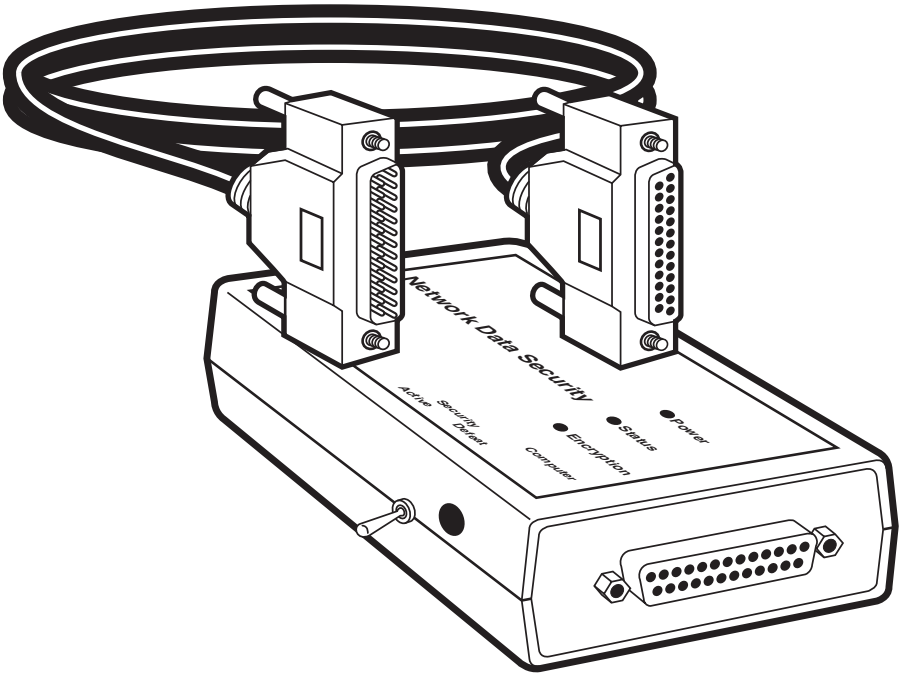
BLACK BOX®
NETWORK SERVICES

NOVEMBER 1994
AC431A

Network Data Security



CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S. 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENT

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an experienced radio/TV technician for help.

Caution:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Contents

Warning!

Because of their implementation of the DES (Data Encryption Standard) encryption algorithm, export of Network Data Security devices is restricted. Export outside the United States is strictly prohibited without prior authorization by the appropriate Federal Government agencies. Export of Network Data Security is governed by the U.S. Department of State under the International Traffic in Arms Regulations.

1. Specifications

Authorization Programming — Single connection of two Network Data Security units, internal handshakes and automatic proprietary authorization protocol exchange. One-Way or Two-Way authorization determines which can *initiate* session connection.

Authorized Connections — After modems connect, Network Data Security units establish authorized identification based on previously stored table information. If unauthorized, modems receive hang-up commands.

Session Setup Time — Less than 1 second

Real Time Encryption Speed — >1 Mbps

Data Encryption Method — DES, plus multiple levels of algorithms, record masking, and cipher-block chaining

Key Generation — Automatic, based on numerous coefficients and internal factors unique to each pair. Key generation occurs independently within each Network Data Security and is never transmitted. Weak keys are automatically detected and re-generated.

Connectors — DB25, 25-pin RS-232, 1-M, 1-F

Active Pins During Modem Session — 1–8, 20, 22, both ACTIVE and DEFEAT modes

Cable — 24-inch RS-232, two 25-pin (DB25) connectors, one male and one female; straight-through wiring, shielded

SECURITY Switch, Programming — *Switch Position as of disconnect*:

Both ACTIVE: Two-Way Authorization

One ACTIVE, one DEFEAT: DEFEAT Network Data Security can initiate a session to other (ACTIVE) Network Data Security

Both DEFEAT: Authorizations between those two Network Data Security units are removed

SECURITY Switch, Session —

ACTIVE: Unit in full operation

DEFEAT: Unit in standby, simple passthrough of all data and RTS/CTS

Modem Control Commands Passed — All "AT" modem commands are passed without encryption. Request To Send (RTS) and Clear To Send (CTS) are passed between DTE (computer) and DCE (modem).

