Black•Door
Black•Door GIG

User's Guide

Engage Communication, Inc.
9565 Soquel Drive, Suite 201
Aptos, California 95003

TEL: 831-688-1021 FAX: 831-688-1421

www.engageinc.com
support@engageinc.com

Revision 10

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

Information in this document is subject to change without notice and does not represent a commitment on the part of Engage Communication, Inc.

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 Telecommunication (T1 or E1) and 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 any Engage equipment, 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 x3	Fax	+1.831.688.1421
Email:	**support@engageinc.com**		
Web:	**www.engageinc.com**		

Table of Contents

Chapter 1

Introduction

The Black•Door and Black•Door GIG User's Guide provides the information users require to install, configure and operate the Black•Door product developed and manufactured by Engage Communication Inc.

The Black•Door family protects the confidentiality and integrity of Intranet and Internet Ethernet networks with the strongest commercially available cryptography. The Black•Door Ethernet Encryptor, which supports Point to Point and Multipoint information assurance configurations with unique dynamic keys, is specifically designed for real time wireline backbones and the full spectrum of outdoor Wireless WAN technologies including: Free Space Optics, licensed and unlicensed Radios.

The Black•Door transparently AES encrypts Ethernet networks. Ethernet Voice, Video or Data packets, that are destined for a device located on a remote network or a different local network segment, are AES encrypted at the Link, Network or Transport Layer and then tunneled, bridged or routed to the destination network. At the destination network the packets are decrypted and the original Ethernet packets are securely delivered to the destination Ethernet device.

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.

Management

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

Unit Ports and Indicators

Console Port

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

LAN Interface

The Black•Door Provides two 10/100 BaseT Full/Half Ethernet LAN interfaces with autonegotiation or configurable speed, and duplex. Management via the LAN ports is enabled when remote access to the unit is more convenient. LAN1 is the unencrypted Ethernet Network. LAN2 port is the encrypted network. The LAN LNK indicators show connectivity with a green light.

The Black•Door GIG provides two 10/100/1000 BaseT Full Ethernet LAN interfaces. Currently these interfaces must be manually configured for proper communication. Please see Chapter 2: *Installation QuickStart* for configuration settings for the LAN ports. Management via the LAN ports can be enabled when remote access to the unit is more convenient. LAN1 is the unencrypted Ethernet Network, while LAN2 is the encrypted network. The LAN SPD indicators show 1000Mbps with green, 100Mbps with amber and no light with 10Mbps connectivity. The LAN RD/TD will show when the port is receiving or transmitting data. The IND1 indicator will light approximately every 2 seconds showing that the unit is up and operational.

About this Guide

Organization

Chapter 1 - *Introduction* provides an overview of the *Black•Door, Black•Door GIG User's Guide* as well as feature descriptions.

Chapter 2 - *QuickStart* provides a concise description of the installation and configuration process, plus, examples to get the experienced user up and running in a minimum amount of time.

Chapter 3 - *Installation* of the Black•Door 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.

Chapter 4 - *Command Line Interface* provides a command-by-command description of the upper level interface as well as the interfaces to the various ports.

Chapter 5 - *Operation and Configuration* details the configuration and ongoing operation of the Black•Door.

Chapter 6 - *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.

Appendices - Black•Door specifications, connector pinouts and crossover wiring details and includes diagrams of the units.

Glossary - Telecommunication and TCP/IP terminology.

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 Black•Door products be familiar with IP networking and data communication concepts, such as network addressing. These terms are central to an understanding of Black•Door functionality and are covered in the Glossary section.

Chapter 2

Installation QuickStart

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

Communication with the Black•Door and Black•Door GIG

Console Port

Initial communication with the Black•Door product is made through the Console port, utilizing the Command Line interface. The CLI is detailed in Chapter 4: *Command Line Interface.*

The Console port on the Black•Door uses an RJ45 jack. An RJ45/DB9 adapter is provided in the shipment which, in addition to providing a physical interface, permits direct connection to DTE equipment, such as the COM connections of a PC.

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

The default login is: **root**.

No password is needed for first time login.

Telnet

Once an IP address has been assigned and a serial line connected, the user can log into the unit via the Ethernet network and continue configuration using telnet.

Editing & Pasting Configurations

Users of either CLI have the option of editing a standard Black•Door configuration in a text editor and pasting that configuration to the Black•Door.

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

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

NOTE: Pasting configurations into the Black•Door GIG does not work at this time.

To save a Black•Door or Black•Door GIG configuration to a file, issue the command: **show configuration all**, and copy the output of the command to a file with your text editor.

Cabling

The Black•Door uses standard 10/100BaseT Ethernet cabling to connect to an Ethernet switch, router or hub. The cabling used to connect the Black•Door LAN Ports to a switch, router or hub is straight through Ethernet cabling. Refer to the *Appendices* for the details of the wiring and pinouts of this cable.

A crossover 10/100BaseT cable can be used for direct connection to a single router, wireless radio or other Ethernet device.

The Black•Door GIG must use 1000BaseT Ethernet cabling (CAT6) to connect to any Gigabit Ethernet device.

Configuration Parameters

The setup of the Black•Door involves configuration of the:

- System Parameters
- Interface Specific Parameters
- Security Parameters

The SHOW CONFIG command lists the configuration parameters of the system, the LAN ports, and the Security Parameters. The SHOW INFO command lists the status of the LAN ports and the Security Engine.

System Parameters

System parameters are Host Name, Host Contact, Host Location, the Systems Default-router, Telnet on/off and timeout, SNMP on/off, SNMP Community Name, SNMP Traps on/off and traps on/off.

Host Name, Host Contact, Host Location are useful parameters to identify the BlackDoor.

Interface Specific Parameters

Black•Door Console Configuration Parameters
The console port is an RJ45 port and uses an RJ45/DB9 adapter, included with the unit, and can be connected directly to a desktop or laptop computer for access to the Black•Door.
The console port configuration is: **9600 baud, 1 stop bit, no parity, 8 bit data, flow control none**

Black•Door GIG Console Configuration Parameters
The console port is an RJ45 port and uses an RJ45/DB9 adapter, included with the unit, and can be connected directly to a desktop or laptop computer for access to the Black•Door GIG.
The console port configuration is: **115200 baud, 1 stop bit, no parity, 8 bit data, flow control none**

Black•Door LAN Configuration Parameters
The Black•Door has two 10/100 BaseT Ethernet interfaces: LAN1 and LAN2. LAN1 is Unencrypted and LAN2 is Encrypted. The following parameters must match the configuration of the LAN interface to which it is connected: **Autonegotiation, Duplex, and Speed**

Black•Door GIG LAN Configuration Parameters

The Black•Door has two 10/100/1000 BaseT Ethernet interfaces: LAN1 and LAN2. LAN1 is Unencrypted and LAN2 is Encrypted. The following parameters must match the configuration of the LAN interface to which it is connected: **Duplex, and Speed**. **MaxFileSize** (MTU) must also be set, for normal traffic use 1514 bytes, for VLAN traffic use 1518 bytes. Maximum setting can be as large as 1552

Note: Autonegotiation is currently unavailable as an option for the Black•Door GIG

Black•Door Security Parameters

The BlackDoor AES'S encryption and decryption uses a 256 bit key. The key is entered as 64 hex characters. An internal FIPS 140 approved Random number generator is used to generate the AES 256 bit Key. The BlackDoor's GENKEY function generates a 256 bit random number. The BlackDoor at each end of the link needs to have its AES key set identically by using the ENTERKEY command.

The easiest way to enter the AES KEY into both units is to copy and paste the result of GENKEY to a .txt file and edit it so that it is a single string of characters, then paste it into each unit using the ENTERKEY command.

The BlackDoor supports automatically scheduled rekeying by having REKEY ON and configuring the REKEY PERIOD. When REKEY is configured for OFF, there is only one rekey performed and then no further rekey will take place. REKEY NONE is configured the key that is entered becomes the encryption key.

DualPath is an option that can be added for Geo-Diverse redundancy for disaster recovery applications. There are physically two locations, a Primary and Secondary. The BlackDoor will default and send communications to the Primary site, but when the path is disconnected or no longer available the BlackDoor will then send data to the Secondary location.

Black•Door DualPath

DualPath allows one to configure two peers, a Primary and a Secondary for data flow between one or the other depending upon whether the Primary is available. The BlackDoor polls the network availability of the Primary, and if it is not available, it switches to the Secondary.

Data encryption flows only to the Primary or Secondary, but not both at the same time.

The BlackDoor polls the Primary and Secondary periodically in intervals specified by the PollInterval. When a Primary does not respond to a poll, the BlackDoor will retry the poll the number of times specified by the AliveRetry parameter. When the number of poll retries exceeds the AliveRetry parameter, the BlackDoor closes the Primary path and opens the Secondary path. When the Secondary path is open and the Primary responds to a poll, the BlackDoor immediately closes the Secondary path and opens the Primary path.

The Primary and Secondary are specified in the command line interface like this:

Server IP Address 192.168.1.50 Secondary 192.168.1.51

Keys and VLANIDs can be associated with the Primary and Secondary like this:

Server IP Address 192.168.1.50 key 1 vlan 3 Secondary 192.168.1.51 key 4 vlan 5

This configuration is used on the unit having a Primary and Secondary peer. The Primary or Secondary peer itself indicates it is a Remote in the DualPath configuration like this:

Client IP Address 192.168.2.52 DualPath

A unit configured as DualPath will respond to poll requests from its peer and open or close its path as commanded by the peer.

Peers designated as Primary or Secondary on one BlackDoor must be designated as DualPath on the remote BlackDoors.

The PollInterval and AliveRetry parameters are configured like this:

```
Tunnel DualPath PollInterval 5
Tunnel DualPath AliveRetry 2
```

This configuration would poll the Primary and Secondary every 5 seconds and would switch to the Secondary when the Primary failed to respond to 3 poll requests.

In Mode Route when the Primary and Secondary Black routes are the same network, configure the ip route like this:

```
IP Route  192.168.6.0/24 192.168.5.120 1  LAN2  DualPath
```

In this example, BOTH the Primary and Secondary black routes are 192.168.6.0. The gateway 192.168.5.120 **MUST** be the IP address of the Primary. DualPath MUST be specified in the ip route configuration command line.

Normally the BlackDoor doesn't allow configuration of two gateways for the same network. The DualPath as the route Type indicates to the BlackDoor there is also a Secondary gateway for the route. The routing function knows for this type the Primary may be closed and thus would forward to the Secondary (even without the gateway being specified in the static routes).

There is no special consideration if the Primary and Secondary Black routes are on different networks. One would create a Black static route for each network and gateway as normally done.

When DualPath is configured, the display of Show Info will look like this when a Primary and Secondary is configured:

```
Black Info
----- ----
 Client Host 1 Peer Allowed
 Tunnel Mode 2 Peers Configured
 192.168.5.120: Tunnel State, 2 Rekeys, DualPath Secondary, Not Alive, Path Closed
 192.168.5.121: Tunnel State, 2 Rekeys, DualPath Primary, Alive, Path Open
```

The DualPath Primary or Secondary indicates the mode of the peer. The Alive or Not Alive indicates whether the peer is responding to alive packets from the client. The Open Path is where the BlackDoor is sending the packets. The BlackDoor is not sending packets to the Closed Path.

