



Datacryptor™ 64F

Frame Relay Encryption Device

- End-to-end frame relay security
- Supports up to 992 PVCs at speeds up to 128 Kbps
- Handles encrypted and unencrypted PVCs simultaneously
- Secure key management system
- SNMP management
- Configurable from PC or unit front panel
- Automatic diagnostic testing
- User-selectable interfaces (RS-232, V.35, V.11)
- Extensive alarm reporting
- Battery-backed memory

Datacryptor™ 64F

Frame Relay Encryption Device

Frame Relay Encryption Device Provides Secure Communications Over Public Networks

As migration to frame relay continues to expand, more and more people are discovering the advantages of frame relay network services — less expense, fewer networking delays, and higher throughput. However, since frame relay is a public service, information transmitted over frame relay networks is vulnerable to disclosure and attack. The Racal Datacryptor™ 64F (DC 64F) frame relay encryption device is designed to provide secure communications over frame relay networks on an end-to-end basis — effectively creating a virtual private network within the public network.

End-to-end encryption protects your data from source to destination by encrypting prior to transmission and decrypting at final destination. Only data fields within frames are encrypted, while address and control information remain “in the clear” for routing through the frame relay network. In a typical installation, the DC 64F connects between a frame relay DTE device such as the Racal FastFrame™ 200 FRAD (Frame Relay Access Device) or a frame relay router, and a DCE at end points of the network.

Supports 992 PVCs at Speeds up to 128 Kbps

The DC 64F supports a maximum of 992 PVCs (Permanent Virtual Circuits) at speeds up to 128 Kbps, allowing your network to expand without constant device upgrades or replacement. The DC 64F protects each PVC with a unique crypto-key for optimum security. Frame sizes up to 4096 bytes are supported for additional flexibility.

Handles Encrypted and Unencrypted PVCs Simultaneously

The DC 64F can be configured to transmit encrypted (secure) or unencrypted (clear) data on an individual PVC basis. This feature allows the DC 64F to communicate with both secured and unsecured sites. When a connection is made to an unsecured site (no DC 64F present), data is transmitted unencrypted. Alternatively, when a connection is made to a site equipped with a DC 64F, data is transmitted encrypted.

Secure Key Management System

Ensuring the highest level of security possible, the DC 64F performs key management in accordance with the American National Standards Institute (ANSI) X9.17 Key Management Standard and National Institute of Standards and Technology (NIST) FIPS 140-1 for use in government and commercial applications.

The DC 64F is compatible with the Racal Datacryptor Key Management Center, which provides centralized key management and control for your entire network of encryption devices. When used with the Key Center, a 3-key hierarchy is used for key management. When used without the Key Center, a 2-key hierarchy is used.

The DC 64F can be configured so that key changes are performed on an automatic, pre-timed basis without operator intervention. Cryptographic service messages transmitted between encryptors or from the Key Center are authenticated using a secure protocol ensuring service message integrity.

SNMP Management

The DC 64F supports industry-standard SNMP (Simple Network Management Protocol), enabling you to monitor unit status using any SNMP-based management application. With an SNMP manager at a central location, you can communicate inband through the frame relay network with all DC 64F units. The DC 64F responds to SNMP Gets, providing information on unit identity, configuration, connections, and current status. It also issues Traps to alert you to network events and alarms.

DES Encryption

The DC 64F uses the Data Encryption Standard (DES) algorithm to encrypt and decrypt the data portion of each frame. Data is encrypted in the 8-bit cipher feedback mode for automatic resynchronization without operator intervention at speeds up to 128 Kbps.

PC Connection/Key Center Port

The DC 64F rear panel includes a port for connection to a PC with a terminal emulator (or VT-type terminal) or the Key Center. Connecting to a PC/terminal allows you to configure the unit, view up to 100 logged events, verify unit status, etc.

Connecting to the Key Center allows one or more designated DC 64F units to communicate with the Key Center and forward commands to other DC 64F units within the frame relay network. These commands include key checks and changes, mode checks and changes, diagnostic testing, etc.

Front Panel Programmability

The front panel has an LCD screen and nine soft-touch controls, allowing full and easy configuration of the unit. By simply pressing a few buttons and viewing the LCD, you can control key management, unit configuration, diagnostic testing, and operating mode selection. A 32-character display provides valuable information on unit status including operating mode, active alarms or advisories, and the date and time of important unit events.

Diagnostic Testing

Diagnostic testing helps maintain trouble-free operation. DC 64F tests can be initiated in several ways: automatically on power-up, from the front panel, or in response to Key Center commands. Several tests are available: ROM/RAM, S-box, key parity, cipher feedback, checkword, and memory test.