Serial Speed — 300 bps to 38,400 bps, automatic detect

System Throughput Speed — The benefit, if any, of data compression performed by modems is reduced when using encryption. Computer-to-modem serial speeds of 38,400 bps, or even 19,200 bps, should enable V.32 bis modems to operate at maximum speed (14,400 bps).

Authorized Address Storage Capacity — Maximum 500 valid Network Data Security IDs

Microprocessor — 16 bit, RISC, on-board ROM and RAM, DUARTs, anti-tamper firmware

Memory — Additional SRAM, backed-up by lithium battery when external power is not present

MTBF — 720,000 hours of continuous operation

Operating Temperature — 32° to 122°F (0° to 50°C)

Internal Power — Lithium battery, 5 year, active only when external power is removed

External Power — Transformer, output 9 VDC, 300 mA

Tamper Resistance — Auto-zero uP firmware, polyurethane potting, total encryption of all external signals and handshakes

Size — 4.9"H x 2.8"W x 1.8"D (12.5 x 7.1 x 4.6 cm)

Weight — 11 oz. (311.8 g)

2. Introduction

2.1 What's Included

(1) Data Network Security

(1) 1-foot (0.3-m) Serial Cable

(1) Power Transformer

This User's Manual

2.2 Overview

Network Data Security provides effective security against unauthorized access to your valuable computing assets while maintaining full, simple dialup capabilities.

Network Data Security enhances the security of modem access and dialup connections. A computing resource can be accessible through a modem while protected from unauthorized access by Network Data Security. Network Data Security units are initially programmed to establish which nodes are to be allowed access.

Installed between the computer and modem, Network Data Security intercepts all incoming access attempts and authenticates the calling node before allowing connection to the protected computer, host, server, or network.

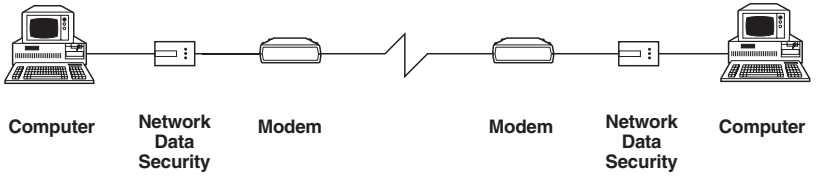


Figure 2-1. Network Data Security installs between the serial port of a computer and a modem.

Network Data Security units are programmed to allow authorized communications between them by simply plugging the units together, one at a time. After a multilevel handshake occurs, each device has stored information about the other, enabling secure authorizations to be established without transmitting any information which could cause compromise.

Once an authorized communications session has been established, a unique DES base-key and cipher vector are generated by each Network Data Security and all transmitted data is encrypted, in real time.

Network Data Security has been designed with the assumption that all communications are subject to unwelcome monitoring. Therefore, all handshakes and data exchanges are manipulated by multiple algorithms and encrypted to preclude any node-specific information from being monitored and decoded.

2.2.1 Authorization Programming

During the initial authorization programming, information regarding each node is embedded within a larger record, masked, encrypted, and then exchanged with the other Network Data Security. After the information is decoded, certain factors and coefficients are stored in the authorization tables unique only to that particular authorized Network Data Security pair.

2.2.2 Authentication and Encryption

When two authorized Network Data Security units are connected via modems, their multilevel handshaking protocol first establishes that each is authorized. Then, using some of the information generated and stored *during the initial programming*, both generate a unique encryption environment for the session. Since the keys and ciphers are never available to the user or transmitted between the two nodes, security is maintained.

3. Authorization Programming

Network Data Security installs between your computer and modem in the serial line. Each Network Data Security is programmed by you, authorizing it to connect with other Network Data Security units.

Network Data Security allows only authorized nodes to connect. You must first program your Network Data Security with other Network Data Security units to establish authorization. They are then installed and provide automatic authentication and data encryption.

To establish authorization:

1) Plug in both power supplies and attach one to each Network Data Security, in the receptacle on the side as shown in Figure 3-1. All three indicators (Power, Status, and Encryption) will go on for 2 or 3 seconds while an automatic self-test is performed, and then the Power indicator will remain lit. (For more information on the indicators see Table 3-1 on page 11.)