On a BlackDoor configured as a DualPath remote, the show info looks likethis:

```
Black Info
----- ----
 Server Host 20 Peers Allowed
 Tunnel Mode 1 Peer Configured
 192.168.5.122: Tunnel State, 1 Rekey, DualPath Remote, Path Closed
```

The DualPath Remote indicates it is functioning as a remote end (Primary or Secondary) of a DualPath. Path Closed or Open indicates whether the BlackDoor has set its path to be opened or closed. If the path is closed, the unit is not sending packets to its peer.

There is an additional statistic "Pkts on Closed Port" that indicates how many packets have been dropped because a path is Closed. It would be normal to see packet counts to accumulate on a Closed Path.

```
Black
 |      Pkts on Closed Port                 4417
```

BlackDoor Example Configurations

Server to Client Bridge Configuration Example

Below is an example of a configuration of the Bridging configuration of the Black•Door Server to Client with SNMP Traps turned off and Autonegotiation turned on so that "Speed" and "Duplex" will be set automatically. The IP Address are all on the Same Subnet i.e., 192.168.1.x. AES in on.

```
# Bridge Mode Server

Host Name "BlackDoor Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router

Telnet On
UserTimeout Off

SNMP Off
SNMP Traps Off

Interface LAN1
 Auto Negotiation:  On

 IP Address 192.168.1.52/24
 Port On
 IP State: RUNNING

Interface LAN2
 Auto Negotiation:  On

 IP Address 192.168.1.53/24
 Port On
 IP State: RUNNING

Black
 # Capabilities Bridge, Tunnel
 Mode Bridge
 Client IP Address 192.168.1.55
 Tunnel UDP Port 3175

Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

```
# Bridge Mode Client

Host Name "BlackDoor Client"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router

Telnet On
UserTimeout Off

SNMP Off
SNMP Traps Off

Interface LAN1
 Auto Negotiation:  On

 IP Address 192.168.1.54/24
 Port On
 IP State: RUNNING

Interface LAN2
 Auto Negotiation:  On

 IP Address 192.168.1.55/24
 Port On
 IP State: RUNNING

Black
 # Capabilities Bridge, Tunnel
 Mode Bridge
Server IP Address 192.168.1.53
Tunnel UDP Port 3175

Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

Server to Client Tunnel Configuration Example

Below is an example of a configuration of a Tunneling configuration of the Black•Door Server to Client with SNMP Traps turned off and Autonegotiation turned on so that "Speed" and "Duplex" will be set automatically. AES is on.

```
# Tunnel Mode Server

Host Name "BlackDoor Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router

Telnet On
UserTimeout Off

SNMP Off
SNMP Traps Off

Interface LAN1
 Auto Negotiation:  On

 IP Address 192.168.1.52/24
 Port On
 IP State: RUNNING

Interface LAN2
 Auto Negotiation:  On
 IP Address 192.168.2.52/24
 Port On
 IP State: RUNNING

Black
 # Capabilities Bridge, Tunnel

 Mode Tunnel
 Client IP Address 192.168.2.54
 Tunnel UDP Port 3175

Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

```
# Tunnel Mode Client

Host Name "BlackDoor Client"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router

Telnet On
UserTimeout Off

SNMP Off
SNMP Traps Off

Interface LAN1
 Auto Negotiation:  On

 IP Address 192.168.1.54/24
 Port On
 IP State: RUNNING

Interface LAN2
 Auto Negotiation:  On
 IP Address 192.168.2.54/24
 Port On
 IP State: RUNNING

Black
 # Capabilities Bridge, Tunnel

 Mode Tunnel
 Server IP Address 192.168.2.52
 Tunnel UDP Port 3175

Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

Server to Server Tunnel Configuration Example

Below is an example of a configuration of a Tunneling configuration of the Black•Door Server to Server with SNMP Traps turned off and Autonegotiation turned on so that "Speed" and "Duplex" will be set automatically. The IP Address are all on the Same Subnet i.e., 192.168.1.x. AES is on.

```
# Tunnel Mode Server 1

Host Name "BlackDoor Local Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router

Telnet On
UserTimeout Off

SNMP Off
SNMP Traps Off

Interface LAN1
 AutoNegotiation On

 IP Address 192.168.1.50/24
 Port On

Interface LAN2
 AutoNegotiation On
 IP Address 192.168.2.50/24
 Port On

# Black
# Capabilities Bridge, Tunnel

 Mode Tunnel
 Server IP Address 192.168.2.51
 Tunnel UDP Port 3175

# Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

```
# Tunnel Mode Server 2

Host Name "BlackDoor Remote Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router

Telnet On
UserTimeout Off

SNMP Off
SNMP Traps Off

Interface LAN1
 AutoNegotiation On

 IP Address 192.168.1.51/24
 Port On

Interface LAN2
 AutoNegotiation On
 IP Address 192.168.2.51/24
 Port On

# Black
# Capabilities Bridge, Tunnel

 Mode Tunnel
 Server IP Address 192.168.2.50
 Tunnel UDP Port 3175

# Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

Server to Server Tunnel Configuration Example - Black•Door GIG

Below is an example of a Black•Door GIG configuration with Tunneling of the Black•Door Server to Server with SNMP Traps turned off and Autonegotiation turned off so "Speed" and "Duplex" must be manually set.

```
# Tunnel Mode Server 1

Host Name "BlackDoor Server"
Host Contact "No contact specified"
Host Location "No location specified"

OurDNSServer

IP Default-router

Telnet On

UserTimeout Off

SNMP Off

SNMP Traps Off

Interface LAN1
 Auto Negotiation:  Off
 Speed (in Mbps):   1
 Duplex Mode:  Full
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.1.54/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName

Interface LAN2
 Auto Negotiation:  Off
 Speed (in Mbps):   1
 Duplex Mode:  Full
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.2.54/24
 Port On
 IP State: RUNNING

 DDNS Off

 OurDomainName

Black

 # Capabilities Bridge, Tunnel, Route

 Mode Tunnel
 Server IP Address 192.168.2.55
 Tunnel UDP Port 3175

Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

```
# Tunnel Mode Server 2

Host Name "BlackDoor Client"
Host Contact "No contact specified"
Host Location "No location specified"

IOurDNSServer

IP Default-router

Telnet On

UserTimeout Off

SNMP Off

SNMP Traps Off

Interface LAN1
 Auto Negotiation:  Off
 Speed (in Mbps):   1
 Duplex Mode:  Full
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.1.55/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName

Interface LAN2
 Auto Negotiation:  Off
 Speed (in Mbps):   1
 Duplex Mode:  Full
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.2.55/24
 Port On
 IP State: RUNNING

 DDNS Off

 OurDomainName

Black

 # Capabilities Bridge, Tunnel, Route

 Mode Tunnel
 Server IP Address 192.168.2.54
 Tunnel UDP Port 3175

Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

Server Tunnel Configuration with Multiple Clients Example

Below is an example of a configuration of a Tunneling configuration of the Black•Door Server with multiple Clients with SNMP Traps turned off and Autonegotiation turned on so that "Speed" and "Duplex" will be set automatically. AES is on.

```
# Tunnel Mode Server

Host Name "BlackDoor Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router

Telnet On
UserTimeout Off

SNMP Off
SNMP Traps Off

Interface LAN1
 Auto Negotiation:  On

 IP Address 192.168.1.52/24
 Port On
 IP State: RUNNING

Interface LAN2
 Auto Negotiation:  On
 IP Address 192.168.2.52/24
 Port On
 IP State: RUNNING

Black
 # Capabilities Bridge, Tunnel

 Mode Tunnel
 Client IP Address 192.168.2.54
 Client IP Address 192.168.2.55
 Client IP Address 192.168.2.56
 Client IP Address 192.168.2.57
 Tunnel UDP Port 3175

Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

Dual Path (Two Servers) with multiple Clients Example

Below is a DualPath Tunneling example configuration. The Primary and Secondary Servers and the Client Black•Door configurations are displayed below. SNMP Traps turned off and Autonegotiation turned on so that "Speed" and "Duplex" will be set automatically. AES is on.

```
# Tunnel Mode Primary Server

Host Name "BlackDoor Local Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router 192.168.4.1

Interface LAN1
 Auto Negotiation:  On
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.4.120/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName a.engageinc.com

Interface LAN2
 Auto Negotiation:  On
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.5.120/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName

Black
 # Capabilities Bridge, Tunnel, Route,
DualPath

 Mode Tunnel
 Client IP Address 192.168.5.122 DualPath
 Client IP Address 192.168.5.123 DualPath
 Client IP Address 192.168.5.124 DualPath
 Client IP Address 192.168.5.125 DualPath
 Tunnel UDP Port 3175
 Tunnel DualPath PollInterval 5
 Tunnel DualPath AliveRetry 2

# Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

```
# Tunnel Mode Secondary Server

Host Name "BlackDoor Remote Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router 192.168.4.1

Interface LAN1
 Auto Negotiation:  On
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.4.121/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName a.engageinc.com

Interface LAN2
 Auto Negotiation:  On
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.5.121/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName

Black
 # Capabilities Bridge, Tunnel, Route,
DualPath

 Mode Tunnel
 Client IP Address 192.168.5.122 DualPath
 Client IP Address 192.168.5.123 DualPath
 Client IP Address 192.168.5.124 DualPath
 Client IP Address 192.168.5.125 DualPath
 Tunnel UDP Port 3175
 Tunnel DualPath PollInterval 5
 Tunnel DualPath AliveRetry 2

# Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

Dual Path (Two Servers) with multiple Clients Example, continued...

Below is a DualPath Tunneling example configuration. The Primary and Secondary Servers and the Client Black•Door configurations are displayed below. SNMP Traps turned off and Autonegotiation turned on so that "Speed" and "Duplex" will be set automatically. AES is on.

```
# Tunnel Mode Client 1

Host Name "BlackDoor Local Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router 192.168.4.1

Interface LAN1
 Auto Negotiation:  On
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.4.122/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName a.engageinc.com

Interface LAN2
 Auto Negotiation:  On
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.5.122/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName

Black
 # Capabilities Bridge, Tunnel, Route,
DualPath

 Mode Tunnel
 Server IP Address 192.168.5.121
            Secondary 192.168.5.120
 Tunnel UDP Port 3175
 Tunnel DualPath PollInterval 5
 Tunnel DualPath AliveRetry 2

# Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

```
# Tunnel Mode Client 2

Host Name "BlackDoor Remote Server"
Host Contact "No contact specified"
Host Location "No location specified"

IP Default-router 192.168.4.1

Interface LAN1
 Auto Negotiation:  On
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.4.123/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName a.engageinc.com

Interface LAN2
 Auto Negotiation:  On
 MaxFrameSize  1514

 DHCPClient Off
 IP Address 192.168.5.123/24
 Port On
 IP State: RUNNING
 DDNS Off
 OurDomainName

Black
 # Capabilities Bridge, Tunnel, Route,
DualPath

 Mode Tunnel
 Server IP Address 192.168.5.121
            Secondary 192.168.5.120
 Tunnel UDP Port 3175
 Tunnel DualPath PollInterval 5
 Tunnel DualPath AliveRetry 2

# Security
 AES On
 Rekey On
 Rekey Period 1 Day
```

Chapter 3

Installation of the Black•Door Products

This chapter provides details on the physical location and connections required for the installation of Engage Black•Door equipment. Also covered is the initial communication with the Black•Door.

