From the CONFIGURATION menu, select SECURITY. 3. From the CONFIGURE SECURITY menu, select IP TFS. <u>Result</u>: The IP TFS menu is displayed: -----IP TFS------>FIXED PKT PSEQN CHECK BYPASS ICMP HOST SELECT ACTION: _____ SELECT | SAVE | CANCEL 4. Select BYPASS. <u>Result</u>: The BYPASS screen is displayed: -----BYPASS------DF BIT: CLEAR DSCP: >OFF IGMP: OFF <down for more> PMTU: OFF SELECT ACTION: CHANGE DONE

(U) Configuring DSCP Bypass, continued

Procedure (continued)

Step	Action
5.	Use the arrow keys to navigate down to the DSCP parameter.
6.	Select CHANGE to toggle the DSCP bypass parameter between ON, LIMITED, and OFF.
7.	Select DONE to return to the IP TFS menu.
	<u>Note</u> : Changes to IP TFS parameters must still be saved. However, other IP TFS parameters may be configured before selecting SAVE. When SAVE is selected, all IP TFS configuration changes will be saved at once.
8.	To save the IP TFS configuration, select SAVE.
	<u>Note</u> : Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
9.	Select YES to restart the TACLANE and return to the OFFLINE MAIN MENU.

7.4 (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 in one of three ways: "CLEAR" – always sets the DF bit in the CT IP header to "0" "SET" – always sets the DF bit in the CT IP header to "1" "COPY" – bypasses or copies the incoming DF bit value to the CT IP header DF bit value (U//FOUO) The DF Bit bypass parameter can only be configured by the SSO. (U//FOUO) The DF Bit bypass setting affects FPL and PMTU processing. See those sections and Appendix B.3 for details.
DF Bit Bypass Parameter and Processing	 (U//FOUO) The DF Bit bypass parameter can be configured as either: CLEAR, SET, or COPY. The default setting for this parameter is CLEAR. 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 CLEAR, the DF bit in the CT IP header is always set to "0". (U//FOUO) When the DF Bit bypass is set to SET, the DF bit in the CT IP header is always set to "1". (U//FOUO) When the DF Bit bypass is set to COPY, the DF bit in the CT IP header is set to the incoming DF bit value (bypass).
IP TFS Configuration	(U//FOUO) IP TFS parameters must be saved once they are modified. When SAVE is selected from the IP TFS menu, all modifications to IP TFS parameters are saved. Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
Notes	 (U//FOUO) The following notes apply to configuring the DF Bit Bypass: TACLANE must be offline with no security level selected in order to configure the DF Bit bypass parameter. Only the SSO has the privilege to configure the DSCP bypass parameter. An audit log entry is generated when the DF Bit bypass parameter is modified. A change in the IP TFS parameters does not take effect until the TACLANE has been restarted. To minimize the number of restarts, all IP TFS parameters may be configured from the IP TFS menu prior to selecting SAVE. When SAVE is selected, all modifications to IP TFS parameters are saved.

Procedure

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

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

Step	Action
1.	From the OFFLINE MAIN MENU, select CONFIG.
2.	From the CONFIGURATION menu, select SECURITY.
3.	From the CONFIGURE SECURITY menu, select IP TFS.
	Result: The IP TFS menu is displayed:
	IP TFS
	>FIXED PKT PSEQN CHECK BYPASS ICMP HOST
	SELECT ACTION:
	SELECT SAVE CANCEL
4.	Select BYPASS.
	Result: The BYPASS screen is displayed:
	DF BIT: CLEAR DSCP: >OFF IGMP: OFF <down for="" more=""> PMTU: OFF</down>
	SELECT ACTION:
	CHANGE DONE
5.	Select CHANGE to toggle the DF Bit bypass parameter between CLEAR, SET, and COPY.

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

Procedure (continued)

Step	Action
6.	Select DONE to return to the IP TFS menu.
	Note: Changes to IP TFS parameters must still be saved. However, other IP TFS parameters may be configured before selecting SAVE. When SAVE is selected, all IP TFS configuration changes will be saved at once. See the other sections in this chapter for instructions on configuring the other IP TFS parameters.
7.	To save the IP TFS configuration, select SAVE.
	<u>Note</u> : Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
8.	Select YES to restart the TACLANE and return to the OFFLINE MAIN MENU.

FPL

7.5 (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. In order to support PMTU discovery, the PMTU Bypass parameter must be configured to "ON" in order for the TACLANE to process ICMP Destination Unreachable messages.

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

PMTU Bypass (U//FOUO) The TACLANE PMTU Bypass support is independent of the DF Bit and DF Bit Bypass support, however, only certain combinations are practical. The DF bit must Bypass and be bypassed (i.e., the DF Bit Bypass set to "SET") in order for full PT host PMTU discovery support. In PMTU Discovery, a host would set the DF bit to "don't fragment" in order to learn the MTU size of the path. A packet set to "don't fragment" that is too large for the network element is dropped and a Destination Unreachable message is sent to the originator, telling what the MTU size is. Then the originator adjusts its MTU size accordingly and has optimum performance. Only if the host sets the DF bit to "don't fragment" does the host get feedback about the maximum MTU size of the path.

- If PMTU Bypass is set to OFF, the DF Bit Bypass should always be set to "may fragment" (i.e., the DF Bit Bypass set to "CLEAR" or "COPY"). The only reason to set the DF Bit Bypass to "don't fragment" (i.e., "SET") is to gain knowledge of the path MTU size so that the host may adjust its MTU size.
- When PMTU Bypass is ON, the DF Bit Bypass should always be set to "COPY". PMTU discovery is dynamic and the MTU associated with a given SA may change at any time during communications. After a period of time, the TACLANE increases the MTU to the maximum MTU size. This allows for cases where the PMTU was lowered due to a temporary link failure that has since been corrected. The PMTU discovery mechanisms in the network continue to adjust the MTU as needed.
- If FPL is enabled, PMTU should be OFF so that the MTU of the host can be set to the most efficient length based on the FPL.

(U) Configuring PMTU Bypass, continued

PMTU Bypass Parameter and Processing	(U//FOUO) If the TACLANE's PMTU Bypass parameter is set to ON, 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 OFF, 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 OFF.
	(U//FOUO) Note that if the TACLANE's ICMP Notification Host is configured, the ICMP Destination Unreachable message received at the CT interface will result in an SNMP trap message to the ICMP notification host indicating that a Destination Unreachable was received.
	(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.
IP TFS Configuration	(U//FOUO) IP TFS parameters must be saved once they are modified. When SAVE is selected from the IP TFS menu, all modifications to IP TFS parameters are saved. Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
Notes	(U//FOUO) The following notes apply to configuring the PMTU Bypass parameter:
	 TACLANE must be offline with no security level selected in order to configure 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. A change in the IP TFS parameters does not take effect until the TACLANE has been restarted. To minimize the number of restarts, all IP TFS parameters may be configured from the IP TFS menu prior to selecting SAVE. When SAVE is selected, all modifications to IP TFS parameters are saved.

(U) Configuring PMTU Bypass, continued

Procedure (U//FC

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

Step	Action
1.	From the OFFLINE MAIN MENU, select CONFIG.
2.	From the CONFIGURATION menu, select SECURITY.
3.	From the CONFIGURE SECURITY menu, select IP TFS.
	Result: The IP TFS menu is displayed:
	IP TFS
	>FIXED PKT PSEQN CHECK BYPASS ICMP HOST
	SELECT ACTION:
	SELECT SAVE CANCEL
4.	Select BYPASS.
	Result: The BYPASS screen is displayed:
	BYPASS
	DF BIT: CLEAR DSCP: OFF IGMP: OFF <down for="" more=""> PMTU: >OFF</down>
	SELECT ACTION:
	CHANGE DONE
5.	Select CHANGE to toggle the PMTU bypass parameter between ON and OFF.
6.	Select DONE to return to the IP TFS menu.
	<u>Note</u> : Changes to IP TFS parameters must still be saved. However, other IP TFS parameters may be configured before selecting SAVE. When SAVE is selected, all IP TFS configuration changes will be saved at once. See the other sections in this chapter for instructions on configuring the other IP TFS parameters.

(U) Configuring PMTU Bypass, continued

Procedure (continued)

Step	Action
7.	To save the IP TFS configuration, select SAVE.
	<u>Note</u> : Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
8.	Select YES to restart the TACLANE and return to the OFFLINE MAIN MENU.

7.6 (U) Configuring IGMP Bypass

Introduction	 (U//FOUO) The Internet Group Management Protocol (IGMP) 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 Bypass parameter, configurable as ON or OFF, determines whether the TACLANE will regenerate IGMP traffic for user multicast traffic.
IGMP Bypass Parameter and Processing	(U//FOUO) When the IGMP Bypass is set to ON, 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 Bypass is set to ON, the TACLANE regenerates user IGMP messages traveling from both CT-to-PT as well as from PT-to-CT.
	(U//FOUO) When the IGMP Bypass is set to OFF, the TACLANE treats all PT IGMP messages from the PT network as user multicast traffic to be encrypted. Similarly, the TACLANE (with IGMP Bypass set to OFF) treats all IGMP messages from the CT network as user multicast traffic to be decrypted.
	(U//FOUO) The default for the IGMP Bypass parameter is OFF.
	(U//FOUO) Setting the IGMP Bypass parameter to ON is necessary in the case where the multicast router(s) exist on the TACLANE's CT network.
	(U//FOUO) Note that the TACLANE also supports IGMP on the CT side in order to support the HAIPIS 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 Bypass parameter is ON or OFF, the TACLANE will support IGMP for SDD traffic so long as the SDD multicast group is configured (i.e., assigned to the SDD PPK).
IP TFS Configuration	(U//FOUO) IP TFS parameters must be saved once they are modified. When SAVE is selected from the IP TFS menu, all modifications to IP TFS parameters are saved. Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
(U) Configuring IGMP Bypass, continued

Notes (U//FOUO) The following notes apply to configuring the IGMP Bypass: • TACLANE must be offline with no security level selected in order to configure the IGMP 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. • A change in the IP TFS parameters does not take effect until the TACLANE has been restarted. To minimize the number of restarts, all IP TFS parameters may be configured from the IP TFS menu prior to selecting SAVE. When SAVE is selected, all modifications to IP TFS parameters are saved. Procedure (U//FOUO) Follow these steps to configure the IGMP bypass parameter: Step Action 1. From the OFFLINE MAIN MENU, select CONFIG. 2. From the CONFIGURATION menu, select SECURITY. 3. From the SECURITY menu, select IP TFS. Result: The IP TFS menu is displayed: -----IP TFS------FIXED PKT BYPASS PSEQN CHECK >ICMP HOST SELECT ACTION: _____ SELECT | SAVE | CANCEL 4. Select BYPASS. Result: The BYPASS screen is displayed: -----BYPASS------DF BIT: CLEAR DSCP: OFF IGMP: OFF <down for more> PMTU: >OFF SELECT ACTION: _____ CHANGE DONE 5. Select CHANGE to toggle the IGMP bypass parameter between ON and OFF.

(U) Configuring IGMP Bypass, continued

Procedure (continued)

Step	Action
6.	Select DONE to return to the IP TFS menu.
	Note: Changes to IP TFS parameters must still be saved. However, other IP TFS parameters may be configured before selecting SAVE. When SAVE is selected, all IP TFS configuration changes will be saved at once. See the other sections in this chapter for instructions on configuring the other IP TFS parameters.
7.	To save the IP TFS configuration, select SAVE.
	<u>Note</u> : Selecting CANCEL from the IP TFS menu will cause any unsaved changes to TFS parameter settings to be lost.
8.	Select YES to restart the TACLANE and return to the OFFLINE MAIN MENU.

7.7 (U) Configuring the ICMP Notification Host

Introduction	(U//FOU When th SNMP ti message	O) The ICMP Notification Host address can be configured by the SSO. e ICMP Host is configured, TACLANE will attempt to notify this host via rap messages when an ICMP Source Quench or Destination Unreachable is received from the CT network.
	(U//FOU the ICM	O) This feature is disabled by default. To disable after using the feature, set P Notification Host IP address to 0.0.0.0.
	(U//FOU manager	O) The ICMP Notification Host address can be the same as the PT network IP address.
IP TFS Configuration	(U//FOU is selecting paramete	O) IP TFS parameters must be saved once they are modified. When SAVE ad from the IP TFS menu, all modifications to IP TFS parameters are saved. B CANCEL from the IP TFS menu will cause any unsaved changes to TFS per settings to be lost.
Notes	(U//FOU	O) The following notes apply to configuring the ICMP Host:
	 TAC the l Only An a A ch beer be c select 	CANE must be offline with no security level selected in order to configure CMP Host. The SSO has the privilege to configure the ICMP Host. Udit log entry is generated when the ICMP Host is modified. ange in the IP TFS parameters does not take effect until the TACLANE has restarted. To minimize the number of restarts, all IP TFS parameters may onfigured from the IP TFS menu prior to selecting SAVE. When SAVE is cted, all modifications to IP TFS parameters are saved.
Procedure	(U//FOU	O) Follow these steps to configure the ICMP Host:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select SECURITY.