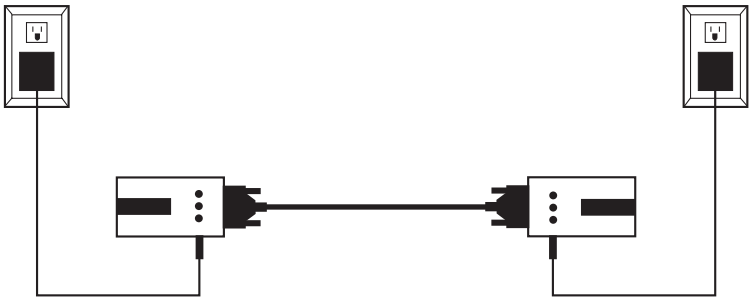


Figure 3-1. Power supplies.

2) If each Network Data Security is to be authorized to initiate a session with the other (two-way authorization), move both SECURITY switches to ACTIVE.

3) If only one Network Data Security will be authorized to initiate a session with the other (one-way authorization), move the authorized *caller's* SECURITY switch to DEFEAT and the authorized *receiver's* SECURITY switch to ACTIVE.

4) Plug each Network Data Security into the supplied cable (see Figure 3-1), so that the COMPUTER connector of one Network Data Security is connected through the cable to the MODEM connector of the other. Which Network Data Security is on the right or left does not matter. The STATUS indicator will go on.

NOTE

The supplied cable is custom-made; other 25-conductor cables can be used, but make certain that all 25 conductors are wired. Network Data Security units employ proprietary communications and handshakes during the programming sequence which use pins that are not part of the EIA Serial RS-232 standard.

If either Network Data Security unit's Authorization Table is full (500+ authorizations), its Status and Encryption lights will blink. In this case, an authorization must be removed before another can be programmed into that Network Data Security.

5) After a few moments, the Encryption indicator will go on. All three lights remain on, indicating completion of the Network Data Security unit's communications and handshakes for Authorization Programming.

6) With the switches correctly positioned, disconnect either Network Data Security from the cable, *with power still applied to both.* If both Status and Encryption lights go off on each Network Data Security when they are disconnected, programming is complete.

The switches can be changed repeatedly while the Network Data Security units are connected. The switch positions *at the time the Network Data Security units are disconnected* determine the final programming configuration for that pair.

If your programming is now complete, deploy or install your Network Data Security units as necessary.

7) To remove authorizations from Network Data Security units, plug both Network Data Security units together, through the cable, with power applied. With both Status and Encryption lights on and *both switches in the DEFEAT position*, disconnect the two Network Data Security units. Any previous authorization (one-way or two-way) of those two Network Data Security units has now been deleted from both.

When authorizations are deleted from a Network Data Security, a memory location is freed up for future programming.

Note that one-way or two-way authorization programming pertains to the *session initiation only*, not to the actual data transfer. Once a valid session is initiated between authorized Network Data Security pairs, standard full-duplex serial communication is supported and available.

Table 3-1. Light sequences during authorization

	Mode	Status Indicator	Encryption Indicator
While Plugged Together	Authorization programming in progress	ON	Fast Blink
	Authorization programming complete	ON	ON
	Authorization programming error	Slow Flash	Slow Flash
	Table full—Will not save	Alt Flash	Alt Flash
Upon Separation	Saved in table—Ready	OFF	OFF

4. Installation

1) Verify that your computer and modem are set up properly and communicating with desired nodes before installing Network Data Security in your system (see Figure 4-1).

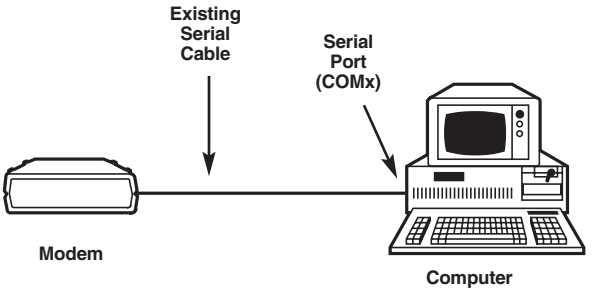


Figure 4-1. Before installing Network Data Security, make sure your system is set up properly.

2) Turn off all power to your computer and modem and unplug all line cords.

3) Remove your existing serial-cable connection from either your modem or your computer. Your choice here will depend upon the physical requirements and layout of your system. Either end will function properly.

4) Install your existing serial cable, Network Data Security, and its new serial cable as shown in Figure 4-2.

