BlackDoor OPS
User's Guide

Engage Black

August 28, 2023

Engage Black
9565 Soquel Drive, Suite 200
Aptos, California 95003
TEL: 831-688-1021 FAX: 831-688-1421
www.engageblack.com
support@engageinc.com

Product Warranty

Seller warrants to the Original Buyer that any unit shipped to the Original Buyer, under normal and proper use, be free from defects in material and workmanship for a period of 24 months from the date of shipment to the Original Buyer. This warranty will not be extended to items repaired by anyone other than the Seller or its authorized agent. The foregoing warranty is exclusive and in lieu of all other warranties of merchantability, fitness for purpose, or any other type, whether express or implied.

Remedies and Limitation of Liability

A. All claims for breach of the foregoing warranty shall be deemed waived unless notice of such claim is received by Seller during the applicable warranty period and unless the items to be defective are returned to Seller within thirty (30) days after such claim. Failure of Seller to receive written notice of any such claim within the applicable time period shall be deemed an absolute and unconditional waiver by buyer of such claim irrespective of whether the facts giving rise to such a claim shall have been discovered or whether processing, further manufacturing, other use or resale of such items shall have then taken place.

B. Buyer's exclusive remedy, and Seller's total liability, for any and all losses and damages arising out of any cause whatsoever (whether such cause be based in contract, negligence, strict liability, other tort or otherwise) shall in no event exceed the repair price of the work to which such cause arises. In no event shall Seller be liable for incidental, consequential, or punitive damages resulting from any such cause. Seller may, at its sole option, either repair or replace defective goods or work, and shall have no further obligations to Buyer. Return of the defective items to Seller shall be at Buyer's risk and expense.

C. Seller shall not be liable for failure to perform its obligations under the contract if such failure results directly or indirectly from, or is contributed to by any act of God or of Buyer; riot; fire; explosion; accident; flood; sabotage; epidemics; delays in transportation; lack of or inability to obtain raw materials, components, labor, fuel or supplies; governmental laws, regulations or orders; other circumstances beyond Seller's reasonable control, whether similar or dissimilar to the foregoing; or labor trouble, strike, lockout or injunction (whether or not such labor event is within the reasonable control of Seller)

Copyright Notice

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

NOTE - Shielded ethernet cables must be used with the Engage IP■Tube to ensure compliance with FCC Part 15 Class A limits.

CAUTION - To reduce the risk of fire, use only No. 26 AWG or larger listed Telecommunication cables.

Equipment Malfunction

If trouble is experienced with an BlackDoor OPS, please contact the Engage Communication Service Center. If the equipment is causing harm to the telephone network, the telecommunications service provider may request that you disconnect the equipment until the problem is resolved.

Engage Communication Service Center:

Phone (U.S.) +1.831.688.1021

Fax +1.831.688.1421

Email support@engageinc.com

Web www.engageinc.com

Contents

1 Introduction

BlackDoor OPS User's Guide provides the information users require to install, configure and operate the BlackDoor OPS product developed and manufactured by Engage Communication Inc. This product will enable the user to install the function, across an IP network, to move data in a securely packaged form, to a unit in a remote location. Protocols supported include legacy protocols such as NetBEUI, IPX, AppleTalk and Decnet. Legacy applications that utilize non-routable protocols are able to access services across an IP point to point connection.

1.1 Security

BlackDoor OPS provides a high level secure communication by only exchanging packets with the remote network. The Ethernet frames within the IP envelope must be addressed to specific Ethernet MAC addresses.

Network security is established with Full On Source, Destination Address, UDP Port and IP Packet filtering. Interconnectivity is selectively controlled at the interface, network device and application layers.

1.2 Management

Management of BlackDoor OPS is accomplished with a Command Line Interface, (CLI), that is accessed through the console port or an SSH connection. Templates of the most common configurations provide for an Edit and Paste approach.

1.3 Unit Ports and Indicators

1.3.1 Console Port

A console port for "Out of Band" management access to the unit.

1.3.2 LAN Interface

BlackDoor OPS provides two 10/100/1000BaseT Ethernet LAN interfaces. Management via the LAN ports is enabled when access to the unit is more convenient remotely. LAN1 typically receives unencrypted data from a local network and the LAN2 port moves the encrypted data to a remote BlackDoor OPS. LAN protocols IP, TCP and ICMP are supported.