References are made to the Black•Door *Command Line Interface* as well as *Configuration and Operation*. These topics are covered in detail in later chapters.

The use of Engage Black•Door systems to create a bridge between two Ethernet LANs over an IP network requires one Black•Door unit at each end.

A standard Black•Door package includes:

- Black•Door unit - with installed LAN interface
- Console port adapter and cable
- Power Converter (110 or 220 VAC input 12 to 30 VDC output)
- Documentation Compact Disk with Black•Door User's Guide and configuration examples

Installing the Hardware

Locating the Black•Door products

Site consideration is important for proper operation of the Black•Door and Black•Door GIG. 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, the units can be mounted in a standard 19 inch equipment rack, (rack mounts are available from Engage).

Powering the Black•Door

Engage Black•Door units utilize an external universal power adapter with 100/240 VAC 50/60 Hertz Input with a DC output of 12 Volts DC at 2.5A.

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

Connect the power adapter to an appropriate AC power outlet and check the POWER LED on the front panel of the Engage Black•Door. The POWER LED is GREEN.

Powering the Black•Door GIG

Engage Black•Door GIG units utilize an external universal power adapter with 100/240 VAC 50/60 Hertz Input with a DC output of 12 Volts DC at 4.1A.

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

Connect the power adapter to an appropriate AC power outlet and check the POWER LED on the rear panel of the Engage Black•Door GIG. The POWER LED is GREEN.

Console Port

The Black•Door 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 an RJ45/DB9 jack.

Black•Door console port is configured as a DTE (Data Terminal Equipment) port. This allows direct connection to a DCE (Data Communication Equipment) device such as a modem.

An RJ45 to DB9 adapter is provided with the Black•Door and Black•Door GIG permitting direct connection to DTE equipment, such as the COM1 interface of a PC.

Pinouts for the Console port, as well as Engage supplied adapters, are provided in the *Appendices*.

Communication to the **Black•Door** console port should be set for:

9600 baud, 1 stop bit, no parity, 8 bit fixed, flow control none

Communication to the **Black•Door GIG** 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 the Black•Door console port is established and a carriage return **<CR>** is entered, a **Login** prompt will appear.

The default login is: **root**.

A password is not needed until it is user set.

Configuring the LAN

The Black•Door and Black•Door GIG needs to be configured with a number of parameters for proper operation on the network, including:

- Ethernet IP address and subnet mask
- Default gateway if the IP data target is on another IP network

The configuration procedure depends on the network environment in which the Black•Door equipment is to be installed.

Note: It is strongly suggested that you configure the Black•Door with its unique network identity before making any Ethernet or Wide Area connections.

Ethernet Interfaces - Black•Door

Engage Black•Door systems utilize 10/100BaseT Ethernet cable to connect to the Local Area Network. Each system provides a 10/100BaseT 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 10/100BaseT crossover cable.

LAN1 connects to the Internal Network that is to be encrypted and LAN2 connects to the interconnecting network.

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

Ethernet Interfaces - Black•Door GIG

Engage Black•Door GIG 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.

LAN1 connects to the Internal Network that is to be encrypted and LAN2 connects to the interconnecting network.

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

Status LEDs

LEDs provide Power, Console and LAN Interface status.

Power

Black•Door front panel, the Power LED will be green if power has been properly connected and turned on.

Black•Door GIG rear panel, the PR LED will be green if power has been properly connected and turned on.

Status

Black•Door:
The IND1 LED flashes on and off every second when the CPU timer process is active.
The IND2 LED is undefined at this time.
The IND3 LED is green when the BlackDoor has established an encrypted tunnel with its peer.

Black•Door GIG
The IND1 LED flashes on and off every second when the CPU timer process is active

Ethernet

The Black•Door provides specific information, with RD and TD indicators providing status on packet transmission and receipt, respectively, on the Ethernet interface.

- When receiving, the RD will show a steady or flashing GREEN.
- When transmitting, the TD will show a steady or flashing GREEN.
- If, after power-on, the Black•Door is unable to acquire a unique network address on the LAN both TD and RD will be solid green.
  Note: during full duplex high packet rate both TD and RD will be on simultaneously also.

The Black•Door GIG provides specific information, with SPD and RD/TD indicators providing status on packet activity on the Ethernet interface.

- SPD LED color information
  - 1000BaseT, Green LED
  - 100BaseT, Amber LED
  - 10BaseT, No LED
- RD/TD LED will be Yellow when there is activity on the port

Internal Switches

Black•Door contains an internal four position DIP Switch which is accessible by removing the unit rear panel and sliding out the motherboard.

The default setting for all DIP switches is **OFF**.

Switch 1 - Power cycling the unit with DIP Switch 1 **ON** forces the Black•Door to return to Base Flash operation, (parameters shown in "SHOW CONFIG" are not cleared). This includes operation from Base Flash and deleting any download upgrades. Ensure Switch 1 is returned to the **OFF** position after clearing an upgrade so future upgrades can be performed successfully.

Switch 2 - Must be in the **OFF** position for normal operation.

Switch 3 - This switch must also be set to **OFF** for normal operation.

Switch 4 - DIP Switch 4 can cause internal loopbacks and should be left **OFF**.

NOTE: The Black•Door GIG does not have an internal switch.

Chapter 4

Command Line Interface

Command Line access to the Black•Door family may be via a serial connection to the Console port or a Telnet connection to the Ethernet interface.

Telnet, part of the TCP/IP Protocol Suite, provides a general communications facility defining a standard method of interfacing terminal devices to each other. Any standard Telnet application can be used to communicate to an Engage Black•Door product provided there is IP connectivity between the User Host and the unit.

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

Console Communication

Black•Door serial communication to the console port needs to be configured for:

9600 baud, 1 stop bit, no parity, 8 bit fixed, flow control none

Black•Door GIG serial communication to the console port needs to be configured for:

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

The Black•Door and Black•Door GIG console ports have a RJ45 connector. A RJ45 to DB9 adapter and an 8 wire straight cable are provided with the Black•Door for use with standard PC 9 pin COM ports.

Logging in to the Black•Door family

- A Telnet session is opened by providing the IP address of the Black•Door. On opening a Command Line Interface, (CLI) session, via the Console port or Telnet, the **login** prompt requires entry of a login ID.
- The default login ID: **root.**
- The Black•Door is shipped with no password set. Passwords are set or modified with the **passwd** command, detailed below.

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.

Categories

The command set can be divided into four categories:

- General
- Show
- Config
- Config Interface

Online Help

Included in the General commands is the **HELP**, **HELP CONFIG** and **HELP SHOW** commands, providing information on the entire command set.

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 Telnet mode
- **name##** - indicates the unit is in the Config mode
- **name(LAN1)##** - the unit 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(LAN1)## **interface lan2**

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

Syntax for Command Parameters

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

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

System Level or General Commands

PASSWD

Allows setting or modifying the login password. The Black•Door ships with no password set. On entering the **passwd** command, the user is prompted to enter, and confirm, the new password.

BYE | QUIT | LOGOUT

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

RESET [CAUSE]

Resets the Black•Door. Reset Cause displays a code for the cause of the last reset. Up to 8 reset causes may be stored. A cause of zero is a normal reset which is either an upgrade, a configuration change, or the reset command.

HELP [HELP | ALL | CONFIG | SHOW]

Provides Help information on a selected list of topics. Typing **help** with no argument provides the Help summary screen which is the top-level list of commands.

CLEAR {BLACK | SECURITY | LAN1 | LAN2 | All}

Clears the statistics for the BlackDoor, Security or the port statistics on the selected port: LAN1, LAN2 or ALL.

TERM NN

Allows the user to tailor the number of display lines to their terminal screen size.

PING {dest.address} [src.address] [[{number}]|spray]

Sends an ICMP ECHO message to the specified address. Any source address from an interface on the Black•Door 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. Also, SPRAY can be used to continually send messages until the ESC key is pressed.

UPGRADE {TFTP Server Addr} {Filename}

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

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

UPGRADE 157.22.234.129 upgrade_filename.upg

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

SHOW Commands

SHOW INTERFACE [LAN1 | LAN2] {INFO | 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 ROUTER provides general configuration and status information, including the Ethernet hardware address and the firmware version.

SHOW IP STATISTICS provides detailed statistics on IP packets only.

SHOW SECURITY STATISTICS provides detailed statistics on Security Engine.

SHOW BLACK STATISTICS provides detailed statistics on BlackDoor.

SHOW CONFIG ALL provides a list of all configuration parameters. No argument is the same as **ALL**. This list provides the basis for storing a Black•Door configuration into a local text file. The full configuration can be edited offline.

SHOW CONFIG INTERFACE [LAN1 | 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 Black•Door Hostname, Software Revision, Mac Address, etc.

SHOW SECURITY INFO details the Key, AES and Rekey States.

SHOW BLACK INFO details the BlackDoor State: Bridge, Tunnel, Router.

The BlackDoor lists the IP address of the remote BlackDoor and the state of the Tunnel. The Tunnel states are explained below.

Init State - The BlackDoor has not made contact with the remote BlackDoor

Authorizing - The BlackDoor has made contact with the remote BlackDoor and is verifying its identity. Both BlackDoors must be configured with the same key for their identities to be confirmed.

Key Exchange - The BlackDoor is in the process of changing to a new key.

Tunnel State - The BlackDoor is sending and receiving encrypted data. The Tunnel State is the only state in which data is encrypted and secure.

AES Off - AES is configured Off. The BlackDoor is sending and receiving unencrypted data. Data is not secure.

DualPath Remote - indicates it is functioning as a remote end (Primary or Secondary) of a DualPath. Path Closed or Open indicates whether the BlackDoor has set its path to be opened or closed. If the path is closed, the unit is not sending packets to its peer.

SHOW CONFIG IP [ALL] details the IP configuration. No argument is the same as **ALL**, which provides IP configuration items which don't pertain to a specific port, i.e. default router, etc.

CONFIGURATION Commands

Config Commands

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

SAVE
Save the changes and exit Configuration mode.

END [SAVE]
Exit Configuration mode. The optional SAVE instructs the Black•Door to save configuration changes.

RESTORE
Restores the current Black•Door configuration, ignoring any changes which have been made during the current Telnet **CONFIG** session.

HOST NAME
Provide a unique name for the Black•Door.
Example:
HOST NAME Aptos Black•Door

HOST CONTACT
Provide name of the individual or department that manages the BlackDoor.
Example:
HOST CONTACT Aptos NOC

HOST LOCATION
Specify Location of the Black•Door.
Example:
HOST LOCATION 17th Floor Telco Closet 12

DEFAULT ROUTER
If the Black•Door is to be accessed from an IP Network that is not part of the BlackDoor's IP Address Range and an IP Route to that network is not available, then a default router must be specified. The Default Router can be specified at the System level or at the LAN interface level. If the LAN interface Default Router is configured it is used.