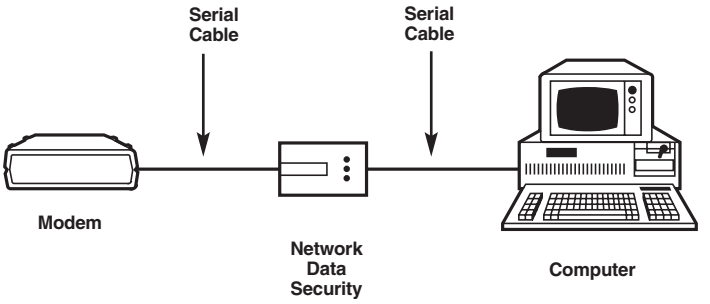


Figure 4-2. Install the Network Data Security.

5) Reconnect power to the modem and the computer.

6) Plug the Network Data Security power supply into a 120-VAC source and insert the connector into the receptacle adjacent to the Network Data Security SECURITY switch. Verify the Power light is on. The indicator sequences are shown in Table 4-1.

7) Place the Network Data Security SECURITY switch in the DEFEAT position.

8) Power on your computer. Load and execute your application software.

9) Re-verify modem operation (non-secure) while the switch remains in the DEFEAT position.

10) Place the Network Data Security SECURITY switch in the ACTIVE position.

11) Initiate a modem connection to a computer with a similarly configured and installed pre-authorized Network Data Security. Verify normal computer/communications operation. Only authorized nodes now are allowed access and all transmitted data is fully encrypted.

Table 4-1. Light sequences during operation

Switch	Mode	Status	Encryption
Defeat	Pass-through, non-secure	Fast Blink	OFF
Active	Modem connected, data carrier present	OFF	ON
Active	Encrypted data communication	OFF	Fast Blink
Active	Cannot authenticate ...hang up	Slow Flash	Slow Flash

5. Operation

1) For secure communications, make certain the SECURITY switch is always in the ACTIVE position. All operation is then automatic. Each node will be authenticated; only authorized nodes will be allowed to connect and all data will be encrypted.

2) Whenever an incoming call is received by your modem, Network Data Security will challenge and authenticate that call. If your Network Data Security does not detect another Network Data Security at the calling node, your modem is instructed to hang up.

3) If your Network Data Security detects another Network Data Security at the calling node but determines that it is not authorized, it will promptly terminate the session and hang up.

   Your computer is unaware of these failed attempts and never "sees" any activity at its COM port.

4) Only if the calling node has an authorized Network Data Security will a connection be allowed. The two computers will then connect and exchange data in an encrypted fashion.

Multilevel Handshaking

When two authorized Network Data Security units are connected via modems, a multilevel handshake occurs, enabling the independent, simultaneous, and secure creation of a unique DES base-key within each Network Data Security. This base-key is never transmitted between the two Network Data Security units and will be used by both to encrypt all transmitted data and to decrypt all received data.

Both computers are then connected to their respective modems through Network Data Security units (see Figure 5-1) and secure data transmission is enabled.

This authentication and key generation process takes less than one second at the start of each communications session.

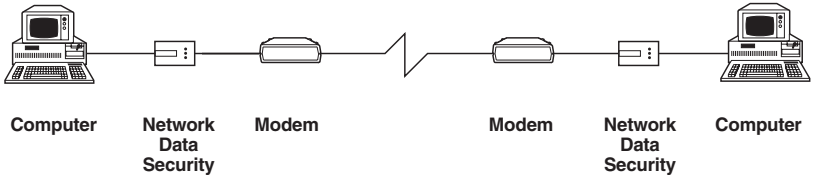


Figure 5-1. Each modem is connected to a separate Network Data Security, which is connected to a computer.

Operation Notes

- During a communication session, all transmitted data is encrypted by the "sending" Network Data Security and decrypted by the "receiving" Network Data Security. This is a two-way capability (both can simultaneously encrypt and decrypt), therefore enabling standard full-duplex serial communications.
- Network Data Security units have automatic baud-rate detection and perform full encryption and decryption while automatically adjusting to any serial baud rate from 300 to 38,400 bits per second.
- During a communication session, standard computer-modem control commands, are recognized in real time and transferred un-encrypted. In addition, hardware flow control (RTS & CTS) is monitored and communicated between DTE and DCE.