The LAN1 interface is labeled 1G PORT3 on the front panel. The LAN2 interface is labled 1G PORT1 on the front panel.

1.4 About this Guide

1.4.1 Organization

Introduction provides an overview of the BlackDoor OPS User s Guide as well as feature descriptions.

Installation QuickStart provides a concise description of the installation and configuration process, plus examples to get the experienced user up and running in a minimum of time.

Installation of BlackDoor OPS gives a detailed step by step of the installation and initial configuration of the units. It covers the physical environment and connections required to install the units then steps the administrator through the configuration process of the console port and LAN connections.

Command Line Interface provides a command-by-command description of the upper level interface as well as the interfaces to the various ports.

Troubleshooting reviews some of the common issues that may occur during installation and normal operation of the units and provides descriptions of causes and solutions to these issues.

Appendix - BlackDoor OPS specifications, connector pinouts and crossover wiring details and includes diagrams of the units.

Glossary - Telecommunication and TCP/IP terminology.

1.4.2 Intended Audience

This manual is intended for administrators of telecommunication and network systems. The technical content is written for readers who have basic computer, telecommunication and networking experience.

It is important that any administrator responsible for the installation and operation of Engage BlackDoor products be familiar with IP networking and data communication concepts, such as network addressing and synchronous serial interfaces. These terms are central to an understanding of BlackDoor functionality, and are covered in the Glossary section.

2 Installation QuickStart

This QuickStart Chapter is intended for users who understand how they want their BlackDoor OPS installed and configured and only require the mechanics of performing that installation.

2.1 Communication with BlackDoor OPS

2.1.1 Console Port

Initial communication with BlackDoor OPS unit is made through the Console port, utilizing the Command Line interface, (CLI) detailed in Chapter 4: Command Line Interface.

Please use the provided USB A to Micro USB B cable to connect to the BlackDoor OPS's Micro USB B port labled UART1 on the rear panel. The USB A side of the cable will connect to a computer that is running a Terminal Server program (TeraTerm, HyperTerm, etc.).

Once a serial connection between a workstation and the BlackDoor OPS console port is established and a carriage return <CR> is entered, a Login prompt will appear.

The default login is: root.

The default password for first time login is also root. It is highly recommended that the password be changed upon initial login.

2.1.2 SSH

Once an IP address has been assigned, the user can log into the unit via the network and continue configuration using SSH. Most SSH clients are compatible with the BlackDoor OPS.

2.2 Editing & Pasting Configurations

Users of either CLI have the option of editing a standard BlackDoor OPS configuration in a text editor and pasting that configuration to BlackDoor OPS. The examples in this section are included in a configuration file found on the shipping disk.

Edit the desired configuration listing using a simple text editor. Connect to the BlackDoor OPS unit through SSH or the Console port, then enter the configuration mode with the command: config.

Paste the edited text, comments and all, to the BlackDoor OPS, then issue the command: save. The unit will reset and come up with the new configuration.

To save an BlackDoor OPS configuration to a file, issue the command: show configuration all, and copy the output of the command to a file with your text editor.

2.3 BlackDoor OPS Cabling

BlackDoor OPS uses standard 10/100/1000BaseT Ethernet cabling to connect to an Ethernet switch, router or hub. A crossover 10/100/1000BaseT cable can be used for direct connection to a single router, wireless radio or other Ethernet device.

The cabling used to connect BlackDoor OPS LAN Ports to a switch, router or hub is straight through Ethernet cabling.

2.4 BlackDoor OPS Configuration Parameters

The setup of BlackDoor OPS involves configuration of the:

- Interface Specific Parameters
- BlackDoor OPS System Parameters

2.4.1 Interface Specific Parameters

Console Configuration Parameters

Serial communication settings to the USB serial port should be set as:

115200 baud, 1 stop bit, no parity, 8 bit data, flow control none

LAN Configuration Parameters

BlackDoor OPS Ethernet number 2 (LAN2) is configured for network connectivity. The following parameters must match the configuration of the LAN interface to which it is connected.

2.4.2 BlackDoor OPS System Parameters

System parameters include BlackDoor OPS Host name, the Ethernet IP address and the default router.

host name

Provide a unique name for BlackDoor OPS.