(U) Configuring the ICMP Notification Host, continued

Procedure (continued)

Step	Action
3.	From the SECURITY menu, select IP TFS.
	Result: The IP TFS menu is displayed:
	IP TFS
	FIXED PKT BYPASS
	PSEQN CHECK >ICMP HOST
	SELECT ACTION:
	SELECT SAVE CANCEL
	Salect ICMP HOST
ч.	Popult: The CONFICURE ICMR HOST series is displayed:
	<u>Result</u> . The CONFIGURE ICMP HOST screen is displayed.
	ICMP HOST: 000.000.000
	SELECT ACTION:
	+DIGIT -DIGIT DONE
5.	Use the left and right arrow keys to navigate to a particular digit of the
	ICMP Host address. Use the +DIGIT and -DIGIT function keys to increment or decrement each digit. Leave leading zeroes. For example, an
	IP address of 148.10.127.55 is entered as "148.010.127.055."
6.	Select DONE, then YES, to return to the IP TFS menu.
	Note: Changes to IP TFS parameters must still be saved. However, other
	IP TFS parameters may be configured before selecting SAVE. When
	SAVE is selected, all IP TFS configuration changes will be saved at once.
	other IP TFS parameters
7.	To save the IP TFS configuration. select SAVE.
	Note: Selecting CANCEL from the IP TES menu will cause any unsaved
	changes to TFS parameter settings to be lost.
8.	Select YES to restart the TACLANE and return to the OFFLINE MAIN
	MENU.

7.8 (U) Displaying IP Traffic Flow Security Information

Introduction	(U//FOU Traffic F	JO) The operator can display the information associated with the current IP Flow Security configuration.
Notes	(U//FOU displayin configur displaye	IO) The restrictions on configuring IP TFS parameters do not apply to ng their current settings. The SSO is not required; displaying the IP TFS ation is not limited to the SSO. Also, the IP TFS configuration may be d in any operating mode.
Procedure	(U//FOU informat	IO) Follow these steps to display the IP Traffic Flow Security configuration ion:
	Step	Action
	1.	From the MAIN MENU, select DISPLAY.
	2.	From the DISPLAY INFORMATION menu, select IP TFS.
		Result: The following screen is displayed:
		DISPLAY IP TFS INFO
		FIXED PACKET : ON/FRAG FIXED PKT LEN: 800 <down for="" more=""> PSEQN CHECK: ON DF BIT BYPASS: CLEAR DSCP BYPASS: OFF IGMP BYPASS: OFF IGMP BYPASS: OFF ICMP HOST: 148.10.1.1 SELECT ACTION: </down>
		DONE M_MENU
		Note: Specific values depend on the particular IP TFS configuration.
	3.	Select DONE to return to the DISPLAY INFORMATION menu.

(U) THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 8. (U) Configuring Access Control and the Network Manager

8.1 (U) Turning Discretionary Access Control On/Off

Introduction	(U//FOU discretion TEKs. I (U//FOU pass mar (U//FOU performe FIREFL (See "Cr	 (O) TACLANE discretionary access control can be enabled or disabled. The nary access control check only applies to secure IP paths using FIREFLY Discretionary access control is OFF by default. (O) When OFF (disabled), all secure IP paths using FIREFLY TEKs that adatory access control checks are allowed. (O) When ON (enabled), this additional discretionary access control check is ed: Only secure IP paths using FIREFLY TEKs created using remote Y vector sets with KMIDs on the Access Control List (ACL) are allowed.
Notes	(U//FOU control: • TAC cont • Only • Disc	O) The following notes apply to enable or disable discretionary access CLANE must be offline in order to enable or disable discretionary access rol. the SSO has the privilege to access this command. retionary access control is OFF by default.
Procedure	(U//FOU	O) Follow these steps to enable or disable discretionary access control:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select SECURITY.
	3.	From the CONFIGURE SECURITY menu, select ACCESS MODE.
		Result: The following screen is displayed: ACCESS CONTROL MODE (Current: ON) >ON OFF SELECT ITEM: SELECT DONE M_MENU

(U) Turning Discretionary Access Control On/Off, continued

Procedure (continued)

Step	Action
4.	Use the left and right arrow keys to navigate to the ON or OFF setting.
5.	Select SELECT to change the access control mode and return to the CONFIGURE SECURITY menu.

Operator's Manual
Revision 1.4

8.2 (U) Displaying Discretionary Access Control Mode

Introduction(U//FOUO) The operator can display the discretionary access control (DAC) mode.
The discretionary access control check only applies to secure IP paths using
FIREFLY TEKs.Procedure(U//FOUO) Follow these steps to display the discretionary access control mode:

Step	Action
1.	From the OFFLINE MAIN MENU, select DISPLAY.
2.	From the DISPLAY menu, select ACCESS MODE.
	Result: The following screen is displayed:
	DISPLAY ACCESS MODE
	ACCESS MODE: ON
	SELECT ACTION:
	DONE M_MENU
3.	Select DONE to return to the DISPLAY INFORMATION menu.

8.3 (U) Creating an ACL Entry

Introduction	(U//FOU ACL con remote F secure II ACL are one ACI	JO) The SSO operator can create Access Control List (ACL) entries. The asists of a list of up to 256 KMIDs. These KMIDs are associated with FIREFLY vector sets. When discretionary access control is enabled, only P paths associated with remote FIREFLY vector sets with KMIDs on the allowed. (See "Turning Discretionary Access Control On/Off.") There is L and it applies to all security levels.
Notes	(U//FOU • TAC	JO) The following notes apply to creating an ACL entry: CLANE must be offline to create an ACL entry.
	• Ther • The	The is one ACL and it applies to all security levels. ACL is limited to a maximum of 256 entries.
Procedure	(U//FOU	JO) Follow these steps to create an ACL entry:
	Step	Action
	1.	From the OFFLINE MAIN MENU, select CONFIG.
	2.	From the CONFIGURATION menu, select SECURITY.
	3.	From the CONFIGURE SECURITY menu, select ACL.
	4.	From the ACL menu, select CREATE.
		Result: The following screen is displayed:
		CREATE ACL ENTRY < <unclassified>></unclassified>
		KMID: xxxxxxxxxxxx
		SFLECT ACTION:
		+DIGIT -DIGIT DONE
	5.	Use the arrow keys to navigate to a particular digit of the KMID. Use the +DIGIT and -DIGIT function keys to increment or decrement each digit. Leave leading zeros. For example, an KMID of 123456 is entered as "00000000123456."
		Note: The KMIDs must be unique for each ACL entry.
	6.	Select DONE when finished.
	7.	Select YES to save the ACL entry.
	8.	Select DONE to return to the CONFIGURE SECURITY menu.
	L	

8.4 (U) Modifying an ACL Entry

Introduction (U//FOUO) The SSO operator can modify Access Control List (ACL) entries. The ACL consists of a list of up to 256 KMIDs. The KMIDs are associated with remote FIREFLY vector sets. Notes (U//FOUO) The following notes apply to modifying an ACL entry: • TACLANE must be offline to modify an ACL entry. • Only the SSO has the privilege to access this command. • There is one ACL and it applies to all security levels. **Procedure** (U//FOUO) Follow these steps to modify an ACL entry: Step Action 1. From the OFFLINE MAIN MENU, select CONFIG. 2. From the CONFIGURATION menu, select SECURITY. 3. From the CONFIGURE SECURITY menu, select ACL. 4. From the ACL menu, select MODIFY. <u>Result</u>: The following screen is displayed: ----MODIFY ACL ENTRY-----<<UNCLASSIFIED>> 001: >xxxxxxxxxxxxxx 002: xxxxxxxxxxxxxx 003: xxxxxxxxxxxxxxxx <down for more> SELECT ACTION: _____ SELECT | DONE M_MENU 5. Use the up and down arrow keys to navigate to a particular ACL entry. 6. Select SELECT. 7. Use the arrow keys to navigate to a particular digit of the KMID. Use the +DIGIT and -DIGIT function keys to increment or decrement each digit. Leave leading zeros. For example, a KMID of 123456 is entered as

 "00000000123456."

 Note: The KMIDs must be unique for each ACL entry.

 8.
 Select DONE when finished.

 9.
 Select YES to save the ACL entry.

 10.
 Select DONE to return to the CONFIGURE SECURITY menu.

8.5 (U) Deleting an ACL Entry

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.

Notes

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

- TACLANE must be offline to delete an ACL entry.
- Only the SSO has the privilege to access this command.
- There is one ACL and it applies to all security levels.

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

Step	Action
1.	From the OFFLINE MAIN MENU, select CONFIG.
2.	From the CONFIGURATION menu, select SECURITY.
3.	From the CONFIGURE SECURITY menu, select ACL.
4.	From the ACL menu, select DELETE.
	Result: The following screen is displayed:
	DELETE ACL ENTRY
	< <unclassified>></unclassified>
	001: >XXXXXXXXXXXXX 002: XXXXXXXXXXX 003: XXXXXXXXXXX
5.	Use the up and down arrow keys to navigate to a particular ACL entry.
6.	To delete an ACL entry, select DELETE.
7.	Select YES to delete the ACL entry.
8.	Select DONE to return to the CONFIGURE SECURITY menu.

Operator's Manual
Revision 1.4

8.6 (U) Displaying the ACL

Introduction (U//FOUO) The operator can display the Access Control List (ACL) entries. The ACL consists of a list of up to 256 KMIDs. There is one ACL and it applies to all security levels.

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

Step	Action
1.	From the OFFLINE MAIN MENU, select DISPLAY.
2.	From the DISPLAY menu, select ACL.
	Result: The following screen is displayed:
	DISPLAY ACL
	001: xxxxxxxxxxxx 002: xxxxxxxxxxx 003: xxxxxxxxxxx <down for="" more="" up=""> n : xxxxxxxxxxxxx SELECT ACTION: </down>
3.	Select DONE to return to the DISPLAY INFORMATION menu.

8.7 (U) Configuring the Network Manager

Introduction	 (U//FOUO) The operator can configure the TACLANE to be managed by a remote network manager (GEM). The operator can configure both a primary network manager and a backup network manager. For each manager, the SSO operator configures the following parameters: management interface (CT vs. PT) network manager IP address fronting TACLANE's CT and PT IP addresses* KMID (up to 2 KMID values)* *Note: these last two parameters are only applicable if management interface = CT. 		
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 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.		
Primary and Backup Managers	 (U//FOUO) The following notes apply to the primary and backup managers: The TACLANE supports both a primary and a backup network manager. The TACLANE operator can configure one primary and one backup manager per security level. The backup manager is an optional configuration – e.g., a TACLANE can be configured with only a primary manager and no backup manager. The TACLANE only communicates with one of the managers at a given time. If TACLANE loses communications with the primary manager, the TACLANE will attempt to contact the backup manager (if one is configured) and set up a security association with the backup manager. If successful, the backup manager would become the TACLANE's active manager while the primary manager becomes the inactive manager. If the backup manager should later lose communication, then the TACLANE will attempt to switchover to the primary manager. The local HMI operator can only modify the network manager settings when the TACLANE is in the Offline in Security Level state. The remote manager can only modify the TACLANE's network manager state or the Offline in Security Level state. 		

Backup Manager Configuration Limitation (U//FOUO) If a TACLANE network contains both a primary and backup network manager, there is one scenario in which a security association (SA) problem can arise with a fronting TACLANE.

(U//FOUO) Consider the following network configuration:

```
GEM 1 ----- TL A --+-- TL B ----- GEM 2
|
TL X
```

(U//FOUO) In this example, GEM 1 is the primary network manager, GEM 2 is the backup network manager, TL A is the TACLANE fronting GEM 1, TL B is the TACLANE fronting GEM 2, and TL X is another TACLANE in the network. In this setup, SA establishment problems only arise between TL A and TL B when they both have each other in their network manager configurations. Specifically,

TL A: primary = GEM 1, backup = GEM 2 TL B: primary = GEM 1, backup = GEM 2

(U//FOUO) If users want to configure TLs this way, then they should not enter GEM 2 in the remote manager configuration for TL A. As a work-around, here's the recommended configuration for this sample network above:

TL A: primary = GEM 1, backup = none TL B: primary = GEM 1, backup = GEM 2 TL X: primary = GEM 1, backup = GEM 2

(U//FOUO) In this way, all TLs can be managed by GEM 1, the primary manager. In the event that the primary manager cannot be used, the only TL that cannot be managed by GEM 2, the backup manager, is TL A. This might not be an issue, since TL A could be the reason why the primary manager cannot be used. In order for TL A to be managed by GEM 2, the backup manager configuration must be deleted from TL B and added to TL A. These changes will have to be undone later in order to manage TL B from GEM 1, the primary manager.