The Default Router is typically the BlackDoor's local IP WAN Router.
Example: IP DEFAULT-ROUTER aaa.bbb.ccc.ddd

TELNET {ON | OFF}
Turns on or off Telnet management. Access to the management interface, when Telnet is turned OFF is restricted to the Console Port and to SNMP if turned ON.

USER TIMEOUT {Off | 1-60}
This setting can be turned Off or set to the number of minutes you can leave your console or telnet session idle before the system automatically logs you out. If logged off, you must simply log on again.

TERM NN
Allows the user to tailor the number of display lines to their terminal screen size.

SNMP {ON | OFF}
Turns on or off SNMP management.

SNMP COMMUNITYNAME
Set or modify Tube SNMP community name. This string is used for authentication for SNMP SetRequests and SNMP traps.

SNMP TRAPS {ON | OFF}
Turns on or off generation of SNMPv1 Traps. The Destination Address for these traps must be configured to be an SNMP management station capable of decoding SNMPv1 traps.

SNMP TRAPS ADDRESS address
Sets the Destination IP Address to which the Tube will send SNMPv1 Traps.

Black•Door Config Interface Commands

Configuration of the Black•Door requires setting parameters for the LAN and SECURITY interfaces. The user must specify which interface is being configured with the command:

INTERFACE [LAN1 | 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**

AUTONEGOTIATION {ON | OFF}
Enable or disable IEEE 802.3 Auto-negotiation on the Ethernet interface. Warning: If the device connected to LAN1 uses Auto Negotiation and LAN1 is configured to use full duplex without Auto-Nego- tiation, the other device may operate in half duplex mode by default and successful operation cannot be guaranteed.

DUPLEX {HALF | FULL}
Sets the duplex mode for the Ethernet interface. This command only takes effect when Auto-negotiation is configured to **OFF**. Warning: If the device connected to LAN1 uses Auto-Negotiation and LAN1 is configured to use full duplex without Auto-Negotiation, the other device may operate in half duplex mode by default and successful operation cannot be guaranteed.

SPEED {10 | 100}
Sets the line rate in Mbps for the Ethernet interface. This command only takes effect when Auto-negotiation is configured to **OFF**.

MaxFrameSize {1514-1552}
MaxFrameSize (MTU) defines the maximum length of an ethernet frame. For the LAN port. The possible values are 1514 to 1552. The default value is 1514 for normal traffic. The setting equal to 1518 is needed to make room for accommodating an Ethernet header that includes an 802.1q VLAN tag. In general, the MaxFrameSize for a LAN port can be set to 1518 unless there is a host on the network that cannot accept a frame of that size. In Route Mode, if it is expected that a decrypted packet would be routed back on LAN2, it is best to have MaxFrameSize equal on LAN1 and LAN2.

IP ADDRESS address[/mask]
The interface IP address and subnet mask are required for configuration with telnet or connectivity tests with ping. The subnet mask can be entered in long or short form. This configuration parameter applies to LAN1 only. Examples:

IP ADDRESS 192.168.1.1/255.255.255.0

IP ADDRESS 192.168.1.1/24

IP DEFAULT-ROUTER address
Configures the IP address of the default router or gateway for this Ethernet interface. This must be an IP address on the same network as the Black•Door Ethernet interface. The default Router is not required if the BlackDoor is to be managed from within the same IP subnet.

Black•Door GIG Config Interface Commands

Configuration of the Black•Door requires setting parameters for the LAN and SECURITY interfaces. The user must specify which interface is being configured with the command:

INTERFACE [LAN1 | 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**

AUTONEGOTIATION {ON | OFF}
Auto-negotiation currently doesn't work for the Black•Door GIG, must be set to **OFF**. The LAN interfaces must be manually set to match the port that they are connected to. The Black•Door GIG provides specific information, with SPD and RD/TD indicators providing status on packet activity on the Ethernet interface.

- SPD LED color information
  - 1000BaseT, Green LED
  - 100BaseT, Amber LED
  - 10BaseT, No LED
- RD/TD LED will be Yellow when there is activity on the port

DUPLEX {HALF | FULL}
Sets the duplex mode for the Ethernet interface. This command only takes effect when Auto-negotiation is configured to **OFF**. Warning: If the device connected to LAN1 uses Auto-Negotiation and LAN1 is configured to use full duplex without Auto-Negotiation, the other device may operate in half duplex mode by default and successful operation cannot be guaranteed.

SPEED {10 | 100 | 1}
Sets the line rate in Mbps for the Ethernet interface. This command only takes effect when Auto-negotiation is configured to **OFF**.

- 10 = 10Mbps
- 100 = 100Mbps
- 1 = 1000Mbps

MAXFRAMESIZE {1514-1552}
MaxFrameSize (MTU) defines the maximum length of an ethernet frame. For the LAN port. The possible values are 1514 to 1552. The default value is 1514 for normal traffic. The setting equal to 1518 is needed to make room for accommodating an Ethernet header that includes an 802.1q VLAN tag. In general, the MaxFrameSize for a LAN port can be set to 1518 unless there is a host on the network that cannot accept a frame of that size. In Route Mode, if it is expected that a decrypted packet would be routed back on LAN2, it is best to have MaxFrameSize equal on LAN1 and LAN2.

IP ADDRESS address[/mask]
The interface IP address and subnet mask are required for configuration with telnet or connectivity tests with ping. The subnet mask can be entered in long or short form. This configuration parameter applies to LAN1 only. Examples:

IP ADDRESS 192.168.1.1/255.255.255.0

IP ADDRESS 192.168.1.1/24

IP DEFAULT-ROUTER address
Configures the IP address of the default router or gateway for this Ethernet interface. This must be an IP address on the same network as the Black•Door Ethernet interface. The default Router is not required if the BlackDoor is to be managed from within the same IP subnet.

Config Security Commands

GENKEY

A random 256 bit key is generated with the **GENKEY** command. This key is to be used for the encryption function on the BlackDoors. At the system level enter this command and it will create a key to input into both units. The Key must be identical for decryption to work.

ENTERKEY [N] XXXXXX. ... (the actual key is 64 hex characters)

On both units issue the **ENTERKEY** command and provide the key generated by the output of the master's **GENKEY** command. The output of the GENKEY command can be copied into an editor and prefaced with ENTERKEY command and pasted onto the CLI when in configuration mode. Be sure to remove the linefeed and/or return characters in the key.

Multiple keys may be stored to have unique key relationships with multiple peers. **N** can be a number from 0 to 20 to identify the key. This number can be used to specify the key in the Client or Server peer specification. Key 0 is the default used when N is not specified.

{Server | Client} IP {[Address] <ip address> [Key n] [VLANID n [, n]] [DualPath] [Secondary <ip address> [Key n] [VLANDID n [, n]]] | Delete <ip address> }

Specifies the peer Server or Client. The peer is identified by its IP Address. Peers are deleted from the configuration by specifying its IP Address.

A Server unit may have up to 20 Client or Server peers. A Client unit may have only one Server peer.

Optionally, a key number may be specified. The key would have been previously configured with the ENTERKEY command. Key 0 is the default used when Key is not specified.

Optionally, up to four VLANIDs may be specified. When more than one VLANID is specified, the VLAN numbers n must be separated by commas. The VLANID is useful in Bride or Tunnel mode in a multipoint configuration. In that case, broadcast packets are forwarded only to peers with the associated VLANID in the packet instead of all peers. The BlackDoor forwards VLAN packets transparently and does not discriminate packets with a VLANID or tag packets.

When the DualPath option is installed, Secondary indicates the configuration for the Secondary peer. The Server or Client is the Primary. DualPath indicates the peer has configured the unit as a Primary or Secondary. Peers configured as Primary or Secondary on one BlackDoor must be configured as DualPath on the remote BlackDoors.

Example: Deleting Server/Client IP entries

```
Server IP Delete 192.168.2.55
```

Example: Configuring a Primary and a Secondary Peer

```
Server IP Address 192.168.1.50 Secondary 192.168.1.51
```

Example: Configuring the Primary or Secondary

```
Client IP Address 192.168.1.52 DualPath
```

AES {ON | OFF}

AES ON
Turns encryption **ON**. Packets are forwarded encrypted.

AES OFF
Turns encryption **OFF**. Packets are forwarded without being encrypted. This mode should only be used during debug to assess whether the packet path is operating without encryption enabled.

REKEY {ON | OFF | NONE}

REKEY ON
Turns Rekeying **ON**.

REKEY OFF
Turns Rekeying **OFF**. Black Door will rekey once to establish an encryption key for communication.

REKEY NONE
There is no REKEY. The key entered using the ENTERKEY command then becomes the encryption key for communication. There is no regeneration of this key. It is used as entered.

REKEY PERIOD {NN [Days | Hours | Minutes]}
Sets the cryptoperiod for the Rekey function. The cryptoperiod can be set to maximum of 45 days. NN is the number Days, Hours, or Minutes of the cryptoperiod. NN defaults to a unit of Minutes if Days or Hours are not specified.

Config Commands

BlackDoor Configuration

Mode {Bridge | Tunnel | Route}

Selects the BlackDoor operating mode, Bridge or Tunnel or Route.

Bridge
In Bridge Mode, both LAN ports are assigned the same IP address.

Tunnel
Tunnel IP Address <ip address>

<ip address> specifies the IP address of the remote BlackDoor.

Tunnel UDP Port <udp port number>

<udp port number> specifies the UDP port for the Tunnel. The port number must be the same for the local and remote BlackDoor.

Tunnel DualPath PollInterval {n}

When the DualPath option is installed, PollInterval configures the number of seconds between polls the BlackDoor sends to a Primary and Secondary to see if it is working on the network.

Tunnel DualPath AliveRetry {n}

When the DualPath option is installed, AliveRetry configures the number of consecutive times the unit allows an unanswered poll packet before it switches to the Secondary peer.

Route
In Route Mode the BlackDoor is a router with traffic for selected routes encrypted at the LAN2 port. The selected routes designate a peer BlackDoor as the gateway and the peer decrypts the traffic.

BlackDoor Servers and Clients are configured in the same manner as in Bridge and Tunnel Mode.

Since the BlackDoor in Route Mode is a router, LAN1 and LAN2 are configured on different networks. Selected routes are encrypted on LAN2 and decrypted before forwarding on LAN1. Thus, LAN2 is the encrypted network and LAN1 is the unencrypted network.

Static routes are defined to effect encryption for that route. If the specification of the gateway for a static route is a BlackDoor peer, packets for that route are encrypted and sent to the BlackDoor peer to be unencrypted and routed. If the gateway is not a BlackDoor peer, the packet is sent to the gateway unencrypted.

Route IP Route { <route>/<network mask> } { <gateway ip address> } { <cost> } { <port> } [DLCI] [Black | DualPath]

The **<route>/<network mask>** specify the route’s network number and mask.

A route of 0.0.0.0 specifies a default route.

The <**gateway ip address**> is the IP address of the gateway.

The <**cost**> is the routing cost expressed in hops.

The <**port**> is the LAN1 or LAN2 port interface for the route. Select LAN2 for Mode Route.

The **DLCI** is optional and not used for Route Mode.