Example:

```
host name AptosBlackDoor
```

ip address

BlackDoor OPS requires configuration of the LAN2 interface which will communicate to another BlackDoor OPS. BlackDoor OPS IP packets communicate over LAN2 only. Configuration of the LAN1 (Local Network) interface is required in Mode Route but optional in Mode Bridge. Management access to the unit via SSH is possible via LAN1 or LAN2.

Example:

```
ip address aaa.bbb.ccc.ddd
```

default gateway

If the remote BlackDoor OPS, whose IP address is configured with ip address, resides on a different IP network from the Local BlackDoor OPS, a default gateway must be specified. The default gateway is typically the local IP WAN Router.

Example:

```
default gateway aaa.bbb.ccc.ddd
```

3 Installation of BlackDoor OPS

This section provides details on the physical location and connections required for the installation of Engage BlackDoor OPS equipment. Also covered is the initial communication with BlackDoor OPS.

References are made to BlackDoor OPS Command Line Interface as well as Configuration and Operation. These topics are covered in detail in later chapters.

The use of Engage BlackDoor OPS systems to encrypt traffic between two Ethernet LANs over an IP network requires one BlackDoor OPS unit at each end.

A standard BlackDoor OPS package includes:

- BlackDoor OPS unit - with installed LAN interface
- USB A to Micro USB B cable
- Power Converter (110 or 220 VAC input/12 VDC output)
- Documentation Compact Disk with BlackDoor OPS User's Guide and configuration examples

3.1 Installing the Hardware

3.1.1 Locating BlackDoor OPS

Site consideration is important for proper operation of BlackDoor OPS. The user should install the unit in an environment providing:

A well-ventilated indoor location

Access within six feet of a power outlet

Two feet additional clearance around the unit to permit easy cable connection

As an option, BlackDoor OPS can be mounted in a standard 19 inch equipment rack, (rack mounts are available from Engage).

3.1.2 Powering BlackDoor OPS

Engage BlackDoor OPS units utilize an external power adapter, available in 110 VAC and 220 VAC versions, providing DC output.

The appropriate power adapter is provided with each unit. Ensure the power adapter is not connected to power then plug the DC adapter into the front panel POWER connector.

3.1.3 Console Port

BlackDoor OPS includes a Console port for initial configuration. It may be used for serial communication from a local workstation or for remote connection via a modem. The Console port utilizes a USB port.

Please use the provided USB A to Micro USB B cable to connect to the BlackDoor OPS's Micro USB B port labled UART1 on the rear panel. The USB A side of the cable will connect to a computer that is running a Terminal Server program (TeraTerm, HyperTerm, etc.).

Communication to the console port should be set for:

115200 baud, 1 stop bit, no parity, 8 bit fixed, flow control none

Once a serial connection between a workstation and BlackDoor OPS console port is established and a carriage return <CR> is entered, a Login prompt will appear.

The default login is: root.

The default password for first time login is also root. It is highly recommended that the password be changed upon initial login.

3.1.4 Configuring the Engage BlackDoor OPS for the LAN

BlackDoor OPS needs to be configured with a number of parameters for proper operation on the network, including:

- Ethernet IP address
- IP data target unit IP address (peer ip address)
- Default gateway if the IP data target is on another IP network
- Mode Route or Mode Bridge. Mode Route utilizes layer 3 encryption where the BlackDoor OPS acts as a router. Mode Bridge utilizes layer 2 encryption where the BlackDoor OPS acts as a bridge between the LAN1 ports of the local and remote units.

The configuration procedure depends on the network environment in which BlackDoor OPS is to be installed.

Note: It is strongly suggested that you configure BlackDoor OPS with its unique network identity before making any Ethernet or Wide Area connections.

3.1.5 Ethernet Interfaces

Engage BlackDoor OPS systems utilize 10/100/1000BaseT Ethernet cable to connect to the Local Area Network. Each system provides a 10/100/1000BaseT interface on the front panel for connection to an Ethernet switch or hub using a straight-thru Ethernet cable. For direct connection to a PC or other LAN device, the user should obtain a 10/100/1000BaseT crossover cable.