Network Manager

(GEM)

Network	(U//FOUO) The follo	wing notes apply to the	e network manager K	MID:	
Manager KMID	• For a network ma no need for the T	anager that connects via ACLANE operator to	a the TACLANE's PI enter a KMID value s	T interface, there is ince the traffic is	
	 For a network manager that connects via the TACLANE's CT interface, the TACLANE operator must configure the KMID number of the FIREFLY vector set of the TACLANE fronting the network manager. The managed TACLAN verifies that the KMID number matches one of the configured KMID values for the remote manager. TACLANE only accepts management traffic from the authorized remote managers. When the vector set of the TACLANE fronting the network manager is replaced the managed TACLANEs need to be reconfigured with the new KMID. To support this, the TACLANE now supports two KMID values per network manager (while TACLANE new supports two KMID values per network manager (while TACLANE is in the Secure Communications state or in the Offline in Security Level state) or by the local TACLANE operator (while TACLANE is in the Offline in Security Level state). As an example, the remomanager can remotely fill in the KMID value for the new vector set in the 2nd KMID slot for the manager. When the new vector set is used, the TACLANE ready to authorize the remote manager and accept management traffic. The network manager can only edit the 'inactive' KMID value in the TACLANE network manager SA) After switching to a new KMID value, the operator should delete the previous KMID value. 				
HMI vs. Remote Manager Update	(U//FOUO) The following table summarizes the differences between the local HMI operator (SSO) updating the TACLANE's network manager parameters vs. the remote network manager updating the TACLANE's network manager parameters:			een the local HMI meters vs. the ager parameters:	
		State of TACLANE	TI Not Man	TACIANE	
		necessary to undate	norometers that	restorted on	
		TL Net Mor narams	are configurable	undate?	
	Local HMI	Offline in Security	All NM parameters	Yes except in	
	operator (SSO)	Level	Parameters	case where only	
	r (22.2)			KMID values updated	

No

Offline in Security

Level or Secure

Communications

1) The Active Net

Mgr's 'inactive'

KMID 2) All of the Inactive Net Mgr parameters

(U) Configu	ring the Network Manager, continued
Secure Remote Management Using SNMP	 (U//FOUO) TACLANEs can be managed by GEM using SNMPv1 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 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 full (at 80% full and 100% full) and low battery SNMP traps) Configuring a Bad Guy List (BGL) which is a list of up to 256 KMIDs with which the TACLANE cannot set up security associations (U//FOUO) GEM also provides network management of TACLANE-protected network elements using SNMPv1. Please refer to the appropriate GEM Operator's Manual for more information on configuring the TACLANE fronting the GEM and for more information on GEM.
Notes	 (U//FOUO) The following notes apply to a local HMI operator configuring the network manager parameters: The TACLANE must be Offline with a security level selected state. Only the SSO can perform this function It is possible to save network manager configuration information for multiple security levels. For example, a TACLANE unit at the UNCLASSIFIED level can have one set of network manager configuration. If that same TACLANE unit is configured at the SECRET security level, the operator can enter different network manager parameters while not overriding the other network manager parameters. TACLANE will restart after completing this command except in the case where only the KMID value(s) were updated.
	Continued on next page

TL-275-06

15 March 2006

Operator's Manual

Revision 1.4

UNCLASSIFIED//FOUO

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

Step	Action		
1.	From the OFFLINE MAIN MENU, select CONFIG.		
2.	From the CONFIGURATION menu, select SECURITY.		
3.	From the CONFIGURE SECURITY menu, select NETWORK MGR.		
4.	Select CONFIGURE.		
	Result: The following screen is displayed:		
	CONFIGURE NETWORK MGR		
	>PRIMARY BACKUP		
	SELECT ITEM: SELECT SAVE CANCEL		
5.	From the CONFIGURE NETWORK MGR menu, select either the PRIMARY or BACKUP network manager to configure.		
	Result: The following screen is displayed:		
	CONFIGURE NETWORK MGR < <primary>></primary>		
	>KMID MANAGER ADDR MGMT I/F RMT INE ADDR		
	SELECT ITEM:		
	SELECT SAVE CANCEL		

Procedure (continued)

Step	Action		
6.	To configure the network manager interface, select MGMT I/F.		
	Result: The following screen is displayed:		
	MANAGEMENT I/F		
	(Current: CT)		
	>CT PT		
	SELECT ITEM:		
	SELECT DONE		
	<u>Note</u> : When configuring a TACLANE which is FRONTING a network manager, the MGMT I/F must be set to PT.		
7.	Use the left and right arrow keys to navigate between the CT and PT setting.		
8.	Select SELECT.		
9.	Select DONE.		
10.	To configure the CT and PT IP addresses of the INE fronting the		
	network manager (note: only necessary if using remote TACLANE static routing), select RMT INE ADDR.		
	Result: The following screen is displayed:		
	REMOTE IP ADDRESSES		
	DMT CT: 149 020 152 097		
	RMT PT: 148.020.152.087		
	SELECT ACTION:		
	+DIGIT -DIGIT DONE		
	Note: If the INE is fronting this particular manager (i.e., the manager		
	interface is via the TACLANE's PT interface), then do not set the RMT		
	CT and PT IP addresses.		
11.	Use the arrow keys to navigate to a particular digit of the IP address. Use		
	the +DIGIT and –DIGIT function keys to increment or decrement each		
	digit. Leave leading zeros. For example, an IP address of 148.20.152.87		
	1s entered as "148.020.152.087."		

Procedure (continued)

Step	Action		
12.	Select DONE when finished.		
13.	Select YES to confirm the information.		
14.	To configure the network manager IP address , select MANAGER ADDR.		
	Result: The following screen is displayed:		
	MANAGER IP ADDRESS		
	MGR ADDR: 148.010.127.055		
	SELECT ACTION:		
	+DIGIT -DIGIT DONE		
15.	Use the arrow keys to navigate to a particular digit of the IP address. Use the +DIGIT and –DIGIT function keys to increment or decrement each digit. Leave leading zeros. For example, an IP address of 148.10.127.55 is entered as "148.010.127.055."		
16.	Select DONE when finished.		
17.	Select YES to confirm the information.		
18.	To configure the network manager KMIDs, select KMID.		
	Result: The following screen is displayed:		
	KMID		
	KMID 1: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
	SELECT ACTION:		
	+DIGIT -DIGIT DONE		
	<u>Note</u> : If the TACLANE is fronting this particular manager (i.e., the manager interface is via the TACLANE's PT interface), then the KMID values should be left blank.		

Procedure (continued)

Step	Action
19.	Use the arrow keys to navigate to a particular digit of the KMID. Use the +DIGIT and –DIGIT function keys to increment or decrement each digit. Leave leading zeros. For example, an KMID of 123456 is entered as "00000000123456."
20.	Select DONE when finished.
21.	Select YES to confirm the information.
22.	To save the network manager configuration, select SAVE.
23.	Select YES to confirm the information, and select YES to restart the TACLANE and return to the OFFLINE MAIN MENU.

8.8 (U) Displaying Network Manager Information

Introduction	(U//FOU	O) The operator can display the configured network manager information.
Note	(U//FOU with a se	O) The TACLANE must be in either the Secure Communications or Offline curity level selected state.
Procedure	(U//FOU	O) Follow these steps to display the network management information:
	Step	Action
	1.	From the MAIN MENU, select DISPLAY.
	2.	From the DISPLAY INFORMATION menu, select NETWORK MGR.
		Result: The following screen is displayed:
		DISPLAY MANAGEMENT INFO-
		(ACTIVE: PRIMARY)
		PRIMARY
		KMID 1: 00000002123456
		KMID 2: 00000002123457
		MGR ADDR: 155.095.124.011
		<down for="" more=""></down>
		MGMT I/F: CT
		RMT CI: 010.125.110.001
		BACKUP
		KMTD 1: 00000004123456
		KMID 2: 00000004123457
		MGR ADDR: 155.095.125.011
		<down for="" more=""></down>
		MGMT I/F: CT
		RMT CT: 010.125.118.002
		RMT PT: 010.125.137.002
		SELECT ACTION:
		Note: Specific values depend on the particular configuration.
	3.	Select DONE to return to the DISPLAY INFORMATION menu.

8.9 (U) Deleting the Network Manager

Introduction	(U//FOU	(U//FOUO) The operator can delete the network manager configuration information.		
Notes	(U//FOU • The ' • Only	O) The following notes apply to deleting the network manager: TACLANE must be Offline with a security level selected state the SSO can perform this function		
Procedure	(U//FOU	O) Follow these steps to delete the network manager:		
	Step	Action		
	1.	From the OFFLINE MAIN MENU, select CONFIG.		
	2.	From the CONFIGURATION menu, select SECURITY.		
	3.	From the CONFIGURE SECURITY menu, select NETWORK MGR.		
	4.	Select DELETE.		
		Result: The following screen is displayed:		
		DELETE NETWORK MGR		
		PRIMARY >BACKUP BOTH		
		SELECT ACTION:		
		SELECT DONE M_MENU		

(U) Deleting the Network Manager, continued

Procedure (continued)

Step	Action	
5.	Select the desired Network Manager to delete (Primary, Backup, or Both).	
	Result: The following screen is displayed (assumes Backup was selected):	
	DELETE NETWORK MGR	
	BACKUP	
	KMID 1: >00000002123456	
	KMID 2: 00000002123457	
	MGR ADDR: 155.095.125.011	
	MGMT I/F: CT	
	<down for="" more=""></down>	
	RMT CT: 010.125.118.001	
	RMT PT: 010.125.118.001	
	DELETE INFORMATION?:	
	YES NO	
	Note: Specific values depend on the particular configuration.	
6.	Select YES to confirm the deletion.	
7.	Select YES to restart the TACLANE and return to the OFFLINE MAIN MENU.	

Chapter 9. (U) Maintaining TACLANE

9.1 (U) Setting the Date and Time

Introduction	(U//FOUO) The operator can set the TACLANE date and time.		
Notes	(U//FOU 55 minut	IO) All communicating TACLANEs must have their date and time set within tes of each other to ensure that no communications blackout periods occur.	
	(U//FOU	O) After this command is executed, the TACLANE will restart.	
Clock Drift	(U//FOU date and adjusted	IO) Nominal TACLANE clock drift is maximum 2 min./month. TACLANE time should be checked for accuracy at least once every 6 months and if needed.	
Setting the Date and Time Using GEM	(U//FOU appropri	O) GEM can remotely change the system date and time. See the ate GEM Operator's Manual for more information.	
Procedure (U//FOUO) Follow these steps to set the date and time:		O) Follow these steps to set the date and time:	
	Step	Action	
	1.	From the MAIN MENU, select MAINT.	
	2.	From the MAINTENANCE menu, select DATE/TIME.	
		Result: The following screen is displayed:	
		DATE/TIME (GMT)	
		DATE: 2004/08/16	
		TIME: 08:55:34	
		SELECT ACTION:	
		+DIGIT -DIGIT DONE	
	3.	Use the arrow keys to navigate to a particular digit of the date and time. Use the +DIGIT and –DIGIT function keys to increment or decrement each digit.	

(U) Setting the Date and Time, continued

Procedure (continued)

Step	Action		
4.	Select DONE when finished, and YES to save changes.		
	Result: The following screen is displayed:		
	DATE/TIME (GMT)		
	TACLANE will restart and PPKs may be deleted		
	MODIFY DATE/TIME?		
	YES NO		
	<u>Note</u> : 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.		
5.	Select YES to save changes and restart the TACLANE.		

9.2 (U) Displaying the Date and Time

Introduction	(U//FOU	O) The operator can display the TACLANE date and time.
Procedure	(U//FOU	O) Follow these steps to display the date and time:
	Step	Action
	1.	From the MAIN MENU, select DISPLAY.
	2.	From the DISPLAY menu, select DATE/TIME.
		Result: The following screen is displayed:
		DISPLAY DATE/TIME (GMT)-
		DATE: 2004/08/16 TIME: 08:55:34
		SELECT ACTION:
	3.	Select DONE to return to the DISPLAY INFORMATION menu.

9.3 (U) Displaying CIK Information

Introduction	(U//FOU	O) The operator can display the CIK configuration information.
Procedure	(U//FOU	O) Follow these steps to display the CIK information:
	Step	Action
	1.	From the MAIN MENU, select DISPLAY.
	2.	From the DISPLAY INFORMATION menu, select CIK INFO.
		Result: The following screen is displayed:
		DISPLAY CIK INFO
		CIK 1 of 3: CREATED CIK 2 of 3: CREATED CIK 3 of 3: EMPTY
		SELECT ACTION:
		DONE
	3.	Select DONE to return to the DISPLAY INFORMATION menu.