Black is optional and forces the route to be a Black route. Omission of this parameter is recommended since the route will automatically be typed as Black if the gateway is a BlackDoor peer. Behavior is undefined if type Black is forced and the gateway is not a BlackDoor peer.

DualPath is allowed when the DualPath option is installed. DualPath indicates the Primary and Secondary have a Black route for which the network is the same. In this case, DualPath is not optional and must be specified. The gateway must be the IP address of the Primary peer.

IP Delete <route>
Deletes a route from the static route table.

IP Delete 255.255.255.255
Deletes all the routes from the static route table.

Route Mode Configuration steps:

1. Set the Mode to Route and define the BlackDoor peers

```
 Mode Route

 Server IP Address 192.168.2.54

 Server IP Address 192.168.2.56

 Tunnel UDP Port 3175
```

2. Set up the static routes

In configuration mode, configure the static routes

```
IP Route      192.168.3.0/24  192.168.2.54   1    LAN2

IP Route      192.168.4.0/24  192.168.2.56   1    LAN2
```

Note the gateways are Server peers. The route will be designated as Type Black indicating packets for that gateway are encrypted.

Chapter 5

Black•Door Family Operation & Configuration

This chapter provides operational theory and configuration details specific to the Black•Door. The Black•Door has unique requirements regarding its interface to other equipment.

Black•Door and Black•Door GIG Operation

The Black·Door transparently AES encrypts Ethernet networks. Ethernet Voice, Video or Data packets that are destined for a device located on a remote network or a different local network segment, are AES encrypted at the Data Link, Network or Transport Layer and then tunneled, bridged or routed to the destination network. At the destination network the packets are decrypted and the original Ethernet packets are securely delivered to the destination Ethernet device.

Advanced Encryption Standard
FIPS approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive information.

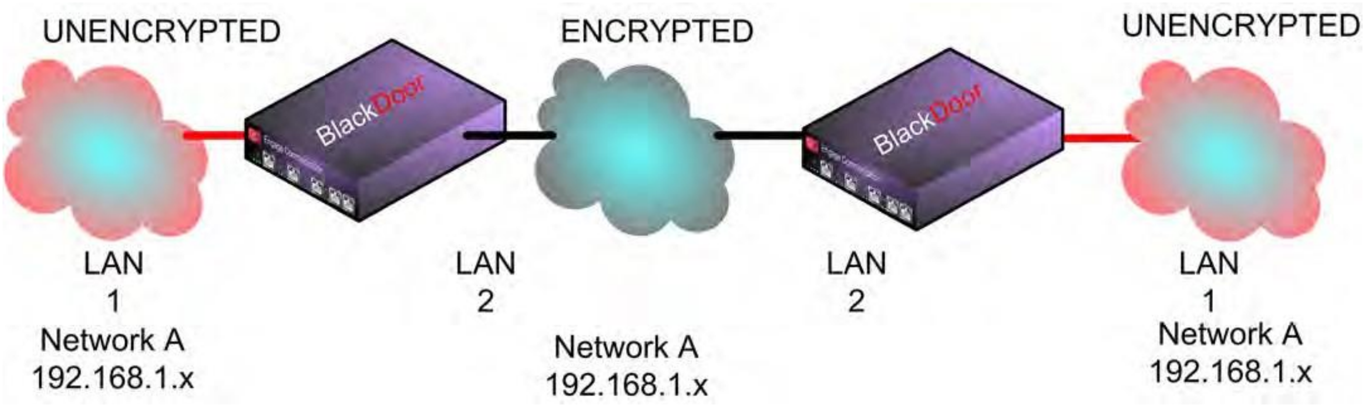
Key Management
Automated 256 bit key management configurations ensure timely key transitions and eliminate the operational and maintenance costs of managing an encrypted network with manual key distribution.

Management
An IP Ethernet interface enables ease of management, configuration, and upgradeability. Management is accomplished with a Command Line Interface that is accessed through a Console or Telnet connection. Templates of the most common configurations provide for an Edit and Paste configura- tion. The Black·Door's SNMP MIB I and II supports interface status change traps.

Black Bridge

The BlackDoor transparently monitors all the packet traffic. Non Local Packets are encrypted at the Mac layer and tunneled to the destination network. Note: the devices on the bridged networks must be in the same IP Network.

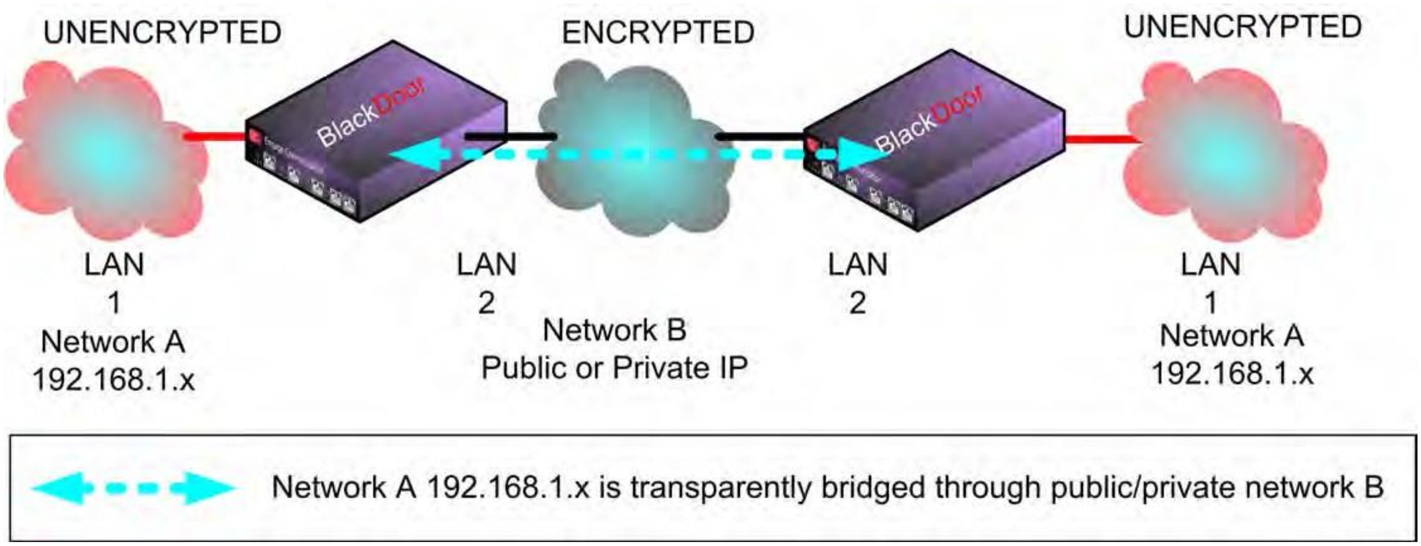
AES ENCRYPTED BRIDGE



Black Tunnel

Interconnects Ethernet LANs through an IP Transparent Encrypted Tunnel. Original packets are entirely encrypted and then encapsulated into an IP packet that is forwarded to the destination network.

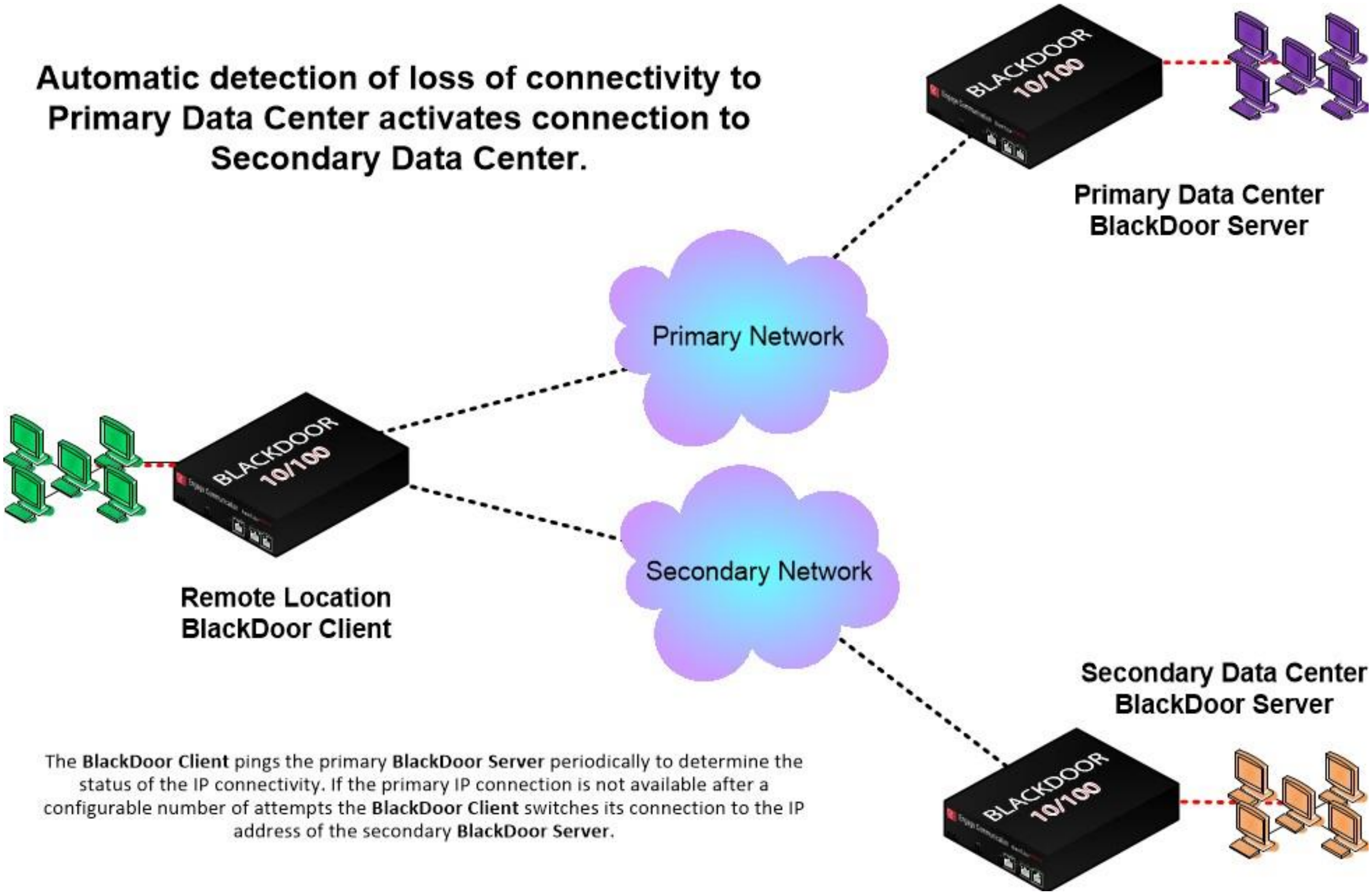
AES ENCRYPTED TUNNEL



DualPath Tunnel

DualPath allows one to configure two peers, a Primary and a Secondary for data flow between one or the other depending upon whether the Primary is available. The BlackDoor polls the network availability of the Primary, and if it is not available, it switches to the Secondary. Data encryption flows only to the Primary or Secondary, but not both at the same time.