The LAN1 interface is labeled 1G PORT3 on the front panel. The LAN2 interface is labled 1G PORT1 on the front panel.

10/100/1000BaseT Ethernet cabling and crossover pinouts are provided in the Appendices.

3.1.6 Ethernet Status LEDs

The green LED on the left side of the Ethernet interface indicates link established and it will blink for activity.

The amber LED on the right side of the Ethernet interface indicates a 1000BaseT link established.

4 Command Line Interface

Command Line access to BlackDoor OPS may be via a serial connection to the Console port or an SSH connection to the Ethernet interface.

SSH provides a secure communications facility defining a standard method of interfacing terminal devices to each other. Any standard SSH client can be used to communicate to an Engage BlackDoor OPS provided there is IP connectivity between the User Host and the BlackDoor OPS.

For communication through the Console port, standard terminal communication software is used.

4.1 Console Communication

Serial communication to the console port should be configured for:

115200 baud, 1 stop bit, no parity, 8 bit fixed, flow control none

Please use the provided USB A to Micro USB B cable to connect to the BlackDoor OPS's Micro USB B port labled UART1 on the rear panel. The USB A side of the cable will connect to a computer that is running a Terminal Server program (TeraTerm, HyperTerm, etc.).

4.2 Logging in to BlackDoor OPS

- An SSH session is opened by providing the IP address of the BlackDoor OPS. On opening a Command Line Interface (CLI) session via the Console port or SSH the login prompt requires entry of a login ID.
- The default login ID: root.
- BlackDoor OPS is shipped with default passwords. Passwords are set or modified with the passwd command, detailed below.

4.3 Overview of Commands

The Engage CLI supports shorthand character entry. At most 3 characters are required for the parsing of commands. For example: show configuration can be entered as: sh con. The CLI is not case sensitive. Description of the commands uses both upper and lower case for syntax definitions and examples. A full description of the command line interface follows.

4.3.1 Categories

The command set can be divided into four categories:

- General
- Show
- Config
- Config Interface

4.3.2 Configuration Modes

For the config and config interface commands, Engage employs a modal approach. The user enters the Config mode, makes changes, then Saves those changes. On Saving the changes the user leaves the Config mode.

The Config interface mode, within the Config mode, is used to set parameters for a specified interface. Once in the Configuration mode, the user enters the interface command. All subsequent commands apply to the specified interface.

The command prompt indicates the mode of operation:

- `name#` the single "#" indicates standard mode
- `name##` indicates BlackDoor OPS is in the Config mode
- `name(LAN1)##` BlackDoor OPS is in Config Interface mode for LAN Port 1

To move up one level, from Interface Config mode to Config mode, enter the interface command with no argument. To change between interfaces when in Interface Config mode, specify the new interface. For example:

```
name(s1)## interface lan1
```

Note: The LAN1 port is the private (local) interface, commonly receives data and LAN2 is the public (WAN) port and generally sends data.

4.3.3 Syntax for Command Parameters

{} == one of the parameters in set is required

[ ] == one of the parameters in set is allowed (optional)

4.4 System Level or General Commands

passwd

Allows setting or modifying the login password. The BlackDoor OPS ships with default passwords. On entering the passwd command, the user is prompted to enter, and confirm, the new password.

bye I quit I logout

Any of these commands will terminate the user session. If you have unsaved configuration changes, you will be prompted to save or discard the new configuration.

reset

Resets BlackDoor OPS.

ping {dest.address} [src.address] [[{number}]]

Sends an ICMP ECHO message to the specified address. Any source address from an interface on BlackDoor OPS can be used. This can be useful to test routes across a LAN or WAN interface.

By default, only 1 message (packet) is sent. A numeric value can be entered to send more than one message.

upgrade [user@]{SFTP host}:{Filename}

SFTP (secure file transfer protocol) provides a means for upgrading BlackDoor OPS firmware in a TCP/IP environment. An SFTP upgrade may be accomplished from a CD provided by Engage Communication if the user can configure their own local SFTP server and place the appropriate upgrade file, from the CD or from Engage Tech Support, on the server.