9.4 (U) Copying a CIK

Introduction (U Us all	J//FOUO) The operator can create up to two user CIKs via the Copy CIK function. ser CIKs have lesser configuration privileges than the SSO CIK does. User CIKs low the TACLANE to be transitioned to Secure Communications mode.
Make a Copy (U op wł tag TA	J//FOUO) A spare blank KSD-1 CIK is included with the TACLANE. The perator must use this spare KSD-1 CIK to create a user CIK copy. The SSO CIK, hich is inserted in the TACLANE when it arrives from the factory, should be gged and kept in a safe place. Only the user CIK is capable of putting the ACLANE in the Secure Communications state.
Important CIK (U Notes TA Fid sta "In the the ge for	J//FOUO) It is recommended that a CIK be inserted or removed only when the ACLANE is powered off (except when creating a user CIK copy or performing a ield Tamper Recovery). Inserting a CIK at the wrong time during TACLANE artup could cause the data on the CIK to become invalid. This would cause an invalid CIK" message to be displayed upon startup. If a user CIK becomes invalid, we SSO CIK can be used to delete the invalid user CIK and create a new copy. If the SSO CIK becomes invalid, a Field Tamper Recovery can be performed to enerate a new SSO CIK (See Section 10.3, "Performing a Field Tamper Recovery," or more information).
(U esj bro	J//FOUO) Use care in turning a CIK (KSD-1) when inserting and removing, specially the first few times a CIK is inserted and removed. Tabs on the CIK may reak if the CIK is forced.
(U pa ou wi un	J//FOUO) The following CIK insertion technique is recommended: insert the CIK artially with the flanges straight up and down until the flanges are up against the utside of the TACLANE. Turn the CIK counterclockwise until the flanges line up ith the slots, then push to insert. While pushing, turn clockwise on quarter turn ntil the CIK is locked.
(U TA	J//FOUO) It is recommended to practice CIK insertion and removal with the ACLANE powered off before actually creating a CIK copy.
(U (or	J//FOUO) If a CIK is inserted, do not remove the CIK during TACLANE startup or restart).
(U aft tec	J//FOUO) Check that KSD-1 devices used as TACLANE CIKs were manufactured fter 1995. KSD-1 devices manufactured before 1995 use slower memory chnology and may not work correctly when used as TACLANE CIKs.
	Continued on next page

Continued on next page

(U) Copying a CIK, continued

4.

Notes (U//FOUO) The following notes apply to copying a CIK: • The TACLANE must not be in a security level to copy a CIK. • Only the SSO or a privileged user (see Section 9.16 "Configuring Delegate Privileges") can access this command • Up to two additional CIKs may be created. • It is not possible to copy the Field Tamper Recovery (FTR) CIK. • Any KSD-1 device that is not an active CIK in the local TACLANE may be reused for a CIK copy. The KSD-1 is erased as part of the CIK copy operation. • During CIK copy operations, the operator has one minute to complete each CIK replacement step. If the CIK replacement step is not completed within one minute, the TACLANE restarts automatically. Procedure (U//FOUO) Follow these steps to copy a CIK: Step Action 1. From the OFFLINE MAIN MENU, select CONFIG. 2. From the CONFIGURATION menu, select SECURITY. 3. Select CIK COPY from the CONFIGURE SECURITY menu. <u>Result</u>: The following screen is displayed: -----COPY CIK------CIK: 2 of 3 CIK: 3 of 3 SELECT ITEM:

Note: Only empty CIK slots are displayed.

SELECT | DONE | M MENU

Use the up and down arrow keys to navigate to a particular CIK slot.

(U) Copying a CIK, continued

Procedure (continued)

Step	Action		
5.	Select SELECT.		
	Result: The following screen is displayed:		
	Remove CIK		
	Note: If the CIK copy is not completed within 1 minute, the TACLANE		
	automatically restarts.		
6.	Turn the CIK counter-clockwise to unlock and remove.		
	Result: The following screen is displayed:		
	Insert and turn blank CIK		

(U) Copying a CIK, continued

Procedure (continued)

Step	Action		
7.	Insert a blank CIK and turn clockwise to lock.		
	<u>Result</u> : The following screen is displayed:		
	Generating CIK		
	<u>Result</u> : The following screen is displayed after successful CIK generation:		
	CIK: 2 of 3 CREATED		
	Remove CIK		
8.	Turn the CIK counter-clockwise to unlock and remove.		
	Result: The following screen is displayed:		
	Insert and turn original CIK		
9.	Insert the original CIK and turn clockwise to lock.		
10.	Select DONE to return to the CONFIGURE SECURITY menu.		

9.5 (U) Deleting a CIK

Introduction	(U//FOUO) The operator can delete a User CIK.			
Important CIK Notes	(U//FOUO) It is recommended that a CIK be inserted or removed only when the TACLANE is powered off (except when creating a user CIK copy or performing a Field Tamper Recovery). Inserting a CIK at the wrong time during TACLANE startup could cause the data on the CIK to become invalid. This would cause an "Invalid CIK" message to be displayed upon startup. If a user CIK becomes invalid, the SSO CIK can be used to delete the invalid user CIK and create a new copy. If the SSO CIK becomes invalid, a Field Tamper Recovery can be performed to generate a new SSO CIK (See Section 10.3, "Performing a Field Tamper Recovery," for more information).			
	(U//FOUO) Use care in turning a CIK (KSD-1) when inserting and removing, especially the first few times a CIK is inserted and removed. Tabs on the CIK may break if the CIK is forced.			
	(U//FOUO) The following CIK insertion technique is recommended: insert the CIK partially with the flanges straight up and down until the flanges are up against the outside of the TACLANE. Turn the CIK counterclockwise until the flanges line up with the slots, then push to insert. While pushing, turn clockwise on quarter turn until the CIK is locked.			
	(U//FOUO) If a CIK is inserted, do not remove the CIK during TACLANE startup (or restart).			
	(U//FOUO) Check that KSD-1 devices used as TACLANE CIKs were manufactured after 1995. KSD-1 devices manufactured before 1995 use slower memory technology and may not work correctly when used as TACLANE CIKs.			
Notes	 (U//FOUO) The following notes apply to deleting a CIK: The TACLANE must <u>not</u> be in a security level to copy a CIK. Only the SSO or a privileged user (see Section 9.16 "Configuring Delegate Privileges") can access this command. A CIK may not delete itself. The SSO CIK cannot be deleted. The Field Tamper Recovery (FTR) CIK cannot be deleted. 			

(U) Deleting a CIK, continued

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

Step	Action		
1.	From the OFFLINE MAIN MENU, select CONFIG.		
2.	From the CONFIGURATION menu, select SECURITY.		
3.	Select CIK DELETE from the CONFIGURE SECURITY menu.		
	Result: The following screen is displayed:		
	DELETE CIK		
	CIK 2 of 3 CIK 3 of 3		
	SELECT ITEM:		
	SELECT DONE M_MENU		
	Note: Only created CIK slots are displayed. CIK #1 (SSO CIK) is not displayed since it cannot be deleted.		
4.	Use the up and down arrow keys to navigate to a particular CIK slot.		
5.	Select SELECT.		
	<u>Result</u> : The following screen is displayed:		
	DELETE CIK		
	CIK: 2 of 3		
	DELETE CIK SLOT?		
	YES NO		
6.	Select YES to delete the CIK.		
7.	Select DONE to return to the CONFIGURE SECURITY menu.		

9.6 (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. TACLANE will automatically recover to the state it was in before the restart.		
Note	(U//FOU recover.	O) All secure IP paths are lost on a restart. Secure IP paths will auto-	
Procedure	(U//FOU	O) Follow these steps to restart the TACLANE:	
	Step	Action	
	1.	From the MAIN MENU, select OPERATION.	
	2.	From the OPERATIONS menu, select RESTART.	
		Result: The following screen is displayed:	
		TACLANE RESTART	
		All calls will be lost	
		PERFORM RESTART?	
		YES NO	
	3.	Select YES to perform the restart.	

9.7 (U) Shutting Down the TACLANE

Introduction	(U//FOUO) The operator can gracefully shutdown the TACLANE. These steps are optional, as the operator can simply turn off the TACLANE using the power switch.		
Important CIK Note	(U//FOUO) Use care in turning a CIK (KSD-1) when inserting and removing, especially the first few times a CIK is inserted and removed. Tabs on the CIK may break if the CIK is forced.		
Notes	(U//FOUO) Only the SSO or a privileged user (see Section 9.16 "Configuring Delegate Privileges") can access this command.		
	(U//FOU	O) All secure IP paths are lost on a shutdown.	
Procedure	(U//FOU TACLA) between preserve level is e	O) Shutting down the TACLANE via this command will cause the NE to exit the security level (if it is in one). Note that this is one difference powering off the TACLANE unit (where previous security level is d) vs. issuing the TACLANE Shutdown command (where previous security exited).	
Procedure	(U//FOL	O) Follow these steps to gracefully shutdown the TACLANE:	
	Step	Action	
	1.	From the OPERATIONS menu select SHUTDOWN	
	2.	Result: The following screen is displayed:	
		TACLANE SHUTDOWN	
		All calls	
		WIII DE IOSC	
		PERFORM SHUTDOWN?	
		YES NO	
(U) Shutting Down the TACLANE, continued

Procedure (continued)

Step	Action		
3.	Select YES to perform the shutdown.		
	<u>Result</u> : When the shutdown is complete, the following screen is displayed:		
	TACLANE **Shutdown Complete**		
	It is now safe to turn off TACLANE		
	Note: If the TACLANE restarts rather than shutting down, repeat the procedure and verify that the TACLANE shuts down or simply turn the TACLANE OFF.		
4.	Turn the TACLANE OFF.		
5.	Turn the CIK counter-clockwise to unlock and remove.		

9.8 (U) Displaying Version Information

Introduction (U//FOUO) The operator can display version information for TACLANE software components. The "Release" number by itself uniquely specifies a combination of hardware and software.

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

Step	Action		
1.	From the MAIN MENU, select DISPLAY.		
2.	From the DISPLAY INFORMATION menu, select VERSION.		
	Result: The following screen is displayed:		
	DISPLAY VERSION INFO		
	PLATFORM: E100 RELEASE: r3.0v1 CC KRL: 40.256 CC SW: 50.128 SELECT ACTION:		
	DONE M_MENU		
	Note: Specific values depend on the particular TACLANE version.		
3.	Select DONE to return to the DISPLAY INFORMATION menu.		

9.9 (U) Displaying Battery Installed Date

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

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

Step	Action		
1.	From the MAIN MENU, select DISPLAY.		
2.	From the DISPLAY INFORMATION menu, select BATTERY.		
	Result: The following screen is displayed:		
	DISPLAY BATTERY		
	INSTALLED: 2004/04/25		
	SELECT ACTION: DONE M_MENU		
3.	Select DONE to return to the DISPLAY INFORMATION menu.		

9.10 (U) Performing a Field Software Upgrade

Introduction	(U//FOUO) The operator can perform a Field Software Upgrade (FSU) via a serial download to load a new software release into the TACLANE. Field Software Upgrade cannot be used to upgrade the software in TACLANEs running software versions prior to R2.0E. Those units need to be upgraded by depot personnel to a release that supports Field Software Upgrade in order for future upgrades to be done in the field.		
Important Notes	 (U//FOUO) The following notes apply to performing a Field Software Upgrade: A stable power environment must be maintained throughout the procedure. Use of an uninterruptible power supply (UPS) is recommended. The TACLANE must be offline with no security level selected and the SSO CIK inserted. Loading a new version of TACLANE software will overwrite the old version, erase the configuration, and zeroize all keying material. 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 be a previous major release. Also, major releases must be upgraded consecutively; the operator cannot skip over a major release. The operator can upgrade between minor releases that are part of the same major release. General Dynamics will determine what is a major and what is a minor TACLANE software release.		
	(U//FOUO) TACLANE-E100 Release 3.0v2 is a major release. If a Release 3.0v1 unit is upgraded to Release 3.0v2, it cannot revert to Release 3.0v1 via a software upgrade.		
	(U//FOUO) TACLANE-E100 Release 3.0v1 can be directly upgraded to TACLANE-E100 Release 3.0v2.		
	(U//FOUO) TACLANE-E100 Release 2.0 and Release 2.1.1 can both be directly upgraded to TACLANE-E100 Rel 3.0v1.		
	(U//FOUO) <u>Note</u> : Image decryption will fail for a release that is not permitted as an upgrade to a currently installed TACLANE software release.		