NOTE

When accessing public, non-secure systems, such as on-line services or the Internet, move Network Data Security SECURITY switch to the DEFEAT position. With power still present, your Network Data Security now operates as a simple pass-through device with your computer and modem. Remember to switch back to the ACTIVE position when complete or authorized sessions will be unsuccessful.

6. Additional Programming

Your Network Data Security comes with an internal table, in random-access memory (SRAM), for storing authorizations for communications with other Network Data Security units.

Network Data Security supports standard data communication (full-duplex RS-232 serial data communication). Each programmed authorization allows *either one-way authorization only* or *two-way authorization*. During the authorization programming process, this choice is made through the position of the SECURITY switches at the completion of programming.

Each Network Data Security can store authorizations (one-way or two-way) for communication with up to 500 other Network Data Security units.

For client-server applications, you can choose to allow the server to be *called only* by the valid clients (one-way authorization), or you can program two-way authorizations, enabling the server node to initiate the dialup connection with a client.

Either authorized programming configuration would occupy one of the 500 available locations in each Network Data Security's authorization table.

Consider the following programming example:

A host (server) is located at "corporate headquarters" in New York, with branch offices (clients) in Atlanta, Chicago, Los Angeles, and Honolulu (see Figure 6-1).

All four branches are allowed to communicate with New York. Either node in the pairs can initiate the contact.

Honolulu and Los Angeles should each be able to initiate communication with one another, and Honolulu should also be able to initiate contact with Chicago, for regional support in light of the time-zone variations.

NEW YORK
Data Network Security

Call To	*Called By*
Atlanta	Atlanta
Chicago	Chicago
Los Angeles	Los Angeles
Honolulu	Honolulu

ATLANTA
Data Network Security

Call To	*Called By*
New York	New York

CHICAGO
Data Network Security

Call To	*Called By*
New York	New York
	Honolulu

LOS ANGELES
Data Network Security

Call To	*Called By*
New York	New York
Honolulu	Honolulu

HONOLULU
Data Network Security

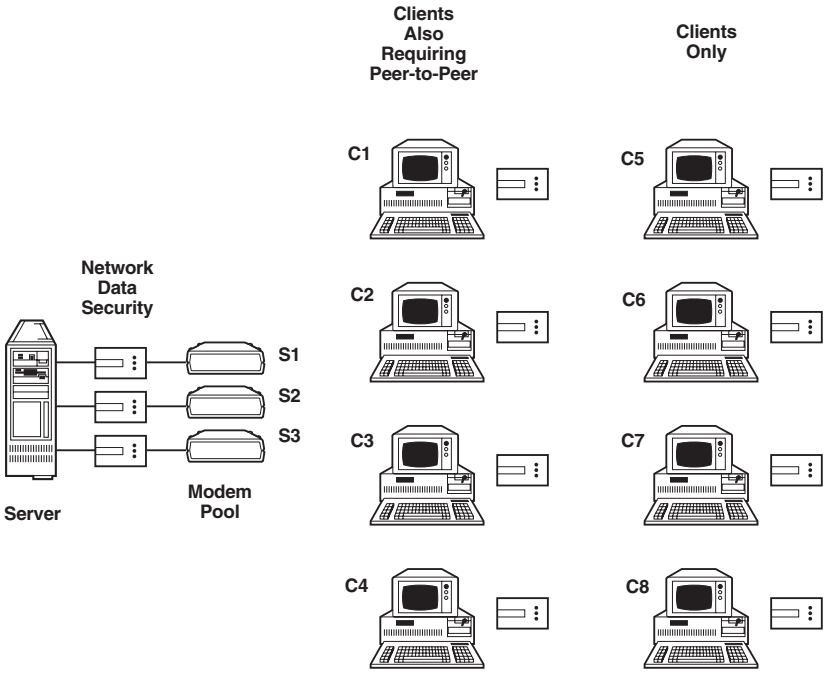
Call To	*Called By*
New York	New York
Los Angeles	Los Angeles
Chicago	

Figure 6-1. The Network Data Security in New York can initiate calls to, and receive calls from, all other Network Data Security units (two-way authorizations) in the branch offices. Los Angeles and Honolulu can communicate, with either one able to initiate the call to the other (two-way authorization). Honolulu can initiate a call to Chicago, but Chicago can't initiate a call to Honolulu (one-way authorization).

7. Configuration

As an illustrative example, consider a Network Data Security configuration within a client-server environment with eight valid clients and a server with three inbound ports accessible through dialup modems (see the figure below).