Once a connection to a SFTP server site has been established, issue the upgrade command.

```
upgrade     chris©157.22.234.129:/users/chris/bd-ops.upg
```

Note that an BlackDoor OPS which is running an upgrade must go through a reset when performing an upgrade. This may cause the SSH connection to drop. If this does occur, simply re-establish the SSH connection.

maxpeersallowed maxpeers-allowed-string

Enter a string provided by Engage Black that is used to change the maximum number of peers allowed on the BlackDoor OPS.

4.5 Show Commands

show interface [lan1 I lan2] {info I statistics}

Provides details on either LAN interface. If no interface is specified, either the current interface per "interface" command will be used, or all interfaces will be shown.

info details the port type, port state, etc.

statistics lists the packets transmitted, received, etc.

show [black I qkd] info

info black details the status of the encryption tunnels. info qkd details the status of the quantum key distribution network.

show router provides general configuration and status information, including the Ethernet hardware address and the firmware version.

show config all provides a list of all configuration parameters. No argument is the same as all. This list provides the basis for storing an BlackDoor OPS configuration into a local text file. The full configuration can be edited offiine.

show config interface [lan1 I lan2]

If no interface is specified, either the current interface per the interface command will be used, or all interfaces will be shown.

show config router lists BlackDoor OPS Hostname, etc.

show log displays a log of the BlackDoor OPS peer to peer QKD communication.

4.6 Configuration Commands

4.6.1 Config Commands

Enter the configuration mode, at which point the following commands may be used.

save

Save the changes and exit Configuration mode.

end

Exit Configuration mode.

restore

Restores the current BlackDoor OPS configuration, ignoring any changes which have been made during the current config session.

host name {namestring}

Provide a unique name for BlackDoor OPS. The new host name does not take effect until a save and reset is performed. For example:

```
host name Dallas IPTube
```

default gateway address

Enter the IP address of the default router or gateway. This must be an IP address on the same network as BlackDoor OPS.

route add {route gateway}

Configures a static route. The route must be in CIDR notation. The gateway is an IP address. The interface is automatically configured LAN1 or LAN2 depending on the gateway IP address.

route del {route}

Deletes a static route. The specified route must be in CIDR notation.

4.6.2 Config Interface Commands

Configuration of BlackDoor OPS involves setting parameters for the LAN interfaces. The user must specify which interface is being configured with the command:

interface [lan1 I lan2]

To move up one level, from Interface Config mode to Config mode, enter the interface command with no argument. To change between interfaces when in Interface Config mode, specify the new interface. For example:

name(LAN1)## interface lan1

ip address address

The interface IP address is required for configuration with SSH or connectivity tests with ping. This configuration parameter is required for LAN2 only. LAN1 is optionally configured for an IP address

Example assigning IP address:

ip address 192.168.1.1

Example removing IP address:

ip address

4.6.3 Config BlackDoor Commands

mode {bridge I route}

bridge specifies layer 2 encryption where the BlackDoor OPS acts as a bridge between the LAN1 ports of the local and remote units.

route specifies layer 3 encryption where the BlackDoor OPS acts as a router and the specified routes are encrypted.

keymode {ikeI manual}

ike uses IKEv2 to establish keys.

manual is selected for manually entering the encryption key via the enterkey command.

rekey period

Specifies the time in minutes the BlackDoor OPS establishes new encryption and message authentication keys with the remote unit. Not used when the keymode is manual.

enterkey {auth I encrypt} string

auth

Enter a string that is used as an authentication secret. The BlackDoor OPS authentication secret must be the same as configured on the remote unit in order for an encryption tunnel to be set up.

encrypt is used for keymode manual. Enter a 64 byte hex string to be used as the encryption key.

The enterkey command causes the unit to reset.

4.6.4 Connection Configuration Commands

The BlackDoor OPS supports multiple connections to other BlackDoor OPS units. There are special commands to configure the parameters for each connection. Connection parameters have underscores. Take care to include the underscores when you type in the parameters.

add conn connection name

Creates a connection with the specified name. All subsequent configuration for this connection specifies the name. The connection initially has no configuration parameters. The connection must be configured with all the required configuration parameters for it to be operational.

remove conn connection name

Removes the named connection from the configuration. The connection and all its configuration parameters are deleted.

setconn connection name peer_ip_address address

Specifies the destination ip address of the remote BlackDoor OPS unit.

setconn connection name peer conn name peer-connection-name

Specifies the peer's connection name.

setconn connection name udp_port value

Specifies the UDP port source and destination address for communication to the remote BlackDoor OPS. The udp_port must be unique for each connection. When mode route is selected the udp_port is used to communicate to the remote connection when sae mode is master or slave.