	-		
Requirements	(U//FOU followin	O) Before beginning a Field Software Upgrade, make sure that you have the g:	
	 Uncl Zmo 9-pin Upga Auth 	assified PC (or notebook) dem file transfer software (e.g., HyperTerminal) n serial cable rade CD norization code (printed on CD jewel case)	
Zmodem file	(U//FOU session u preference	O) HyperTerminal can be configured with a connection description for a using the serial port (e.g., COM1). Whatever your terminal software ce, here are the parameters for the connection:	
transter software settings	 Baud rate: 115200 Data bits: 8 Parity: None Stop bits: 1 Flow control: Hardware 		
Tip (U//FOUO) If an error occurs during the procedure, such as a tamper cond continuous alarm state, Field Tamper Recovery may be used to reset the us generate a new SSO CIK. See Section 13.3, "Performing a Field Tamper I for instructions. Then return to this section and retry the Field Software U		O) If an error occurs during the procedure, such as a tamper condition or us alarm state, Field Tamper Recovery may be used to reset the unit and a new SSO CIK. See Section 13.3, "Performing a Field Tamper Recovery" actions. Then return to this section and retry the Field Software Upgrade.	
Procedure	(U//FOU	O) Follow these steps to perform a Field Software Upgrade:	
	Step	Action	
	1.	From the OFFLINE MAIN MENU, select MAINT.	
	2.	From the MAINTENANCE menu, select SW UPGRADE.	
		<u>Note</u> : If the SW UPGRADE option is not present, then the SSO CIK is not inserted. Shut down the TACLANE, replace the CIK with the SSO CIK, turn on the TL, and return to Step 1.	

(U) Performing a Field Software Upgrade, continued

Procedure (continued)

Step	Action
3.	The TACLANE will display the current software version information.
	<u>Result</u> : The following screen is displayed:
	FIELD SOFTWARE UPGRADE
	CURRENT VERSIONS:
	PLATFORM: E100
	RELEASE: r3.0v1
	CC RKL: 40.236 CC SW: 50.128
	PERFORM UPGRADE?
	YES NO
	<u>Note</u> : Specific version information depends on the particular TACLANE configuration.
4.	Select YES.
	Note: Selecting NO will abort the Field Software Upgrade and return to
	the MAINTENANCE menu.
5.	The TACLANE will restart.
	Result: After the diagnostic messages, the following screens are displayed:
	FIELD SOFTWARE UPGRADE
	Preparing for
	Field Software Upgrade Standby
	FIELD SOFTWARE UPGRADE
	Connect serial cable
	and
	initiate
	upgrade file download
6.	Connect the serial cable and send the new version of TACLANE software.
	The download will take less than 2 minutes.
1	

Procedure (continued)

Step	Action		
7.	After the download is complete, the TACLANE will prompt the operator		
	to enter the authorization code.		
	Result: The following screen is displayed:		
	FIELD SOFTWARE UPGRADE		
	ENTER AUTH CODE: 0000000		
	SELECT ACTION:		
	+DIGIT -DIGIT DONE		
	<u>Note</u> : There is no limit on the number of attempts to enter this code correctly, but the screen will timeout after 24 hours.		
Step	Action		
8.	Use the arrow keys to navigate to a particular hexadecimal digit of the authorization code. Use the +DIGIT and –DIGIT function keys to increment or decrement each digit.		
9.	Select DONE when finished.		
	<u>Result</u> : The following screen is displayed:		
	FIELD SOFTWARE UPGRADE		
	ENTER AUTH CODE: xxxxxxx		
	CONFIRM AUTH CODE?		
	ABORT YES NO		
	Select YES to confirm the authorization code.		
	<u>Note</u> : Selecting NO (or entering an invalid authorization code) will return the operator to the previous screen. Selecting ABORT will abort the Field Software Upgrade by restarting the unit and returning to the OFFLINE MAIN MENU.		

Procedure (continued)

Step	Action			
10.	The TACLANE will display the new software version information.			
	Result: The following screen is displayed:			
	FIELD SOFTWARE UPGRADE UPGRADE VERSIONS:			
	PLATFORM: E100			
	RELEASE: r3.0v1			
	CC KRL: 40.256			
	CC SW: 50.128			
	PERFORM UPGRADE?			
	YES NO			
	<u>Note</u> : Specific version information depends on the particular TACLANE configuration. Confirm that these correspond to the new TACLANE software release to which you want to upgrade.			
11.	Select YES.			
	<u>Note</u> : Selecting NO will abort the Field Software Upgrade by restarting the unit and returning to the OFFLINE MAIN MENU.			

Procedure (continued)

Step	Action		
12.	The TACLANE will decrypt the new software image.		
	<u>Result</u> : The following screen is displayed:		
	FIELD SOFTWARE UPGRADE		
	Upgrade In Progress		
	Do Not Remove Power or CIK		
	Decrypting Image		
	Note: Decryption of the image takes less than 2 minutes.		
13.	If image decryption is successful, the TACLANE will prompt the operator for final confirmation.		
	Result: The following screen is displayed:		
	FIELD SOFTWARE UPGRADE		
	Ready to install images		
	WARNING: Continuing will		
	Zeroize all Key Material		
	CONTINUE UPGRADE?		
	Note: Selecting NO will abort the Field Software Upgrade by restarting the		
	unit and returning to the OFFLINE MAIN MENU. This is the last		
	chance to abort the Field Software Upgrade. Continuing will zeroize		
	all key material and overwrite the current version of TACLANE		
	software.		

Procedure (continued)

Step	Action
14.	Select YES.
	Result: The following screens are displayed:
	FIELD SOFTWARE UPGRADE
	Upgrade In Progress
	Do Not Remove Power
	or CIK
	Unamedina CC Kernel
	FIELD SOFTWARE UPGRADE
	Upgrade In Progress
	Do Not Remove Power
	or CIK
	Upgrading CC Software
	FIELD SOFTWARE UPGRADE
	opgrade in Progress
	Do Not Remove Power
	or CIK
	Upgrading TL Application
	FIELD SOFIWARE OPGRADE
	Upgrade Complete
	IACLANE WIII restart
	PRESS ANY KEY TO CONTINUE:
	Note: Installing the images takes less then 2 minutes
	<u>Note</u> . Instanting the images takes less than 5 minutes.

Procedure (continued)

Step	Action
15.	Press any key and the TACLANE will restart and come up to the OFFLINE MAIN MENU and running the new software version.
16.	At this point, the TACLANE is reset to factory defaults (See Appendix A, "Factory Default Settings and Port Numbers"). The configuration needs to be restored and key material needs to be filled.

9.11 (U) Zeroizing the TACLANE

Introduction	(U//FOU which de particula zeroize, (for mor (U//FOU operator zeroize b	 JO) The TACLANE supports three types of zeroization: 1) Panic zeroize, eletes all keys in the TACLANE, 2) Selective zeroize, which deletes a ar key (for details, see Sections 4.7 and 4.8 of this document), and 3) Tamper which is the result of a tamper condition of the unit and all keys are deleted e tamper details, see Section 10.2). JO) This section describes how the operator can invoke a panic zeroize. An can initiate a panic zeroize either by depressing the TACLANE front panel puttons or by issuing the Zeroize command from the HMI. 		
Notes	 (U//FOUO) The following notes apply to panic zeroizing the TACLANE: A panic zeroize deletes all keys. TACLANE may be filled with key 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 any key 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 both ZEROIZE buttons simultaneously. They must be held down for 5 seconds.		
		<u>Note</u> : This initiates a panic zeroize whether TACLANE is powered ON or OFF.		
	2.	To initiate a panic zeroize from the HMI display , select OPERATION from the MAIN MENU.		
	3.	From the OPERATIONS menu, select ZEROIZE.		
		Result: The following screen is displayed:		
		TACLANE ZEROIZE		
		All keying material will be zeroized		
		PERFORM ZEROIZATION?		
		YES NO		
	4.	Select YES to zeroize and restart the TACLANE.		
		<u>Note</u> : When the TACLANE starts up, acknowledge the message display indicating "TACLANE zeroized. Press any key to continue."		

9-24 UNCLASSIFIED//FOUO

9.12 (U) Configuring the System Name

Introduction	(U//FOU system n (U//FOU identify t	 D) The operator can configure a system name for the TACLANE unit. The me can be up to 20 characters. D) A user-defined system name allows a remote manager to more easily are managed TACLANES. 		
Notes	(U//FOU character I I S (U//FOU default v	 DUO) The 20-character system name can consist of the following types of ters: Letters: A – Z (upper case only) Numbers: 0 – 9 Symbols: "@", "#", "*", "(", ")", "-", "_", "+", ".", "/", " " (blank space) DUO) It is possible to leave the TACLANE system name blank. This is the t value for the system name. 		
Procedure	(U//FOU	O) Follow these steps to configure the system name:		
	Step	Action		
	1.	From the MAIN MENU, select MAINT.		
	2.	From the MAINTENANCE menu, select SYSTEM NAME.		
		Result: The following screen is displayed:		
		SYSTEM NAME		
		NAME: xxxxxxxxxxxxxxxxxxx		
		SELECT ACTION.		
		+DIGIT -DIGIT DONE		
	3.	Use the arrow keys to navigate to a particular character in the system name. Use the +DIGIT and –DIGIT function keys to increment or decrement each character.		
	4.	Select DONE when finished, and YES to save changes and return to the MAINTENANCE menu.		

9.13 (U) Display System Information

Introduction (U//FOUO) The operator can display the following TACLANE system information which identifies the particular TACLANE unit:
 TACLANE Unique Identifier (ID) – the lower three bytes (displayed as six hex characters) of the TACLANE CT interface's MAC address
 TACLANE system name – the up to 20-character, user-configurable system name
 Electronic Serial Number (ESN) – a 12-digit hexadecimal number in which

 Electronic Serial Number (ESN) – a 12-digit hexadecimal number in which the first digit represents the serial number, the next four digits represent the manufacturer ID, the next two digits are the equipment type ID, and the last five digits represent the lower 20 bits of the TACLANE's CT interface MAC address.

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

Step	Action
1.	From the MAIN MENU, select DISPLAY.
2.	From the DISPLAY INFORMATION menu, select SYSTEM INFO.
	Result: The following screen is displayed:
	DISPLAY SYSTEM INFO
	ID: XXXXXX NAME: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	SELECT ACTION:
	DONE M_MENU
3.	Select DONE to return to the DISPLAY menu.

9.14 (U) Configuring Backward Compatibility Mode

Introduction	(U//FOUO) The SSO operator can configure a Rel backward compatible with Rel 2.x TACLANE Cla the SSO operator needs to set the Backward Comp (U//FOUO) When configured with Backward Com TACLANE-E100 interoperates with and has been HAIPIS TACLANE Classics and E100s. Furtherm interoperating with earlier versions; however, since interoperating with earlier versions was not tested. Security Features Users Guide for more information (U//FOUO) The Backward Compatibility parar means a Rel 3.0 TACLANE is not compatible w this parameter is updated to ON.		TACLANE-E100 to be E100 units. Specifically, ty parameter to ON. Note: Specifically, ty parameter to ON. Note: Specifically, with the Rel 3.0v2 with the Rel 3.0v2 with the Rel 2.x pre- pere is nothing to preclude it 2.x was a required upgrade, e refer to the TACLANE Comparison of the TACLANE Comparison of the TACLANE Comparison of the	
Backward Compatibility ON vs. OFF	(U//FOUO) The followir backward compatibility i	ng table identifies the differences is ON vs. OFF:	s in the TACLANE when	
	TACLANE feature	Backward Compatibility = ON	Backward Compatibility = OFF	
	SA protocol	IKE and SAMP	IKE	
	IP TFS	Enforced for all SAs (HAIPIS & non-HAIPIS)	Enforced only for HAIPIS SAs	
	PPK format	DS-100-1 and DS-74 PPKs	DS-100-1 PPKs	
	ESP Header	HAIPIS ESP and pre- HAIPIS ESP	HAIPIS ESP	
Receiving a RECIPeWill delete the pre-HAIPISDroppedNokey messageSA identified in the Nokey messageDropped				

Remote Static Routing for Rel 2.x TACLANEs

(U//FOUO) The 3.0 TACLANE supports the HAIPIS Secure Dynamic Discovery (SDD) protocol and no longer supports RECIPe. Consequently, for a 3.0 TACLANE to interoperate with a Rel 2.x TACLANE, the TACLANEs must use static routing since the Rel 2.x TACLANE does not support SDD. The 3.0 TACLANE must also have the Backward Compatibility set to ON in this case.