For this example, we will also presume a particular subset of the clients (four) also need their own intra-group peer-to-peer connection capabilities.



To accomplish this configuration, each Network Data Security is individually programmed with every other Network Data Security with which it will communicate.

The Server-node Network Data Security units (S1–S3), will be programmed with all valid clients, C1–C8. In addition, each Network Data Security in the subgroup C1–C4 will also be programmed with each other.

For more complex configurations, consider generating an X–Y programming table, showing each Network Data Security's relationship to the others, to facilitate the task. The following table, showing the required programming for each Network Data Security (S1–C8) in this example, can be built upon for your particular configuration.

		All Client Nodes							
		C1	C2	C3	C4	C5	C6	C7	C8
All Server and Peer-Capable Nodes	S1	1	1	1	1	1	1	1	1
	S2	1	1	1	1	1	1	1	1
	S3	1	1	1	1	1	1	1	1
	C1	NA	2	2	2	NA	NA	NA	NA
	C2	2	NA	2	2	NA	NA	NA	NA
	C3	2	2	NA	2	NA	NA	NA	NA
	C4	2	2	2	NA	NA	NA	NA	NA

NA = No programming; no connection allowed

1 = One-way authorization programming

2 = Two-way authorization programming

Table 7-1. All Clients (C1–C8) can call the Server, connecting with any node (S1–S3). C1–C4 can all connect with each other. C5–C8 can call no one but the Server and can receive no calls at all

8. Growth and Management

Available dialup connections within your system may be broad and varied. Your desired configuration will determine the required authorization programming for the Network Data Security units in your system.

While Network Data Security supports peer-to-peer and client-server configurations, it is actually the authorization programming you perform on your own Network Data Security units that allows all types of configurations and network topologies.

8.1 Peer-to-Peer

In its simplest configuration, Network Data Security can be programmed to support a peer-to-peer system. For example, if eight peers are to be included in the system, all of which require dialup access to one another, all eight Network Data Security units would be programmed by plugging each into the other seven, with all switches in the ACTIVE position during programming.

Each Network Data Security would then store valid IDs for *sending to* and *receiving from* each of the other seven.

8.2 Client-Server

Multiple servers and large, varying populations of clients can be configured and supported through Network Data Security programming.

In its simplest configuration, consider the example of one server node accessible by five remote clients. Here, program the *server* Network Data Security by plugging it, individually, into each of the five *client* Network Data Security units. The position of the switches will determine which end can initiate the session(s).

For multiple inbound lines into the server, several modems are used. Include a single Network Data Security at each inbound node, between the server hardware and the modem. A typical system may have four inbound lines on the server with 20 remote clients. Program all 20 client Network Data Security units *with each* of the four server Network Data Security units, creating a total combination of 80 authorized pairs out of the 24 Network Data Security units.

A subset of clients in a client-server configuration could also be authorized to communicate with one another, in a "secondary peer-to-peer" configuration, with additional authorization programming as described in **Section 8.1**. See **Chapter 9** for more information.

9. Application Hints

In peer-to-peer operation, plan for extra Network Data Security units to accommodate future growth. If you have 16 peer nodes, for example, consider programming extra Network Data Security units and securely storing them. Then, when a new employee is brought in or a temporary contractor is retained on a project, a properly programmed Network Data Security is readily available.

In a client-server configuration, extra client nodes can be preprogrammed and securely stored for future use, thus preventing the periodic need to access each server node for new programming.

It is more critical to consider programming extra Network Data Security units at the server nodes, facilitating simple system growth or replacement without having to access or recall remote/client nodes.

After programming your Network Data Security units, installation can be accomplished with minimal or zero system downtime. Simply install your Network Data Security units, one node at a time, and immediately apply power to them with the SECURITY switch in the DEFEAT position. This provides "ordinary" operation of your system, as if Network Data Security wasn't there. Allow plenty of time for all your users to similarly install their Network Data Security units at all nodes. Then communicate to your users the "go live" time, at which point you will move all your switches to ACTIVE mode.

If two nodes are actively communicating, "in the clear," at the time their SECURITY switches are moved to ACTIVE, the two Network Data Security units, if authorized, will establish a secure connection, create their unique DES base-keys, and resume the session fully secure and encrypted. If only one switch is moved to ACTIVE, or if the two Network Data Security units are not authorized, the session will time out and communication will be terminated.