The BlackDoor polls the Primary and Secondary periodically in intervals specified by the PollInterval. When a Primary does not respond to a poll, the BlackDoor will retry the poll the number of times specified by the AliveRetry parameter. When the number of poll retries exceeds the AliveRetry parameter, the BlackDoor closes the Primary path and opens the Secondary path. When the Secondary path is open and the Primary responds to a poll, the BlackDoor immediately closes the Secondary path and opens the Primary path.


Automatic detection of loss of connectivity to Primary Data Center activates connection to Secondary Data Center.
BLACKDOOR 10/100
Primary Data Center BlackDoor Server
Primary Network
Secondary Network
Remote Location BlackDoor Client
Secondary Data Center BlackDoor Server
The BlackDoor Client pings the primary BlackDoor Server periodically to determine the status of the IP connectivity. If the primary IP connection is not available after a configurable number of attempts the BlackDoor Client switches its connection to the IP address of the secondary BlackDoor Server.

Black•Door and Black•Door GIG Installation Steps

The process of installing a Black•Door involves the following steps:

- Planning for Black•Door interconnect
- Installing the Black•Door hardware
- Configuring System, Networking and Security parameters
- Making Ethernet cabling connections
- Verifying the Black•Door connection

Black•Door Cabling

The Black•Door uses standard 10/100BaseT Ethernet cabling to connect to an Ethernet switch or hub. Ethernet Crossover cable required to directly connect to a PC or another BlackDoor's Ethernet interface. Refer to the *Appendices* for the details of the wiring of this cable.

Black•Door GIG Cabiling

The Black•Door uses standard 10/100/1000BaseT Ethernet cabling (CAT6) to connect to an Ethernet switch or hub. Ethernet Crossover cable required to directly connect to a PC or another BlackDoor's Ethernet interface. Refer to the *Appendices* for the details of the wiring of this cable.

Black•Door Configuration Parameters

The setup of the Black•Door involves configuration of the:

- Black•Door System Parameters
- Interface Specific Parameters
- Black•Door Security Parameters

Black•Door Family System Parameters

System parameters are the Host Name, Host Contact, Host Location, the Systems Default-router, Telnet on/off and timeout, SNMP on/off, SNMP Community Name, SNMP Traps on/off and traps on/off.

Host Name, Host Contact, Host Location are useful parameters to identify the BlackDoor.

HOST NAME
Provide a unique name for the Black•Door.
Example:
HOST NAME Aptos Black•Door

HOST CONTACT
Provide name of the individual or department that manages the BlackDoor.
Example:
HOST CONTACT Aptos NOC

HOST LOCATION
Specify Location of the Black•Door.
Example:
HOST LOCATION 17th Floor Telco Closet 12

DEFAULT ROUTER
If the Black•Door is to be accessed from an IP Network that is not part of the BlackDoor's IP Address Range and an IP Route to that network is not available, then a default router must be specified. The Default Router is specified at the System level.

> The Default Router is typically the BlackDoor's local IP WAN Router.
> Example: IP DEFAULT-ROUTER aaa.bbb.ccc.ddd

TELNET {ON | OFF}
Turns on or off Telnet management. Access to the management interface, when Telnet is turned OFF is restricted to the Console Port and to SNMP if turned ON.

USER TIMEOUT {Off | 1-60}
This setting can be turned Off or set to the number of minutes you can leave your console or telnet session idle before the system automatically logs you out. If logged off, you must simply log on again.

TERM NN
Allows the user to tailor the number of display lines to their terminal screen size.

SNMP {ON | OFF}
Turns on or off SNMP management.

SNMP COMMUNITYNAME
Set or modify Tube SNMP community name. This string is used for authentication for SNMP SetRequests and SNMP traps.

SNMP TRAPS {ON | OFF}
Turns on or off generation of SNMPv1 Traps. The Destination Address for these traps must be configured to be an SNMP management station capable of decoding SNMPv1 traps.

SNMP TRAPS ADDRESS address
Sets the Destination IP Address to which the Tube will send SNMPv1 Traps.

Black•Door Interface Specific Parameters

Console Configuration Parameters

The console port is an RJ45 port and uses an RJ45/DB9 adapter, included with the unit, and can be connected directly to a desktop or laptop computer for access to the Black•Door GIG.
The console port configuration is: **9600 baud, 1 stop bit, no parity, 8 bit data, flow control none**

LAN Configuration Parameters

The Black•Door has two 10/100BaseT Ethernet interfaces: LAN1 and LAN2. LAN1 is Unencrypted and LAN2 is Encrypted. The following parameters must match the configuration of the LAN interface to which it is connected.

PORT {ON | OFF}
Turns on or off LAN interface.

AUTONEGOTIATION {ON | OFF}
Enable or disable IEEE 802.3 Auto-Negotiation on the Ethernet interface. The LAN Ethernet DuPLEX and SPEED are negotiated. If Negotiation does not occur the Ethernet interface defaults to 10BaseT Half Duplex.

Warning: If the device connected to LAN1 uses Auto-Negotiation and LAN1 is configured to use full duplex without Auto-Negotiation, the other device may operate in half duplex mode by default and successful operation cannot be guaranteed.

DUPLEX {HALF | FULL}
Sets the duplex mode for the Ethernet interface. This command only takes effect when Auto-negotiation is configured to **OFF**.

SPEED {10 | 100}
Sets the line rate in Mbps for the Ethernet interface. This command only takes effect when Auto-Negotiation is configured to **OFF**.

IP ADDRESS address[/mask]
The interface IP address and subnet mask are required for connection to the network and access with telnet or connectivity tests with ping. The IP ADDRESS must be unique within the network's IP address range. The subnet mask can be entered in long or short form.

Example:

IP ADDRESS aaa.bbb.ccc.ddd/ee

Black•Door GIG Interface Specific Parameters

Console Configuration Parameters

The console port is an RJ45 port and uses an RJ45/DB9 adapter, included with the unit, and can be connected directly to a desktop or laptop computer for access to the Black•Door GIG.
The console port configuration is: **115200 baud, 1 stop bit, no parity, 8 bit data, flow control none**

LAN Configuration Parameters

The Black•Door has two 10/100/1000BaseT Ethernet interfaces: LAN1 and LAN2. LAN1 is Unencrypted and LAN2 is Encrypted. The following parameters must match the configuration of the LAN interface to which it is connected.

PORT {ON | OFF}
Turns on or off LAN interface.

AUTONEGOTIATION {ON | OFF}
Auto-negotiation currently doesn't work for the Black•Door GIG, must be set to **OFF**. The LAN interfaces must be manually set to match the port that they are connected to. The Black•Door GIG provides specific information, with SPD and RD/TD indicators providing status on packet activity on the Ethernet interface.

- SPD LED color information
  - 1000BaseT, Green LED
  - 100BaseT, Amber LED
  - 10BaseT, No LED
- RD/TD LED will be Yellow when there is activity on the port

DUPLEX {HALF | FULL}
Sets the duplex mode for the Ethernet interface. This command only takes effect when Auto-negotiation is configured to **OFF**.

SPEED {10 | 100 | 1}
Sets the line rate in Mbps for the Ethernet interface. This command only takes effect when Auto-Negotiation is configured to **OFF**.

- 10 = 10Mbps
- 100 = 100Mbps
- 1 = 1000Mbps

IP ADDRESS address[/mask]
The interface IP address and subnet mask are required for connection to the network and access with telnet or connectivity tests with ping. The IP ADDRESS must be unique within the network's IP address range. The subnet mask can be entered in long or short form.

Example:

IP ADDRESS aaa.bbb.ccc.ddd/ee

Black•Door Security Parameters

The BlackDoor AES'S encryption and decryption uses a 256 bit key. The key is entered as 64 hex characters. An internal FIPS 140 approved Random number generator is used to generate the AES 256 bit Key. The BlackDoor's GENKEY function generates a 256 bit random number. The BlackDoor at each end of the link needs to have its AES key set identically by using the ENTERKEY command.

The BlackDoor supports automatically scheduled rekeying by having REKEY ON and configuring the REKEY PERIOD.

The BlackDoor must be in Configuration Mode in order to change the Security parameters.

GENKEY
A random 256 bit key is generated with the **GENKEY** command. This key is to be used for the encryption function on the BlackDoors. At the system level enter this command and it will create a key to input into both units. The Key must be identical for the decryption to work.

ENTERKEY [N] XXXXXX. ... (the actual key is 64 hex characters)
On both units issue the **ENTERKEY** command and provide the key generated by the output of the master's **GENKEY** command. The output of the GENKEY command can be copied into an editor and prefaced with ENTERKEY command and pasted onto the CLI when in configuration mode. Be sure to remove the linefeed and/or return characters in the key.

Multiple keys may be stored to have unique key relationships with multiple peers. **N** can be a number from 0 to 20 to identify the key. This number can be used to specify the key in the Client or Server peer specification. Key 0 is the default used when N is not specified.

{Server | Client} IP {[Address] <ip address> [Key n] [VLANID n [, n]] [DualPath] [Secondary <ip address> [Key n] [VLANDID n [, n]]] | Delete <ip address> }

Specifies the peer Server or Client. The peer is identified by its IP Address. Peers are deleted from the configuration by specifying its IP Address.

A Server unit may have up to 20 Client or Server peers. A Client unit may have only one Server peer.

Optionally, a key number may be specified. The key would have been previously configured with the ENTERKEY command. Key 0 is the default used when Key is not specified.

Optionally, up to four VLANIDs may be specified. When more than one VLANID is specified, the VLAN numbers n must be separated by commas. The VLANID is useful in Bride or Tunnel mode in a multipoint configuration. In that case, broadcast packets are forwarded only to peers with the associated VLANID in the packet instead of all peers. The BlackDoor forwards VLAN packets transparently and does not discriminate packets with a VLANID or tag packets.

When the DualPath option is installed, Secondary indicates the configuration for the Secondary peer. The Server or Client is the Primary. DualPath indicates the peer has configured the unit as a Primary or Secondary. Peers configured as Primary or Secondary on one BlackDoor must be configured as DualPath on the remote BlackDoors.

Example: Deleting Server/Client IP entries

```
Server IP Delete 192.168.2.55
```

Example: Configuring a Primary and a Secondary Peer

```
Server IP Address 192.168.1.50 Secondary 192.168.1.51
```

Example: Configuring the Primary or Secondary

```
Client IP Address 192.168.1.52 DualPath
```

AES {ON | OFF}

AES ON
Turns encryption **ON**. Packets are forwarded encrypted.

AES OFF
Turns encryption **OFF**. Packets are forwarded without being encrypted. This mode should only be used during debug to assess whether the packet path is operating without encryption enabled.

REKEY {ON | OFF | NONE}

REKEY ON
Turns Rekeying **ON**.

REKEY OFF
Turns Rekeying **OFF**. One rekey happens to establish secure communication, no future rekeys are performed.

REKEY NONE
The configured key is the encryption key. No rekeying is performed.

REKEY PERIOD {NN [Days | Hours | Minutes]}
Sets the cryptoperiod for the Rekey function. The cryptoperiod can be set to maximum of 45 days. NN is the number Days, Hours, or Minutes of the cryptoperiod. NN defaults to a unit of Minutes if Days or Hours are not specified.