(U) Configuring Backward Compatibility Mode, continued

SA protocol when Backward Compatibility is ON	(U//FOUO) When Backward Compatibility is ON, the TACLANE will allow the development of both HAIPIS security associations (SAs) using IKE (to other 3.0 TACLANEs) as well as the development of pre-HAIPIS SAs using SAMP (to accommodate Rel 2.x TACLANEs).		
	(U//FOUO) When the Backward Compatibility is set to ON, the source TACLANE first initiates an IKE exchange when trying to establish an SA, then if that fails, a SAMP exchange is attempted. Note that this means that a pair of HAIPIS TACLANEs may develop a pre-HAIPIS SA, if IKE times out for some other reason.		
ESP Header when Backward Compatibility is ON	(U//FOUO) When Backward Compatibility is ON and a PPK is used, the ESP header format is derived from the type of PPK. If the PPK format is DS-74, the ESP header is marked for "pre-HAIPIS". If pre-HAIPIS PPK SAs are needed, DS-74 PPKs must be filled and assigned. If the PPK format is DS100-1, the ESP header is marked for "HAIPIS".		
	(U//FOUO) When Backward Compatibility is ON and a FIREFLY is used, the ESP header format is derived from the protocol used to establish the SA. If the SAMP protocol was used, the ESP header is marked for "pre-HAIPIS". If the IKE protocol was used, the ESP header is marked for "HAIPIS".		
R2.1E PSEQN not compatible with HAIPIS PSEQN	(U//FOUO) If communicating in Backward Compatibility mode with a Rel 2.1 TACLANE-E100, it is important to note that the Rel 2.1E-style PSEQN processing is not compatible with the TACLANE Rel 3.0 HAIPIS PSEQN processing, so PSEQN is not enforced in this case.		
Notes	(U//FOUO) The following notes apply to configuring the Backward Compatibility mode:		
	 FACLANE must be offline with no security level selected (See "Exiting a Security Level") in order to set this. Only the SSO can access this command The default Backward Compatibility value is set to OFF 		

(U) Configuring Backward Compatibility Mode, continued

Procedure

(U//FOUO) Follow these steps to configure the backward compatibility mode:

Step	Action
1.	From the OFFLINE MAIN MENU, select MAINTENANCE.
2.	From the MAINTENANCE menu, select SEC ADMIN.
	Result: The SECURITY ADMINISTRATOR screen is displayed:
	SECURITY ADMINISTRATOR
	DELEGATE PRIV: OFF >BACKWARD COMP: OFF
	SELECT ACTION:
	CHANGE SAVE DONE
3.	Use the up and down arrows to navigate to the BACKWARD COMP setting.
4.	Select CHANGE to toggle the BACKWARD COMP between ON and OFF.
5.	Select SAVE to save changes and return to the MAINTENANCE menu.
	I

9.15 (U) Display Backward Compatibility

Introduction (U//FOUO) The operator can display the TACLANE's backward compatibility mode. Refer to the previous section for the details on the differences between backward compatibility ON vs. OFF. If backward compatibility is set to OFF, a Rel 3.0 TACLANE-E100 cannot estabilish security associations with Rel 2.x TACLANE Classic or E100 unit.

Procedure (U//FOUO) Follow these steps to display the backward compatibility mode:

Step	Action
1.	From the MAIN MENU, select DISPLAY.
2.	From the DISPLAY INFORMATION menu, select BACK COMPAT.
	Result: The following screen is displayed:
	DISPLAY BACKWARD COMPAT-
	BACKWARD COMP: OFF
	SELECT ACTION:
	DONE M_MENU
3.	Select DONE to return to the DISPLAY menu.

9.16 (U) Configuring Delegate Privileges

Introduction	(U//FOUO) The SSO has the ability to grant non-SSO operators the privilege to access certain configuration screens, which are otherwise restricted for the non-SSO operator. The TACLANE HMI consists of certain commands that are 'SSO delegatable' and these are only available to a non-SSO operator if the delegate privileges mode is configured to ON.		
Categories of TACLANE HMI commands	 (U//FOUO) The TACLANE HMI commands can be broken into four sets of varied access control, based on the operator's role: SSO-only commands – those to which only the SSO can access SSO-delegatable commands – those that a non-SSO operator can access only when the Delegate Privileges setting is ON (note: the SSO can also gain access to these commands) Non-privileged commands – those to which any operator (SSO and non-SSO) can gain access (i.e., regardless of the Delegate Privileges setting) Non-SSO commands – those that the non-SSO can access, but the SSO cannot access (There is currently only one command in this category: Secure Comm. The TACLANE will only go into secure communications and pass traffic if a user CIK, and not the SSO CIK, is inserted.) 		
	(U//FOUO) Refer to the HMI menu tree (in Section 3.8) to see the set of HMI commands and also the notations that indicate which group each command falls in.		
Notes	 (U//FOUO) The following notes apply to configuring the Delegate Privileges mode: TACLANE must be offline with no security level selected (See "Exiting a Security Level") in order to access this command. Only the SSO can access this command. The default Delegate Privileges mode is OFF. The Delegate Privileges mode can only be changed through the SSO operator accessing this Security Administrator HMI command. For example, restarting a TACLANE will not reset the Delegate Privileges mode. All valid User CIKs receive delegated privileges; it is not on a per-CIK basis. 		

TL-275-06 15 March 2006

UNCLASSIFIED//FOUO

(U) Configuring Delegate Privileges, continued

Procedure

(U//FOUO) Follow these steps to configure the delegate privileges mode:

Step	Action
1.	From the OFFLINE MAIN MENU, select MAINTENANCE.
2.	From the MAINTENANCE menu, select SEC ADMIN.
	Result: The SECURITY ADMINISTRATOR screen is displayed:
	SECURITY ADMINISTRATOR
	>DELEGATE PRIV: OFF BACKWARD COMP: OFF
	SELECT ACTION:
	CHANGE SAVE DONE
3.	Use the up and down arrows to navigate to the DELEGATE PRIV setting.
4.	Select CHANGE to toggle the DELEGATE PRIV between ON and OFF.
5.	Select SAVE to save changes and return to the MAINTENANCE menu.

Chapter 10. (U) Troubleshooting TACLANE

10.1 (U) Alarm

Introduction	(U//FOUO) An alarm i alarm condition, the Al may be displayed (The on the LCD screen):	s the result of ar LARM status LI nature of the ala	n internal failure. Wi ED is illuminated, an arm may not allow a	hen a TACLANE is in an d the following screen nything to be displayed
		*****ALARM	DETECTED*****	
		ALARM CODE: FUNCTION:	xxxxxxxx xxxxxxxxxx	
		LINE #:	XXXXXXXX	
		PARAM 1:	XXXXXXXX	
		PARAM 2:	XXXXXXXX	
		PARAM 3:	XXXXXXXX	
		PARAM 4:	XXXXXXXX]
	<u>Note</u> : Specific alarm in <u>Note</u> : The ALARM sta normal.	formation is dis itus LED is illun	played in the spaces ninated briefly during	denoted by "x"s. g diagnostics. This is
Alarm Recovery	(U//FOUO) TACLANI TACLANE automatica previous operating mod the above screen and the cycled by the operator condition persists, the ' note of the alarm inform personnel.	E automatically illy resets during de. After severa ten halt (i.e., it v to attempt to rec TACLANE shou mation displayed	attempts to recover f g alarm recovery and l repeated alarms, th vill stop attempting t cover from a repeated and be returned to the d as this information	From an alarm. attempts to return to the e TACLANE will display o restart). Power can be d alarm condition. If the e depot for repair. Make a may be useful to depot

TL-275-06 15 March 2006	UNCLASSIFIED//FOUO	Operator's Manual Revision 1.4
10.2 (U)	Famper	
Introduction	(U//FOUO) Tamper is the result of opening the TACLANE chassi power when powered off, or removal of the battery while the TAC off. When a TACLANE is in a tamper condition, the ALARM sta illuminated. If a CIK is not inserted, the following screen is displa	is, loss of battery CLANE is powered atus LED is ayed:
	TAMPER DETECTED **TACLANE** **Zeroized and Locked**	
	(U//FOUO) If a CIK is inserted into a tampered TACLANE, the f displayed: Depot Tamper Recovery In Progress	following screen is
Tamper Recovery	<u>Note</u> : All keys are automatically deleted when a tamper condition (U//FOUO) A tampered unit can be recovered in the field. See Se "Performing a Field Tamper Recovery." for more information.	is detected.

10.3 (U) Performing a Field Tamper Recovery

Introduction	(U//FOUO) The operator can perform a Field Tamper Recovery (FTR) using a FTR CIK to recover a TACLANE that has become tampered. FTR can also be used to fix an invalid SSO CIK and 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 lithium 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 SSO CIK	(U//FOUO) References to "SSO CIK" in this procedure refer to the Master CIK (CIK #1) for the TACLANE. Obtain a CIK (can be current SSO CIK or a User CIK) before beginning this procedure. This CIK will become the new SSO CIK for the TACLANE. Do not use a CIK that is required for another TACLANE.		
Field Tamper Recovery CIK	(U//FOUO) A Field Tamper Recovery CIK is unique to the TACLANE labeled with the corresponding serial number. It can be used to recover its associated TACLANE from tamper a maximum of ten times. Once it has been used ten times, a FTR CIK is no longer valid. The tag attached to the FTR CIK should be used to keep a record of each tamper recovery. The FTR CIK is classified SECRET, and must be handled according to NSA doctrine.		
Battery Replacement	(U//FOUO) The most likely cause of a benign tamper is due to a depleted battery. Whether or not this is the case, it is recommended that the battery be replaced.		
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").	
		<u>Note</u> : 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.	

(U) Performing a Field Tamper Recovery, continued

Procedure (continued)

Step	Action		
4.	Turn on the TACLANE.		
	Result: The following screen is displayed:		

	TAMPER DETECTED		
	TACLANE		
	Zeroized and Locked		
5.	Insert the Field Tamper Recovery CIK.		
	<u>Result</u> : The following screen is displayed:		
	TAMPER RECOVERY		
	Field Tamper Recovery		
	In Progress		
	Do Not Remove FTR CIK		
	Note: If the HMI displays "Invalid CIK. Remove CIK," then either an		
	times If the FTR CIK has been used ten times the TACI ANE must be		
	returned to the depot.		
6.	When prompted, remove the FTR CIK.		
7.	When the HMI displays "Insert New SSO CIK," insert a CIK. This can be		
	the current SSO CIK or a User CIK for the TL. The CIK inserted at this		
	point will become the new SSO CIK for this TACLANE. Do not use a		
	CIK that is required for another TACLANE.		
	If the HMI displays "Error writing to SSO CIK. Remove CIK," the CIK is damaged Remove the CIK and replace it with another		
8	The FTR CIK tag contains ten numbered lines for recording tamper		
0.	recoveries. At this time, initial and date the first available line, indicating		
	that a Field Tamper Recovery has been performed.		

(U) Performing a Field Tamper Recovery, continued

Procedure (continued)

Step	Action			
9.	The TACLANE indicates that Field Tamper Recovery is complete and displays the FTR count.			
	Result: The following screen is displayed:			
	TAMPER RECOVERY			
	Field Tamper Recovery			
	Complete			
	Counter: xx			
	TACLANE WIII restart			
	Reset Date and Time			
	PRESS ANI REI IO CONTINUE:			
	<u>Note</u> : The number of times that FTR has been performed on this TACLANE (ten maximum) is displayed in the space denoted by "x"s. This number should match the number of the line on the FTR CIK tag that was used in the previous step.			
10.	Press any key to continue. The TACLANE will restart and return to the OFFLINE MAIN MENU.			
11.	Reset the date and time (See Section 19.1, "Setting the Date and Time").			
12.	Update the battery installed date (See Section 10.5, "Replacing the Battery," for instructions).			
13.	At this point, the TACLANE is reset to factory defaults (See Appendix A, "Factory Default Settings and Port Numbers"). 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 is low at any time during TACLANE operation, the BATTERY LOW status LED on the front panel is illuminated. In addition, the battery is automatically tested periodically and on a startup or restart.		
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:		O) 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.	
<u>Note</u> : The battery low status LED is illuminated briefly d This is normal.		<u>Note</u> : 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 battery has an estimated life of three years. It is recommended to change the battery every 18 months or when the BATTERY LOW status LED is illuminated.			
Important Battery Removal Note	t (U//FOUO) Always remove and replace the battery with the TACLANE remaining powered on. Battery removal with the TACLANE powered off (or powering or the TACLANE after removing the battery) tampers the TACLANE.			
	(U//FOU polarity. be dama	O) It is very important that the new battery be placed in correct If the battery is inserted backwards, there is a risk that the device will ged.		
Lithium Battery	(U//FOUO) TACLANE contains a lithium battery. Do not incinerate lithium batteries because of the risk of explosion.			
Notes	 (U//FOUO) The following notes apply to replacing the battery: The TACLANE must remain powered on during battery replacement to avoid a tamper condition. Replace with a 3.6V AA lithium battery (NSN: 6135-01-301-8776). 			
Procedure (U//FOUO) Follow these steps to replace the battery:				
	Step	Action		
	1.	With the TACLANE powered on, remove the battery cover from the front panel by loosening the two thumbscrews.		
	2.	Pull out the bottom of the battery (positive end) to remove.		
	3. Install a new battery with the positive end down.			
	4. Replace the battery cover and tighten the two thumbscrews.			
	 5. To update the battery installed date, select MAINT from the MAIN MENU. 			