For enhanced security in larger environments, periodic audits can be performed wherein a computer, with a valid authorized Network Data Security, is programmed to automatically call your list of phone numbers or extensions. This will verify the Network Data Security units are properly installed and the SECURITY switches in the ACTIVE position. This can help encourage users to remember to return their switches to ACTIVE after completing non-secure sessions with public databases, services, etc.

10. Troubleshooting

10.1 Symptoms and Solutions

No Power Indicator

Check that the Network Data Security's power transformer is plugged into a 120-VAC source and that the power cable is properly plugged into the Network Data Security.

No Status Indicator During Authorization Programming

Verify that both Network Data Security units' power cables are properly installed. Verify that the supplied cable is properly connected to both Network Data Security units, one end to the MODEM connector, and the other to the COMPUTER connector.

NOTE

The supplied cable is custom-made; other 25-conductor cables can be used, but make certain all 25 conductors are wired. Network Data Security units employ proprietary communications and handshakes during the programming sequence which may use pins otherwise excluded by the EIA Serial RS-232 standard.

Cannot Program Authorization—Table Full

If the status and Encryption indicators alternately flash when the two Network Data Security units are separated, the authorization table is full. See **Chapter 3** for authorization removals.

Modems Will Not Connect

Place both SECURITY switches in the DEFEAT position and verify that modems will connect properly. If not, perform necessary remedies as appropriate for your application software.

Modems Connect, But Session Fails

Verify that the two Network Data Security units are authorized. If the Status and Encryption indicators flash after the modems connect, your Network Data Security cannot authenticate the other node.

Verify that the SECURITY switch is in the ACTIVE position on both Network Data Security units.

Verify that power is properly applied to both Network Data Security units and all cables are securely fastened.

10.2 Calling Black Box

If you determine that your Network Data Security is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box Technical Support at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

10.3 Shipping and Packaging

If you need to transport or ship your Network Data Security:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the Network Data Security for repair, make sure you include its power supply. If you are returning the unit, make sure you include this manual as well. Before you ship, contact Black Box to get a Return Materials Authorization (RMA) number.

Glossary

Authentication—The valid recognition of an authorized Network Data Security pair connected through modems. Authenticity is assured because only an authorized sender can produce data that will be decrypted properly by the receiver with the unique shared key. Authentication occurs at the beginning of each authorized session.

Authorization—A valid Network Data Security ID (specific numerical information unique to a Network Data Security) stored in the internal table (memory) of another Network Data Security, enabling communication.

Authorization Programming—The creation of authorizations within Network Data Security units through the process of plugging them together with various switch settings (see **Chapter 5**).

Authorized Pair—Two Network Data Security units that contain each other's ID within their authorized tables, as a result of authorization programming.

Authorized Session—The communications session enabled by the connection, and authentication, of two authorized Network Data Security units through modems.

Ciphertext—Transmitted or stored data in its encrypted form, which has been encrypted using a cipher, translation table, or an algorithm and a key. Ciphertext requires the proper key and algorithms for decryption (conversion back to cleartext).

Cleartext—Original data or message readable in a common format, such as printed, ASCII, binary, etc. Also called plaintext.

Encryption—Using a cipher, table, or mathematical algorithm to scramble an original message or data (cleartext) into something unreadable (ciphertext). Most encryption algorithms or methods are fixed and will rely on a key to provide security for a particular session.

Key—Numerical information that interacts with encryption and decryption algorithms, enabling specific and secure conversion from cleartext to ciphertext and back again.

Key Management—The controlled creation, storage, distribution, and updating of keys, both public and private, used in encryption and decryption. Secret, or private, keys generally require management in a secure fashion, which makes key management a primary issue in information security.

One-Way Authorization—A configuration of an authorized pair in which one specific Network Data Security can only initiate the session (dial out) and the other Network Data Security can only receive the call.

Private Key—In encryption a key, usually secret, that is used to encrypt data by the sender, and the same key is used to decrypt the data by the receiver.

Public Key—In encryption, a key available to anyone (public), that is used to encrypt data destined for an individual associated with that public key. Decryption is then accomplished by the receiving individual, using a different, private key known only to the owner. Also known as asymmetric key.

Two-Way Authorization—A configuration of an authorized pair in which either Network Data Security can initiate the session by dialing out to the other.

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746