Strap Selectable Interfaces

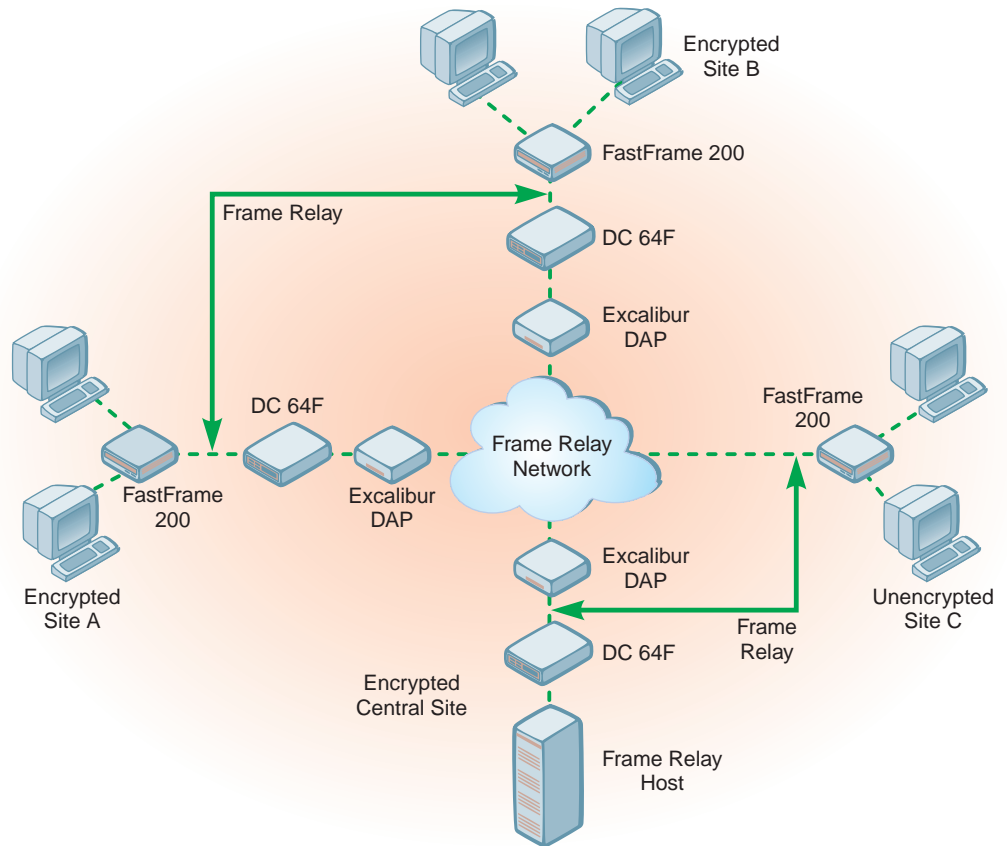
For application flexibility, the DC 64F is equipped with RS-232, V.35, and V.11 electrical interfaces. An internal strap allows you to easily change the interface to satisfy your application. The unit is equipped with standard DB-25 connectors for both DTE and DCE connections.

Alarm Reporting

The DC 64F alerts you to unit failures by issuing a wide variety of alarms. An alarm causes the front panel LED to light, sends an alarm message to the LCD, and activates the alarm relay contact on the rear panel. The alarm relay allows connection of an external alarm indication device for local alerting, or remote alarm reporting to a Racal Key Center or CMS™ network management system.

Battery-Backed Memory

For added security, the DC 64F's internal memory is protected by Lithium battery backup. This feature saves the current keys, system parameters, and time-of-day clock if the unit is unplugged from the power source or if a power failure occurs. Keys and system parameters are retained in memory for up to 10 years.