(U) Replacing the Battery, continued

Procedure (continued)

Step	Action			
6.	From the MAINTENANCE menu, select BATTERY.			
	Result: The following screen is displayed:			
	BATTERY			
	BATTERY REPLACED?			
	YES NO			
7.	Select YES to acknowledge battery replacement and return to the			
	MAINTENANCE menu.			
	Note: This sets the battery installed date to the current date.			
L				

10.6 (U) Adjusting Display Contrast

Introduction	(U//FOU accomm	(U//FOUO) The operator can adjust the display contrast for the LCD display to accommodate various lighting conditions.		
Note	(U//FOU	(U//FOUO) A small flat-head screwdriver is needed to adjust display contrast.		
Procedure	(U//FOU	IO) Follow these steps to adjust display contrast:		
Step Action				
1. With the TACL panel by loosen screw adjustmen remove the bat		panel by loosening the two thumbscrews. The contrast control is the small screw adjustment located directly below the battery. You do not need to remove the battery.		
	2.	Adjust the display contrast to the desired level by turning the screw adjustment with a small flat-head screwdriver.		
	3. Replace the battery cover and tighten the two thumbscrews.			

10.7 (U) Performing Diagnostics

Introduction (U//FOUO) Diagnostics are automatically performed periodically. The operativity initiate diagnostics by restarting the TACLANE.		
Procedure	(U//FOU	O) Follow this step to initiate diagnostics:
Step Action		Action
	1.	Restart the TACLANE (See Section 9.6, "Restarting the TACLANE").
	Ļ	

10.8 (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	Invalid CIK.	Check that a valid CIK is inserted.
CIK to be inserted.	CIK is older and uses slower memory technology.	Check that KSD-1 devices used as TACLANE CIKs were manufactured after 1995.
	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.
LCD display is hard to read.	LCD display contrast out of adjustment.	Adjust LCD display contrast.
Cannot modify date/time ("Invalid date or time").	Invalid date and/or time entered.	Check that the date/time entered is valid.
Cannot copy CIK ("No CIK slots available").	All three CIK slots are full.	Delete an existing CIK copy (CIK #2 or CIK #3) to make room for a new CIK copy. (CIK#1 cannot be deleted.)
Cannot copy CIK ("Error reading from CIK. Remove CIK").	KSD-1 (CIK) device is bad.	Use another KSD-1 to make the CIK copy.
Cannot copy CIK ("Error writing to CIK. Remove CIK").	KSD-1 (CIK) device is bad.	Use another KSD-1 to make the CIK copy.
Cannot copy CIK ("Inserted CIK already exists, Remove CIK").	The KSD-1 for the copy is a valid CIK on this TACLANE.	Use another KSD-1 to make the CIK copy.
Cannot create ACL entry ("ACL is full").	The ACL is full.	The ACL can hold 256 entries. Delete an existing ACL entry to make room for a new entry.
Cannot create/modify ACL entry ("Duplicated KMID").	The KMID entered appears in another ACL entry.	Check that the KMID entered is unique. A KMID can only appear in one entry in the ACL.
Cannot create/modify ACL entry ("Invalid KMID").	Invalid KMID entered.	Check that the KMID entered is valid.

(U) Troubleshooting General Problems, continued

General Problems (continued)

Problem	Cause	Solution
Cannot modify ACL entry ("ACL is empty").	There are no ACL entries to modify.	
Cannot delete ACL entry ("ACL is empty").	There are no ACL entries to delete.	
Cannot create/modify/delete ACL entry ("Configuration error").	The network manager set the TACLANE online before the ACL operation completed.	Coordinate configuration changes with the network manager, if a network manager is configured.
Cannot configure network manager ("Invalid address").	Invalid IP address entered.	Check that the IP address entered is valid.
Cannot configure network manager ("Configuration error").	The network manager set the TACLANE online before the configuration operation completed.	Coordinate configuration changes with the network manager, if a network manager is configured.
Cannot configure network manager ("KMID and address have to be entered").	Both the KMID and IP address are not entered.	Check that both a KMID and IP address are entered.
Cannot configure network manager ("IP already assigned").	The IP address is duplicated elsewhere in the IP configuration.	Check that the IP address entered is unique.
Cannot configure network manager ("IP address required").	The IP address is not entered.	Enter an IP address for the network manager.
Cannot configure network manager ("TACLANE GWY IP address required").	Network manager IP address is in different IP network, and TACLANE default gateway is not defined.	Define the PT or CT default gateway to communicate with an off-net PT or CT network manager, respectively.
Cannot delete network manager ("Network manager not configured or is unavailable").	There is no network manager to delete.	
Cannot delete network manager ("Configuration error").	The network manager set the TACLANE online before the configuration operation completed.	Coordinate configuration changes with the network manager, if a network manager is configured.
Cannot display management interface information ("Network manager not configured or is unavailable").	No network manager is configured.	

10.9 (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 ("Selected key material already present").	A FIREFLY vector set is already filled.	Delete the existing FIREFLY vector set before filling a new FIREFLY vector set.
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 FIREFLY vector set (Key material not filled due to EFF- only switch)	EFF-only switch is on and Basic vector set is being filled	Turn EFF-only switch off or use EFF-capable vector set.
Cannot display FIREFLY vector set information ("Keying material not present").	No FIREFLY vector set is filled.	
Cannot delete FIREFLY vector set ("Keying material not present").	There is no FIREFLY vector set to delete.	
Cannot exit a security level (Configuration error).	The network manager set the TACLANE online before the operation completed.	Coordinate configuration changes with the network manager, if a network manager is configured.
Cannot fill PPK ("PPK ID already filled").	A PPK is already filled under the PPK ID.	Fill the PPK under a different PPK ID, or delete the existing PPK to make room for a new PPK.
Cannot fill PPK ("PPK table is full").	The maximum number of PPKs has already been filled.	The TACLANE can store up to 48 PPKs (total across all security levels). Delete an existing PPK at this security level (or another security level) to make room for a new PPK.
Cannot fill PPK ("Invalid date").	Invalid effective date entered.	Check that the effective date entered is valid.
Cannot fill PPK ("Invalid PPK ID").	Invalid PPK ID entered.	Check that the PPK ID entered is valid.
Cannot fill changeover PPK ("Invalid associated PPK").	No current PPK is filled under the PPK ID for the changeover PPK.	Check that a current PPK is filled under the PPK ID before filling a changeover PPK under the same PPK ID.

(U) Troubleshooting Filling and Managing Keys, continued

Problems with Filling and Managing Keys (continued)

Problem	Cause	Solution
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.
	The PPK is already filled.	Check that the PPK is not already filled.
Cannot fill PPK (TACLANE resets during transfer).	The DTD was set to "issue" the PPK.	Check that the DTD is configured to "fill" the PPK rather than "issue" it.
Cannot display PPK information ("Keying material not present").	No PPKs are filled.	
Cannot delete PPK ("Keying material not present").	There are no PPKs to delete.	
PPKs deleted after changing date/time.	Changing time ahead may expire and automatically delete PPKs.	Automatically deleted PPKs cannot be recovered and must be re-filled. Check the entered date/time carefully before confirming to ensure the entered date/time is accurate.
Cannot delete PPK ("Error deleting PPK").	PPK was automatically deleted before the delete operation completed.	

10.10 (U) Troubleshooting IP/Ethernet

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

Problem	Cause	Solution
Cannot enter TACLANE IP addresses ("Invalid address").	Invalid IP address.	Check that a valid IP address is entered.
Cannot enter TACLANE IP addresses ("Configuration error").	The network manager set the TACLANE online before the operation could be completed.	Coordinate configuration changes with the network manager, if a network manager is configured.
"Duplicate IP address"	The TACLANE CT IP address and/or PT IP address are in use by another host on the CT or PT network.	Check that the TACLANE CT IP address and PT IP address are unique on the IP network.
Cannot enter IP MTU ("Illegal MTU size").	Illegal MTU size.	Check that the MTU size entered is not greater than 1500 and not less than 28.
Cannot enter subnet mask ("Invalid address").	Subnet mask is invalid.	Check that the subnet mask entered is valid.
Cannot enter subnet mask ("Mask inconsistent with IP address").	Subnet mask is invalid for IP addresses entered.	Check that the subnet mask entered is valid for the IP addresses entered.
Cannot save IP TFS parameters ("Address is not unique").	ICMP Host address is the same as another IP address in the TACLANE's configuration.	Check that the ICMP Host address entered is unique in the TACLANE's configuration (may be the same as the PT network manager address).

(U) Troubleshooting IP/Ethernet, continued

IP/Ethernet Configuration Problems (continued)

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.
TACLANE restarted.	The underlying network is experiencing a failure or is not configured correctly.	Check that the underlying network is configured and operating correctly.
	Certain IP configuration changes require an immediate restart.	
	An alarm condition occurred.	See the chapter on "Maintaining TACLANE."
10.11 (U) Troubleshooting Secure IP Paths

Secure IP Path Problems (U//FOUO) The table below describes TACLANE secure IP path problems, their causes, and solutions. Also, see applicable Release Notes for the TACLANE software version.

Problem	Cause	Solution
Cannot enter secure communications mode	IP configuration incorrect or incomplete.	Check that the IP configuration is complete and correct.
("Configuration error").	Using the SSO CIK.	Must use a User CIK to enter secure communications mode.
Cannot secure IP paths. 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.
	The local and remote TACLANE are at different security levels.	Check that the local and remote TACLANE must be at the same security level.

(U) Troubleshooting Secure IP Paths, continued

Secure IP Path Problems (continued)

Problem	Cause	Solution
Cannot secure IP paths. IP communications fail. (cont'd)	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 re-filled. Check the entered date/time carefully before confirming to ensure the entered date/time is accurate.
	Access Control Mode is ON 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.
	The local or remote KMID is on the Bad Guy List (BGL).	Contact the network manager (out of band) and ask.

(U) Troubleshooting Secure IP Paths, continued

Secure IP Path Problems (continued)

Problem	Cause	Solution
Secure IP paths 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.
Cannot display secure IP paths ("No paths exist").	There are no secure IP paths to display.	
Cannot assign PPK to IP slot ("No PPKs available for assignment").	There are no PPKs available for assignments to IP slots.	Fill a PPK before assigning a PPK to an IP slot.
Cannot assign/modify PPK to IP slot ("Invalid address").	Invalid IP address.	Check that the IP address entered is valid.
Cannot assign/modify PPK to IP slot ("RMT IP address already assigned").	The remote TACLANE IP address is already assigned to another PPK.	Delete a remote TACLANE IP address assignment from one PPK before assigning a remote TACLANE IP address assignment to another PPK.
	The remote host IP address is already assigned to another TACLANE.	
Cannot assign PPK to IP slot ("Exceeded assignment limit").	The maximum number of PPK assignments has already been made.	 The TACLANE supports up to 400 PPK assignments. Each of the following count as one PPK assignment: Remote TACLANE assignment to an IP slot. Remote host assignment to a remote TACLANE. Delete an assignment to make room for a new PPK assignment.
Cannot assign/modify PPK to IP slot ("Invalid PPK").	PPK was automatically deleted before the assign/modify operation completed.	

(U) Troubleshooting Secure IP Paths, continued

Secure IP Path Problems (continued)

Problem	Cause	Solution
Cannot assign/modify PPK to IP slot ("Configuration error").	The network manager set the TACLANE online before the configuration operation completed.	Coordinate configuration changes with the network manager, if a network manager is configured.
Cannot deassign a PPK from an IP slot ("remote hosts are still assigned").	Remote hosts are still assigned to the remote TACLANE.	Deassign all remote hosts from the remote TACLANE before deassigning the remote TACLANE.
Cannot deassign a PPK from an IP slot ("Configuration error").	The network manager set the TACLANE online before the configuration operation completed.	Coordinate configuration changes with the network manager, if a network manager is configured.
Cannot create/modify static route ("Invalid address").	The entered Network ID and/or TACLANE CT IP address are not valid Class A, B, or C IP addresses.	Ensure that the entered Network ID and/or TACLANE CT IP address are valid Class A, B, or C IP addresses.
Cannot create/modify static route ("Mask inconsistent with IP address").	The entered Network Mask is not consistent with the Network ID entered. E.g., the number of bits in the mask does not meet the minimum required for the Network ID Class and/or does not match the apparent number of bits defined in the Network ID.	Check that the Network Mask entered is consistent with the entered Network ID.
Cannot create/modify static route ("Duplicate static route entry").	The new/modified static route entry matches an existing static route entry. (No two static route entries can have the exact same Network ID and Network Mask.)	Check that all entries have a unique combination of Network ID and Network Mask.
Cannot create static route ("Static route table full").	There is no room in the table for the new static route entry.	An existing static route entry must be deleted to make room for a new entry.
Cannot modify/delete static route ("Static routes have not been created")	There are no static route entries to modify or delete because no static route entries exist.	