Show Security Info

AES Off - AES is configured Off. The BlackDoor is sending and receiving unencrypted data. Data is not secure.

SHOW SECURITY INFO details the Key, AES, Rekey States and DualPath Information.

Key State:

Key Configured - The key is non-zero.
No Key   - The key is zero.

AES State:

- OFF   No contact with remote unit or AES configured off.
- ON   AES state confirmed, initial key exchanged if Rekey On.

Number of Rekeys: The number of times the BlackDoor has exchanged with its peers.

DualPath: The DualPath Primary or Secondary indicates the mode of the peer. The Alive or Not Alive indicates whether the peer is responding to alive packets from the client. The Open Path is where the BlackDoor is sending the packets. The BlackDoor is not sending packets to the Closed Path.

Example:

```
Black Info
----------
 Client Host 1 Peer Allowed
 Tunnel Mode 2 Peers Configured
192.168.5.120: Tunnel State, 2 Rekeys, DualPath Secondary, Not Alive, Path Closed
192.168.5.121: Tunnel State, 2 Rekeys, DualPath Primary, Alive, Path Open
```

Show BlackDoor Info

The BlackDoor lists the IP address of the remote BlackDoor and the state of the Tunnel. The Tunnel states are explained below.

Init State - The BlackDoor has not made contact with the remote BlackDoor

Authorizing - The BlackDoor has made contact with the remote BlackDoor and is verifying its identity. Both BlackDoors must be configured with the same key for their identities to be confirmed.

Key Exchange - The BlackDoor is in the process of changing to a new key.

Tunnel State - The BlackDoor is sending and receiving encrypted data. The Tunnel State is the only state in which data is encrypted and secure in Tunnel Mode.

AES Off - AES is configured Off. The BlackDoor is sending and receiving unencrypted data. Data is not secure.

SNMP Support

All Engage products support SNMP (Simple Network Management Protocol) version 1. SNMP support provides access via IP to groups of administrative, configuration-related, and statistical information objects about the Engage device. An IP network connection to the device and a PC with an application which provides an SNMP version 1 client are required.

An SNMP client will query the device and display the information objects and their values to the user. Groups of SNMP information objects are referred to as MIBs (Management Information Base). All Engage products support most of MIB-II (MIB-2). The subgroups of information in MIB-II are as follows:

- System group: contains system information such as a designated system identifier, location, and vendor ID (Engage).
- Interface group: contains information about the network connections on the de vice including interface type, link status, packets transmitted and received.
- AT group: contains information about the ARP entries on the device including the values for MAC Address and IP Address for each entry.
- IP group: contains IP statistics and configuration on the device including IP pack ets received, packets discarded, and IP address and subnet mask.
- ICMP group: contains statistics for ICMP statistics including packets sent for redirect, port unreachable, or echo requests (Ping).
- UDP group: contains statistics for UDP including packets received and transmitted, and packets sent to a UDP port with no listener.
- SNMP group: contains statistics for the SNMP protocol including packets received and transmitted, error packets, and number of set requests.

For more detail, MIB-II is fully specified in RFC1213, available at http://www.faqs.org/rfcs/rfc1213.html.

SNMPv1 Traps

The Black•Door supports generation of SNMPv1 Traps. Traps are messages sent from the device's LAN port when specific events occur.

The following traps may be generated:

- coldStart: this trap is generated if the Tube reinitializes itself after a configuration change.

- warmStart: this trap is generated if the Tube reinitializes itself after a reset which does not involve a configuration change.
- linkUp: this trap is generated when a physical interface transitions from being disconnected to connected.
- linkDown: this trap is generated when a physical interface transitions from being connected to disconnected.
- authenticationFailure: this trap is generated when a login to the user interface or an SNMPv1 SetRequest failed because an incorrect password was given.
- enterprisespecific: these are Engage proprietary traps.

We define the following subcategories:

- engageTrapRxOverrun: this trap is generated when excessive receiver overruns are happening on an interface.
- engageTrapTxUnderrun: this trap is generated when excessive transmitter underruns are happening on an interface.
- engageTrapBufferExhaustion: this trap is generated when the device runs out of free buffers for packet processing.
- engageTrapDeafness: this trap is generated when an interface on the box has not received packets for a long period of time.
- engageTrapTubeEnetRxAbsent: this trap is generated when a Black•Door does not receive IPTube-encapsulated IP packets on its LAN interface when it expects.

For more detail on the industry standard traps, please see http://www.faqs.org/rfcs/rfc1157.html.

Chapter 6

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 the Black•Door configuration.

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

Unable to Communicate with the Black•Door

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

Ethernet/General

Cause: Network Cabling is faulty

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

High Ethernet Error Count

Cause: Bad cabling or building wiring

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

Cause: Can not connect to a hub at 100 Mbps with autonegotiate turned on. Connection drops to 10 Mbps at half duplex.

Solution: Change LAN1 interface to match what the hub is configured for, by first turning **Autonegotiate OFF**.

Can’t Communicate using Telnet with the Black•Door

Cause: IP address is not set properly on the Black•Door

Solution: The Console Port, which requires an RJ45 to DB9 adapter, (included with the product), provides direct access to the command line interface of the Black•Door. The Console port utilizes the CLI, detailed in Chapter 4: *Command Line Interface*. Details of the connector pins are in the *Appendices*. Here the IP address can be double checked for accuracy.

Cause: Workstation not on the same subnet as the Black•Door

Solution: During an initial configuration of a Black•Door, communication should come from within the same net/subnet. With no default router, the Black•Door will 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'.

Can’t communicate to the Black•Door - 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 9600 bps, 1 stop bit, no parity, 8 bit fixed and that the Flow control is set to none.

Cause: Transmit and Receive Data swapped

Solution: The console port is configured as a DTE port. For connection to a DCE device, such as a modem, a Null Modem adapter is required.

Black•Door Off Net IP Interconnect Verification

In most applications the Black•Door 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 a Telnet connection to a Black•Door it is possible to verify the ability of the unit to ping its local default router and to ping the remote Black•Door. Note: the console port does not support the Ping Command as it does not have an IP Address.

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 telnet with the Black•Door"

Can't IP Ping Remote Black•Door

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 Black•Door is located.

Solution: Under these circumstances, the two Black•Door units are on different networks or subnets, the **DEFAULT ROUTER** address must be configured.

Using Black•Door Statistics for Debug

Can IP Ping Remote Black•Door, but no traffic

View the Show Black Info statistics.

```
Black Info
----- ----
 Client Host 1 Peer Allowed
 Tunnel Mode 2 Peers Configured
192.168.5.120: Tunnel State, 2 Rekeys, DualPath Secondary, Not Alive, Path Closed
192.168.5.121: Tunnel State, 2 Rekeys, DualPath Primary, Alive, Path Open
```

If the peer IP Address can be pinged successfully, then the Init State probably means the keys don't match. When entering the key, copy the 'genkey' result and paste it into a .txt document. Then remove the line feed and return characters. Copy and paste the same key after the 'enterkey' command for both units.

Tunnel State means the connection is up and running (with encryption if AES is configured On).

The DualPath Primary or Secondary indicates the mode of the peer. The Alive or Not Alive indicates whether the peer is responding to alive packets from the client. The Open Path is where the Black-

Door is sending the packets. The BlackDoor is not sending packets to the Closed Path.

Verify that AES encryption is On

Use Show Security Info to view AES Encryption status.

```
BlackDoor Client# show security info
Security Info
-------- ----
AES State:          On
```

Note that if more than one peer is configured, AES will not be On unless ALL peers are in Tunnel State.

Appendix A

Black•Door Specifications

Ethernet Port

- 10/100 Base T Full/Half Ethernet (Black•Door)
- 10/100/1000 Base T Full/Half Ethernet (Black•Door GIG)

LAN Protocol

- IP, TCP, UDP, ICMP
- Assured Delivery Protocol

Quality of Service Support

- IP Type of Service (TOS) CLI configurable
- IANA Registered UDP Port 3175

TFTP Online Upgrade Capable (FLASH ROMs)

- Black•Door is fully operational during upgrade
- Currently not available on the Black•Door GIG

Management

- Telnet support with Edit and Paste Template Files
- Console Port for Out of Band Management
- SNMP support (MIB I, MIB II)
- Remote configuration & monitoring

Power Supply

- Black•Door - External 12 Volts AC, 2.5Amp, with standard AC plug. International power supplies available.
- Black•Door GIG - External 12 Volts AC, 4.1Amp, with standard AC plug. International power supplies available.

Physical

- Standard 19 inch rack mount kit available
- Dimensions: 9.0 x 7.3 x 1.63 inches
- Weight: approximately 2 lbs., excluding external power adapter.

Black•Door Switch Settings

Black•Door systems contain an internal four position DIP Switch which is accessible by removing the unit rear panel and sliding out the motherboard.

The default setting for all DIP switches is **OFF**.

Switch 1 - Power cycling the unit with DIP Switch 1 **ON** forces the Black•Door to return to Base Flash operation, (parameters shown in "SHOW CONFIG" are not cleared). This includes operation from Base Flash and deleting any download upgrades. Ensure Switch 1 is returned to the **OFF** position after clearing an upgrade so future upgrades can be performed successfully.

Switch 2 - Must be in the **OFF** position for normal operation.

Switch 3 - This switch must also be set to **OFF** for normal operation.

Switch 4 - DIP Switch 4 can cause internal loopbacks and should be left **OFF**.

Note: The Black•Door GIG does not have an internal four position DIP Switch.