When mode bridge is selected the udp port is used for the bridge packet tunnel to the remote BlackDoor OPS. This port number is typically 1701 but can be any available port on the router.

setconn connection name remote_encrypted_routes {route[, route]}

Specifies routes to be encrypted and sent to the remote BlackDoor OPS. The route must be in CIDR notation. Example: 192.168.4.0/24. Multiple routes are separated by a comma with no white space before or after the comma. Valid only in mode route.

setconn connection name local_encrypted_routes {route[, route]}

Specifies local routes that are encrypted by the remote and sent to the local BlackDoor OPS. local_encrypted_routes should match the remote_encrypted routes specified on the remote BlackDoor OPS. The route must be in CIDR notation. Example: 192.168.3.0/24. Multiple routes are separated by a comma with no white space before or after the comma. Valid only in mode route.

setconn connection name sae_peer_id id

Specify a string representing the SAE ID of the BlackDoor OPS remote unit (not this unit). SAE ID assignment is in the scope of the quantum key distribution network.

4.6.5 Config Quantum Key Distribution Commands

kme ip address

Specifies the IP address and optionally port address of the KME unit providing a quantum key to the BlackDoor OPS.

qkd mode{off I master I slave}

When off the BlackDoor OPS does not utilize Quantum Key Distribution. master configures the BlackDoor OPS to act as a master secure application entity in the quantum key distribution network. slave configures the BlackDoor OPS to act as a slave secure application entity.

4.6.6 Configuration Examples

Example:

This is an example of a configuration of the BlackDoor OPS in mode bridge.

unit 1	unit 2

default gateway 192.168.3.254
 	
interface lan1
  ip address 192.168.2.50
 	
interface lan2
  ip address 192.168.3.50
 	
mode bridge
 	
Connections
  bd-1
  peer ip address 192.168.4.50
  peer conn name bd-2
  udp port 1701
	default gateway 192.168.4.254
	
	interface lan1
	  ip address 192.168.2.50
	
	interface lan2
	  ip address 192.168.4.50
	
	mode bridge
	
	Connections
	  bd-2
	  peer ip address 192.168.3.50
	  peer conn name bd-1
	  udp port 1701

Example:

This is an example of a configuration of the BlackDoor OPS in mode route with one encrypted network.

unit 1	unit 2

default gateway 192.168.3.254
 	
interface lan1
  ip address 192.168.2.50
 	
interface lan2
  ip address 192.168.3.50
 	
mode route
 	
rekey period 60
 	
Connections
bd-1
peer ip address 192.168.4.50
peer conn name bd-2
remote encrypted routes 192.168.5.0/24
local encrypted routes 192.168.2.0/24
	default gateway 192.168.4.254
	
	interface lan1
	  ip address 192.168.5.50
	
	interface lan2
	  ip address 192.168.4.50
	
	mode route
	
	rekey period 60
	
	Connections
	bd-2
	peer ip address 192.168.3.50
	peer conn name bd-1
	remote encrypted routes 192.168.2.0/24
	local encrypted routes 192.168.5.0/24

Example:

This is an example of a configuration of the BlackDoor OPS in mode route with two connections and QKD.

unit 1	units 2 and 3

default gateway 192.168.3.254
 	
interface lan1
  ip address 192.168.2.50
 	
interface lan2
  ip address 192.168.3.50
 	
kme ip address 10.0.0.75
 	
sae mode master
 	
mode route
 	
rekey period 60
 	
Connections
 	
bd-1
peer ip address 192.168.4.50
peer conn name bd-1
udp port 1701
remote encrypted routes 192.168.5.0/24
local encrypted routes 192.168.2.0/24
sae peer id ENG-1
 	
bd-2
peer ip address 192.168.6.50
peer conn name bd-1
udp port 1702
remote encrypted routes 192.168.7.0/24
local encrypted routes 192.168.2.0/24
sae peer id ENG-2
	Unit 2
	default gateway 192.168.4.254
	
	interface lan1
	  ip address 192.168.5.50
	interface lan2
	  ip address 192.168.4.50
	
	mode route
	
	rekey period 60
	
	kme ip address 10.0.0.76
	
	sae mode slave
	
	Connections
	bd-1
	peer ip address 192.168.3.50
	peer conn name bd-1
	udp port 1701
	remote encrypted routes 192.168.2.0/24
	local encrypted routes 192.168.5.0/24
	sae peer id ENG-0
	