Appendix A. (U) Factory Default Settings

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

TACLANE-E100
Factory Default
Settings(U//FOUO) The table below identifies the factory default settings for TACLANE-
E100 parameters. The operator may change these parameters.

TACLANE Parameter	Factory Default Setting
IP MTU	1500
PING	ON
MEDIUM	COPPER
E-NET SPEED/DUPLEX	AUTO-SELECT (assumes copper interface)
ENHANCED FIREFLY (EFF)	NEGOTIATE
MTEK UPDATE	DISABLE
FIXED PACKET MODE	ON/FRAGMENT
FIXED PACKET LENGTH	800
PSEQN CHECK	ON
DSCP BYPASS	OFF
DF BIT BYPASS	CLEAR
PMTU BYPASS	OFF
IGMP BYPASS	OFF
ICMP NOTIFICATION	DISABLED
DISCRETIONARY ACCESS CONTROL	OFF
BACKWARD COMPATIBILITY	OFF
DELEGATE PRIVILEGES	OFF

(U) Factory Default Settings and Port Numbers, continued

RECIPe, IKE, ESP, and SAMP Port Numbers

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

Protocol	Port # or Protocol ID	Description
RECIPe	UDP port 3623	RECIPe NoKey is used for recovering/deleting orphan Pre- HAIPIS SAs
IKE	UDP port 500	IKE is used to setup FIREFLY TEKs.
ESP	IP Protocol ID 50	ESP is used to send encrypted IP traffic.
SAMP	TCP port 2643	SAMP is only used to setup pre- HAIPIS SAs (requires Backward Compatibility to be ON).

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 (KG-175).

(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.



UNCLASSIFIED//FOUO

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

B-1 UNCLASSIFIED//FOUO

(U) Example Secure IP Network, continued

Example Secure IP Network (cont'd)	 (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.
Static IP Routes	(U//FOUO) Configure IP routers that are separated by a TACLANE with static IP routes. On CT routers, define static IP routes to PT networks across the TACLANE. On PT routers, define static IP routes to CT networks (and other destination PT networks) across the TACLANE. This is needed since TACLANE does not bypass IP routing protocols.

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

Introduction	(U//FOUO) Listed below are some general TACLANE IP configuration tips.
Optimum PT IP MTU size	(U//FOUO) For optimum performance, PT-side hosts and routers should either configure PT hosts (and the TACLANEs) to support PMTU discovery, or 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 <u>must</u> set their MTU size no greater than the fixed packet length of the TACLANE.
Sequence to Identify the Remote TACLANE	 (U//FOUO) The TACLANE is capable of both static routing and Secure Dynamic Discovery (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: check for specific static route in remote TACLANE static routing table if static route not found, use the default static route, if it is defined 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 perform SDD, then a default static route must <u>not</u> be configured.
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.

(U) 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 subnet mask. 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 subnet mask as 0.0.0. Validation checks on table entries include: Subnet mask must be valid for the network ID. 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 combination of network ID and subnet mask is used to determine the remote TACLANE to which the IP traffic should be sent. GEM can also configure the routing table. One routing table can be generated at the GEM and distributed to all the TACLANEs.
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.

(U) General IP/Ethernet Configuration Tips, continued

Automated Peer TACLANE Discovery	(U//FOUO) TACLANEs support automated peer TACLANE discovery for secure IP paths, through the HAIPIS 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 secure IP paths using FIREFLY TEKs are checked for a match based on the remote TACLANE IP address. If a match is found, the corresponding existing secure IP path (using a FIREFLY TEK) is used to secure the IP traffic.
	(U//FOUO) If there is no matching PPK assignment or secure IP path (using a FIREFLY TEK), and an operational FIREFLY vector set is usable at the current security level, the following occurs:
	• A new secure IP path 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 Secure IP Paths."
	(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.")
PPK Takes Precedence Over FIREFLY	(U//FOUO) For secure IP paths, a PPK assignment takes precedence over generating a FIREFLY TEK.
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.
Autorecovery	(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:
	• Secure IP paths re-establish themselves automatically without operator intervention.
	Continued on next page

B-5 UNCLASSIFIED//FOUO

(U) General IP/Ethernet Configuration Tips, continued

Firewalls must pass IKE, ESP, and optionally RECIPe and SAMP	(U//FOUO) Any firewalls in the path between communicating TACLANEs must be configured to pass IKE, ESP, and RECIPe and SAMP (if backward compatibility is enabled). See Appendix A of this document 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.
Securing	(U//FOUO) TACLANEs support static multicast.
Multicast Traffic	 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 address. Multicast IP datagram traffic is not supported for FIREFLY.
ICMP Notification Host Message Forwarding	(U//FOUO) TACLANE can be configured to support a PT side ICMP Notification Host. The TACLANE will attempt to notify this host via SNMP trap messages when an ICMP Source Quench or Destination Unreachable message is received from the CT network.
	(U//FOUO) This feature is disabled by default. To disable after using the feature, set the ICMP Notification Host IP address to 0.0.0.0.
	(U//FOUO) The ICMP Notification Host can be the same as the PT Network Manager IP address.

(U) General IP/Ethernet Configuration Tips, continued

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 <u>not</u> configured, TACLANE will ARP for all off-net destination IP addresses for decrypted PT IP traffic. Note that this 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 <u>not</u> configured, TACLANE will ARP for all off-net destination IP addresses for encrypted CT IP traffic. Note that this 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.
PMTU Bypass and DF Bit Bypass and FPL	 (U//FOUO) The TACLANE PMTU Bypass support is independent of the DF Bit Bypass support, however, only certain combinations are practical. The DF bit must be bypassed (i.e., the DF Bit Bypass set to "SET") in order for full PT host PMTU discovery support. In PMTU Discovery, a host would set the DF bit to "don't fragment" in order to learn the MTU size of the path. A packet set to "don't fragment" that is too large for the network element is dropped and a Destination Unreachable message is sent to the originator, telling what the MTU size is. Then the originator adjusts its MTU size accordingly and has optimum performance. Only if the host sets the DF bit to "don't fragment" does the host get feedback about the maximum MTU size of the path. If PMTU Bypass is set to OFF, the DF Bit Bypass should always be set to "may fragment" (i.e., the DF Bit Bypass set to "CLEAR" or "COPY"). The only reason to set the DF Bit Bypass to "don't fragment" (i.e., "SET") is to gain knowledge of the path MTU size so that the host may adjust its MTU size. When PMTU Bypass is ON, the DF Bit Bypass should always be set to "COPY". PMTU discovery is dynamic and the MTU associated with a given SA may change at any time during communications. After a period of time, the TACLANE increases the MTU to the maximum MTU size. This allows for cases where the PMTU was lowered due to a temporary link failure that has since been corrected. The PMTU discovery mechanisms in the network continue to adjust the MTU as needed. If FPL is enabled, PMTU should be disabled (OFF) so that the MTU of the host can be set to the most efficient length based on the FPL.

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) <u>Note</u>: 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



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

- <u>User does not control the CT network</u>: E.g., the administrators of Router C may not allow the configuration of Router C to be changed.
- <u>User networks are not routable over the CT network</u>: 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.
- <u>The number of user networks is large</u>: The number of user networks makes configuration of static IP routes on Router C cumbersome (e.g., Router B fronts the Internet).

(U) 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) <u>Note</u> : 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.
	Continued on next page

page

(U) IP Routing Workarounds, continued

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



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	
	Router A Enet. CT PT Enet. PT CT IP Enet. Router B	
	UNCLASSIFIED//FOUO	

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

(U) Connecting Networks Using a Different IP Encryptor, continued

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.)





(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.

(U) Connecting Networks Using a Different IP Encryptor, continued

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.

ΤI	L-275-06	5
15	March	2006

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) <u>Note</u> : 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) <u>Note</u> : 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 it's 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) Connecting Networks at Different Security Levels, continued



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.

(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) <u>Note</u> : TACLANE nesting has been tested in configurations of up to 3 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 it's 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
	Nested TACLANES. Router A D B CT PT TACLANE B

UNCLASSIFIED//FOUO

Enet.

(Unclas.)

Enet.

Enet

Host

B1

(Unclas.)

TACLANE

Е

C

P

Enet.

Host

E1

(Top Sec.)

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

Enet.

(Secret)

CT

TACLANE

А

Host

C1

(Unclas.)

Enet.

Enet.

Host

A1

(Top Sec.)

Enet

PT

CT

CT

TACLANE

в

TACLANE

С

Enet.

Enet.

(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) <u>Note</u>: 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

(U) Multiple Gateways from Network, continued

Introduction (continued)	(U//FOUO) Each TACLANE in this configuration has two possible CT Default Gateways for sending off-net CT datagrams to. 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) <u>Note</u> : 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.

(U) Multiple Gateways from Network, continued

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

- 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



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 24bit 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.

TL-275-06 15 March 2006

(U) Multiple Gateways from Network, continued

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



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.

(U) Multiple Gateways from Network, continued

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

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) <u>Note</u> : Each of the redundancy configurations described in this section can be implemented with any combination of TACLANE Classic models, regardless of whether the TLs are configured for static routing. Either Preplaced Key (PPK) or FIREFLY vector sets may be used.
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 PPK 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 (U//FOUO) The figure below is a two-enclave illustration of a base network where Redundancy TACLANE redundancy is configured only at a gateway enclave, in this case a with Router gateway to the global SIPRNET. Up to 253 SIPRNET enclaves on the base network, Redundancy 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 SIPRNET SIPRNE Router LAN Switch GRE Tunnel 1 (Router A <-> Router B1) ()



UNCLASSIFIED//FOUO



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 a 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



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

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.

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

Partial Device (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) Redundancy Configurations, continued

How it Works (continued)	(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 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.

(U) THIS PAGE INTENTIONALLY LEFT BLANK

Appendix C. (U) Mechanical Drawings for Installation

C.1 (U) Introduction

Purpose (U//FOUO) This appendix provides mounting guidelines for the General Dynamics TACLANE (KG-175). Detailed mechanical drawings showing mounting holes, cable bend radii, and maximum dimensions of the TACLANE enclosure are included. C.2 (U) Mounting Instructions General (U//FOUO) Two TACLANEs can be rack mounted side-by-side in a standard EIA 19 in. rack. The TACLANE has $4 \ 10/32$ in. threaded holes on the bottom cover for mounting to a rack shelf. Spacers must be used to bypass the rubber feet (the rubber feet are not removable). The TACLANE front handles can be removed for rack mounting. An optional rack mount kit (part number 0N649704-1) is available. See Section 3.2 of the Operator's Manual for more information. Mounting (U//FOUO) The recommended mounting pattern for TACLANE is to attach to the Guidelines bottom using four #10-32 screws in a 7.25 x 14.5 in. rectangle. The screws will engage 4 MS124655 (1 diameter long) helical inserts installed per MS33537; the maximum allowable screw protrusion into the enclosure beyond the bottom face is .315 in. The centerlines of the inserts are located within a .014 diameter of true position relative to datums on the left side and front of the enclosure. The TACLANE should be elevated from the mounting surface using standoffs, a minimum of .232 inch in order to clear the mounting feet. The standoffs used must be limited to a maximum outer diameter of .686 inch in order to clear adjacent access cover hardware. Temperature (U//FOUO) TACLANE is passively cooled, i.e., there is no cooling fan. Placement Considerations or mounting must make sure that the TACLANE is operating within its temperature limits for minimum/maximum ambient temperature.

C.3 (U) Mechanical Drawings

About the Drawings

TL-275-06

15 March 2006

(U//FOUO) The following two figures identify the maximum dimensions of the TACLANE enclosure, including clearance for the power and communications cables and connectors. The bottom view of the TACLANE also shows the locations of the $4 \ 10/32$ in. threaded holes for mounting to a rack shelf or isolation tray.



UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO Figure C.3-1 (U) TACLANE Front View

Continued on next page

(U) Mechanical Drawings, continued



Figure C.3-2 (U) TACLANE Bottom View

C-3 UNCLASSIFIED//FOUO

(U) THIS PAGE INTENTIONALLY LEFT BLANK