Console Port Information

RJ45 Console Port Pinout

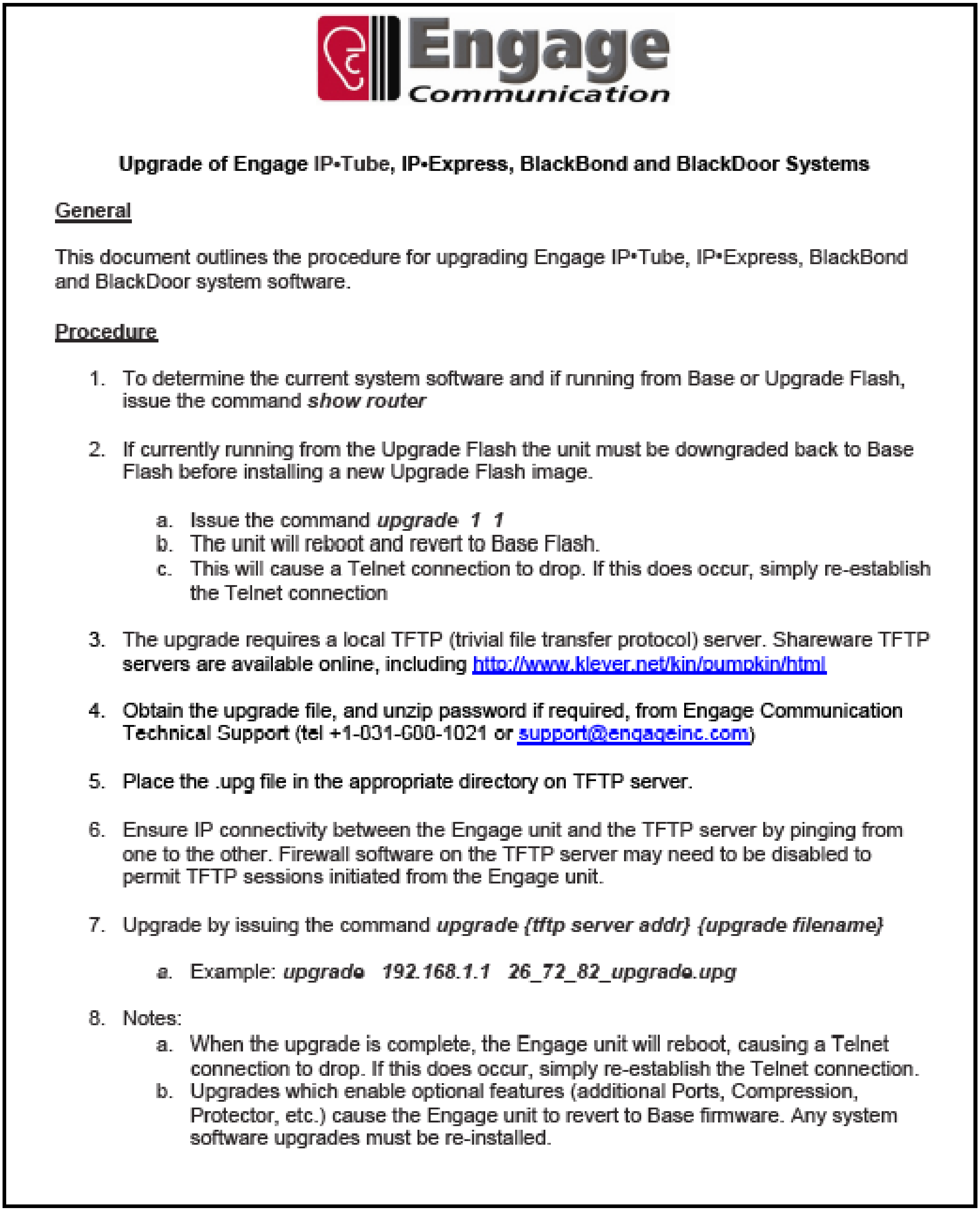
RJ45 pin	Signal Name
3	TxData
6	RxData
1	RTS
8	CTS
4	Gnd
2	DTR

Black•Door RJ45/db9F Null Modem Adapter

RJ45 pin	db9pin
3	2
6	3
1	8
4	5
2	6

Black Door GIG RJ45/db9F Null Modem Adapter

RJ45 pin	db9pin
6	2
5	3
4	5



Upgrade of Engage IP•Tube, IP•Express, BlackBond and BlackDoor Systems

General

This document outlines the procedure for upgrading Engage IP•Tube, IP•Express, BlackBond and BlackDoor system software.

Procedure

1. To determine the current system software and if running from Base or Upgrade Flash, issue the command ***show router***

2. If currently running from the Upgrade Flash the unit must be downgraded back to Base Flash before installing a new Upgrade Flash image.

   a. Issue the command ***upgrade 1 1***
   b. The unit will reboot and revert to Base Flash.
   c. This will cause a Telnet connection to drop. If this does occur, simply re-establish the Telnet connection

3. The upgrade requires a local TFTP (trivial file transfer protocol) server. Shareware TFTP servers are available online, including http://www.klever.net/kin/pumpkin/html

4. Obtain the upgrade file, and unzip password if required, from Engage Communication Technical Support (tel +1-831-688-1021 or support@engageinc.com)

5. Place the .upg file in the appropriate directory on TFTP server.

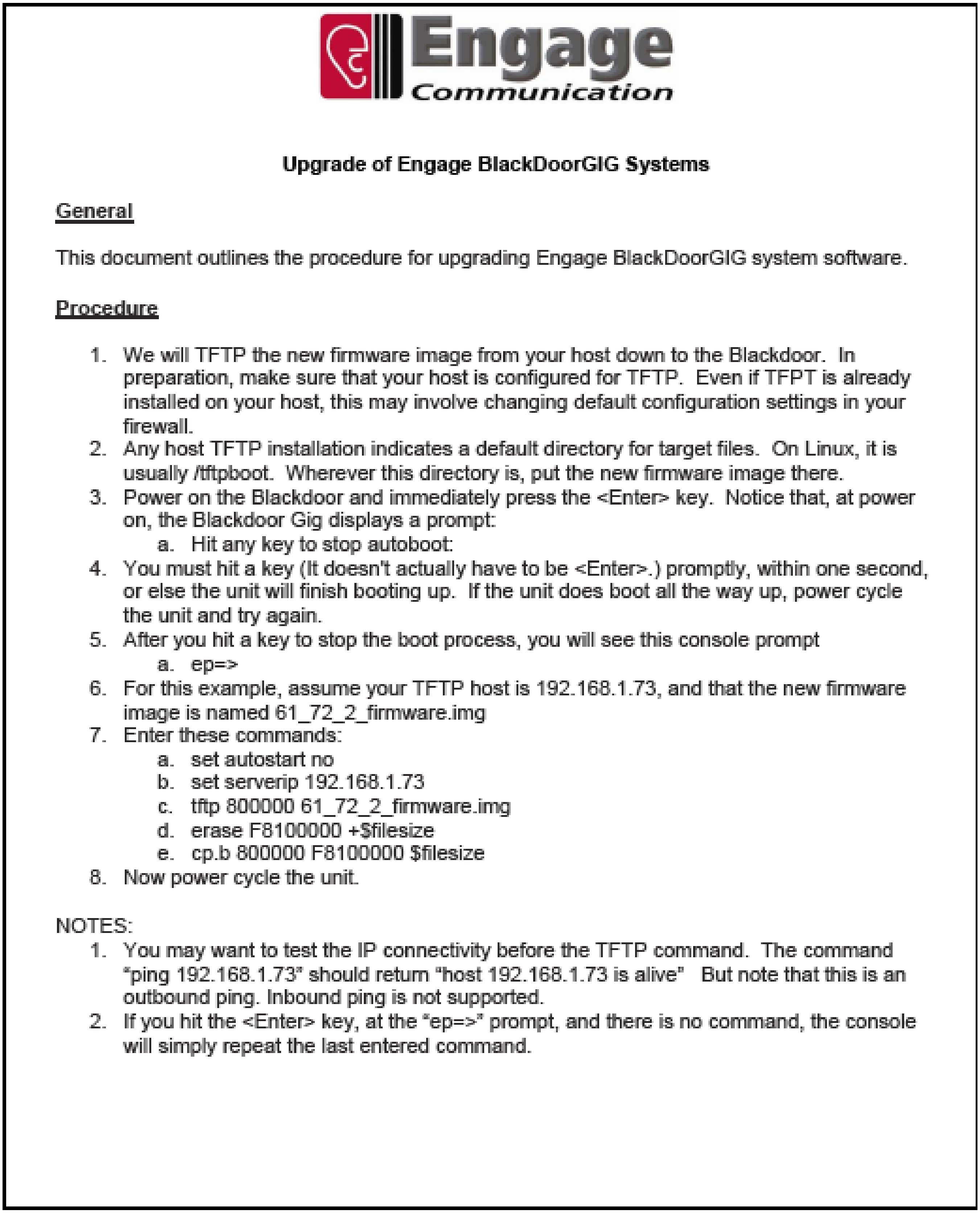
6. Ensure IP connectivity between the Engage unit and the TFTP server by pinging from one to the other. Firewall software on the TFTP server may need to be disabled to permit TFTP sessions initiated from the Engage unit.

7. Upgrade by issuing the command ***upgrade {tftp server addr} {upgrade filename}***

   a. Example: ***upgrade 192.168.1.1 26_72_82_upgrade.upg***

8. Notes:
   a. When the upgrade is complete, the Engage unit will reboot, causing a Telnet connection to drop. If this does occur, simply re-establish the Telnet connection.
   b. Upgrades which enable optional features (additional Ports, Compression, Protector, etc.) cause the Engage unit to revert to Base firmware. Any system software upgrades must be re-installed.

Table 1 - Engage BlackDoor Upgrade Instructions



Engage Communication

Upgrade of Engage BlackDoorGIG Systems

General

This document outlines the procedure for upgrading Engage BlackDoorGIG system software.

Procedure

1. We will TFTP the new firmware image from your host down to the Blackdoor. In preparation, make sure that your host is configured for TFTP. Even if TFPT is already installed on your host, this may involve changing default configuration settings in your firewall.
2. Any host TFTP installation indicates a default directory for target files. On Linux, it is usually /tftpboot. Wherever this directory is, put the new firmware image there.
3. Power on the Blackdoor and immediately press the <Enter> key. Notice that, at power on, the Blackdoor Gig displays a prompt:
   a. Hit any key to stop autoboot:
4. You must hit a key (It doesn't actually have to be <Enter>.) promptly, within one second, or else the unit will finish booting up. If the unit does boot all the way up, power cycle the unit and try again.
5. After you hit a key to stop the boot process, you will see this console prompt
   a. ep=>
6. For this example, assume your TFTP host is 192.168.1.73, and that the new firmware image is named 61_72_2_firmware.img
7. Enter these commands:
   a. set autostart no
   b. set serverip 192.168.1.73
   c. tftp 800000 61_72_2_firmware.img
   d. erase F8100000 +$filesize
   e. cp.b 800000 F8100000 $filesize
8. Now power cycle the unit.

NOTES:

1. You may want to test the IP connectivity before the TFTP command. The command "ping 192.168.1.73" should return "host 192.168.1.73 is alive" But note that this is an outbound ping. Inbound ping is not supported.
2. If you hit the <Enter> key, at the "ep=>" prompt, and there is no command, the console will simply repeat the last entered command.

Table 2 - Engage BlackDoorGIG Upgrade Instructions

Glossary

Terms and Concepts

Before using the Engage Black•Door, 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.

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.

TCP/IP Networking Terms

FTP

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.

Telnet

The TCP/IP standard protocol for remote terminal connection service. A user can Telnet 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, telnet and FTP servers.

Communication Link Definitions

Synchronous Serial Interfaces

A serial interface between two devices which provides for bi-directional data transfer as well as clocking. One device, the DCE, provides the transmit and the receive timing to the second device, the DTE.

Data Communication Equipment (DCE)

This interfaces to the communication service’s transmission/reception medium, and includes T1 Voice/Data Multiplexors, 64/56 Kilobit DSU/CSU's, and Fiber Optic Modems. The DCE provides the transmit and receive data pathways, along with their synchronous clocking signals, which are used by the Engage Router’s DTE interface for full duplex communication between the remotely interconnected networks.

Data Terminal Equipment (DTE)

This equipment, such as an Engage Router, attaches to the terminal side of Data Communication Equipment.

Data Carrier Detect (DCD)

A signal that indicates to the DTE that the DCE is receiving a signal from a remote DCE.

Data Terminal Ready (DTR)

Prepares the DCE to be connected to the phone line, then the connection can be established by dialing. Enables the DCE to answer an incoming call on a switched line.