	Unit 3
	default gateway 192.168.6.254
	
	interface lan1
	  ip address 192.168.7.50
	interface lan2
	  ip address 192.168.6.50
	
	mode route
	
	rekey period 60
	
	kme ip address 10.0.0.77
	
	sae mode slave
	
	Connections
	bd-1
	peer ip address 192.168.3.50
	peer conn name bd-2
	udp port 1702
	remote encrypted routes 192.168.2.0/24
	local encrypted routes 192.168.7.0/24
	sae peer id ENG-0

5 Troubleshooting

Communication and Network systems are subject to problems from a variety of sources. Fortunately, an organized troubleshooting approach usually leads to the area of the problem in short order. It is essential to distinguish between problems caused by the LAN (network system), the WAN equipment (communication equipment) and BlackDoor OPSconfiguration.

This troubleshooting section is structured with symptoms in the order the user might encounter them.

5.1 Unable to Communicate with BlackDoor OPS

Installations first require communication with the BlackDoor OPS through console access or from the network, usually the same network as BlackDoor OPS itself. Proceed through the following symptoms if you are unable to communicate with the local BlackDoor OPS using SSH, Ping, etc. IP Addressing should be double checked if accessing the unit via the network.

5.2 Ethernet/General

Cause: Network Cabling is faulty

Solution: Verify cabling is good by swapping BlackDoor OPS cabling with a known good cable and connection. Check the status LEDs on the 10/100/1000BaseT switch to confirm a good connection. If necessary, create a stand-alone LAN with just the workstation and BlackDoor OPS.

5.3 High Ethernet Error Count

Cause: Bad cabling or building wiring

Solution: Check all cabling. Swap to known good port on 10/100/1000BaseT switch or hub to troubleshoot, (testing with large Ping Packets to ascertain quality of Ethernet Connection). To eliminate issues with building wiring connect BlackDoor OPS with a known good Ethernet cable in the same room as the Ethernet hub.

5.4 Can't Communicate using SSH with the BlackDoor OPS

Cause: IP address is not set properly on the BlackDoor OPS

Solution: The Console Port (using cable included with the product) provides direct access to the command line interface of BlackDoor OPS. The Console port utilizes the CLI, detailed in Command Line Interface. Here the IP address can be double checked for accuracy.

Cause: Workstation not on the same subnet as the BlackDoor OPS

Solution: During an initial configuration of an BlackDoor OPS, communication should come from within the same net/subnet. With no default router, BlackDoor OPSwill not be able to reply to communication off its own subnet.

Cause: IP stack on the workstation not configured

Solution: Ensure that other devices on the same LAN can be pinged, or otherwise 'seen'.

5.5 Can't communicate to BlackDoor OPS - Console Port

Cause: Baud Rate, Stop Bits, etc. set wrong on communication application

Solution: Ensure the communication software is configured for a fixed, asynchronous data rate of 115200 bps, 1 stop bit, no parity, 8 bit fixed and that the Flow control is set to none.

5.6 BlackDoor OPS Off Net IP Interconnect Verification

In most applications BlackDoor OPS will be located on different IP networks and the interconnection is through a routed connection. At each end of the routed connection the Tube's default router IP address needs to be pointed to the first router in the path to that remote IP subnet. Through an SSH connection to an BlackDoor OPS it is possible to verify the ability of the unit to ping its local default router and to ping the remote BlackDoor OPS. Note: the console port does not support the Ping Command as it does not have an IP Address.

5.7 TCP/IP Connection

An IP Ping program is the best tool for troubleshooting TCP/IP connectivity. As a sanity check, first ensure you can ping the local router. If unsuccessful, go back to "Can't Communicate using SSH with BlackDoor OPS"

5.8 Can't IP Ping Remote BlackDoor OPS

Cause: Ping workstation does not have Default Gateway (or Router) set. In the workstation's IP configuration, alongside workstation's own IP address and subnet mask, you must provide the IP address of the device (a router) to which all packets destined off the local net should be sent.

Cause: default router on the net, serving as Default Gateway for all net workstations, does not know about the remote IP net where the remote BlackDoor OPS is located.

Solution: Under these circumstances, the two BlackDoor OPS units are on different networks or subnets, the default gateway address must be configured.

6 Appendix

6.1 BlackDoor OPS Specifications

6.1.1 Ethernet Port

10/100/1000BaseT Ethernet

6.1.2 LAN Protocol

IP, TCP, UDP, ICMP

6.1.3 Upgrade Capable

BlackDoor OPS firmware upgrade via Secure File Transfer Protocol, SFTP.

6.1.4 Management

SSH support with Edit and Paste Template Files
Console Port for Out of Band Management
Remote configuration & monitoring

6.1.5 Power Supply

External 12 Volts DC, 1Amp, with standard AC plug. International power supplies available.

6.1.6 Physical

Standard 19 inch rack mount kit available
Dimensions: 6.125" (L) x 4.25" (W) x 1.125" (H)
Weight: approximately 2 lbs., excluding external power adapter.

7 Glossary

Terms and Concepts

Before using the Engage BlackDoor OPS, you should be familiar with the terms and concepts that describe TCP/IP. If you are experienced with internet routers, these terms may already be familiar to you.

7.1 General Networking Terms

Network

A network is a collection of computers, server devices, and communication devices connected together and capable of communication with one another through a transmission medium.

Internet

An internet is any grouping of two or more networks connected by one or more internet routers.

Network Services

Network services are the capabilities that the network system delivers to users, such as print servers, file servers, and electronic mail.

Addresses

Transmitting information in a network system is made possible by an addressing scheme that identifies the sender and destination of the transmission, using network and node addresses. Data is transmitted to and from these addresses in the form of packets.

Routing Table

A routing table is maintained in each router. This table lists all networks and routers in the internet and enables routers to determine the most efficient route for each packet. The routing table serves as a logical map of the internet, specifying the address of the next router in the path to a given destination network and the distance in hops. The router uses the routing table to determine where and whether to forward a packet.

Each router periodically broadcasts its routing table to other routers on each of its directly connected networks, enabling them to compare and update their own tables with the most recent record of connected networks and routes. In this way, routing tables are kept current as changes are made on the internet.

Hop

A hop is a unit count between networks on the internet. A hop signifies "one router away."

Node

Device on the network.

7.2 TCP/IP Networking Terms

SFTP

Secure File Transfer Protocol gives users the ability to transfer files between IP hosts. It uses TCP to provide connection initiation and reliable data transfer.

Host

A computer with one or more uses that can act as an endpoint of communication if it has TCP/IP.

ICMP

Internet Control Message Protocol provides a means for intermediate gateways and hosts to communicate. There are several types of ICMP messages and they are used for several purposes including IP flow control, routing table correction and host availability.

IP

Internet Protocol which routes the data.

IP Datagram

The basic unit of information passed across an IP Internet. It contains address information and data.

ping

Packet InterNet Groper is a program which uses an ICMP echo request message to check if the specified IP address is accessible from the current host.

Port

A destination point used by transport level protocols to distinguish among multiple destinations within a given host computer.

SubNet Address

An extension of the IP addressing scheme which enables an IP site to use a single IP address for multiple physical networks. Subnetting is applicable when a network grows beyond the number of hosts allowed for the IP address class of the site.

TCP

Transmission Control Protocol ensures reliable, sequential, delivery of data. TCP at each end of the connection ensures that the data is delivered to the application accurately, sequential, completely and free of duplicates. The application passes a stream of bytes to TCP which breaks it into pieces, adds a header, forming a segment, and then passes each segment to IP for transmission.

SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. A user can SSH from the local host to a host at a remote site.

UDP

User Datagram Protocol provides a simple, efficient protocol which is connectionless and thus unreliable. The IP address contained in the UDP header is used to direct the datagram to a specific destination host.

Well-Known Port

Any set of port numbers reserved for specific uses, with transport level protocols (TCP & UDP). Well-known ports exist for echo servers, time servers, SSH and FTP servers.