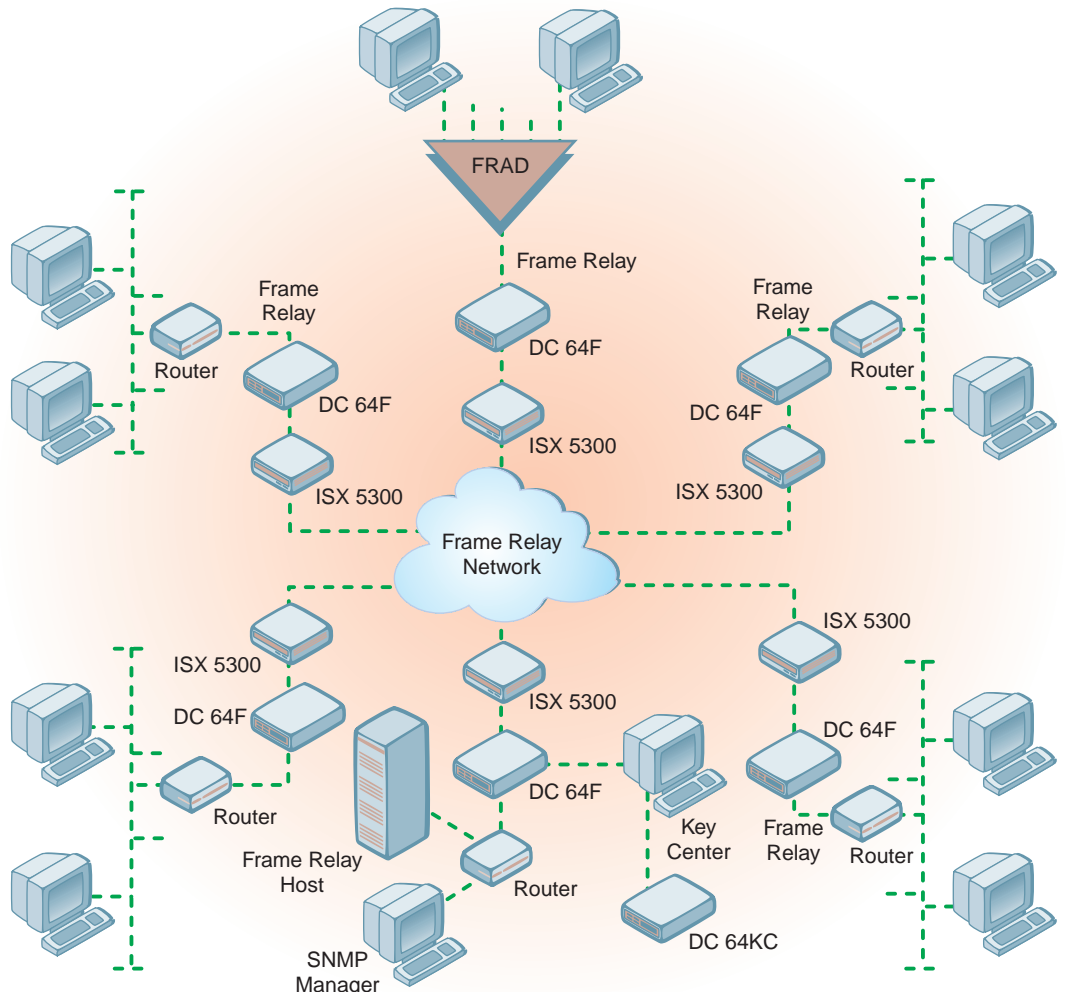
DC 64F Virtual Private Network with Encrypted and Unencrypted Sites

Physical Security

Housed in a wraparound metal enclosure, the DC 64F is designed to restrict unauthorized internal access. An anti-tamper switch activates if an attempt is made to remove the cover. Upon activation, all stored keys are automatically erased and operating parameters are reset to their default values.

Two pick-resistant locks are located on the DC 64F front panel. Setting the locks in the lockout position prevents unauthorized personnel from: reconfiguring operating parameters, loading or changing keys, checking current keys in use, changing operating modes, testing the unit, viewing log displays, and viewing automatic key change parameter settings.

An optional desktop assembly allows secure mounting of the DC 64F to a flat surface such as a table or shelf, preventing unauthorized personnel from removing the unit from its designated location.



Secure LAN-to-LAN Communications with Centralized Key Management and SNMP Manager

Datacryptor 64F

technical specifications

Data Transfer Rates	Up to 128 Kbps, full duplex, frame relay
Encryption Method	DES Algorithm, 8-bit cipher feedback mode
Maximum PVCs Supported	Up to 992 PVCs, individually configurable for encrypted or unencrypted data transmission
Maximum Packet Size	4096 Bytes
Synchronization	Automatic
Operating Modes	Secure (data is encrypted), Bypass (data remains unencrypted), Standby (no data transmitted)
Key Management	ANSI X9.17 Three Key Hierarchy (Key Center) or Two Key Hierarchy (no Key Center)
Diagnostics	S-box, parity check, loopback, ROM/RAM, memory test, key checks, operating mode checks, unattended remote diagnostics (with Key Center)
Alarms	Key parity error, expiration of keys in key list, loss of memory due to physical tampering, encryption/decryption failure, lock failure, and power failure (activates relay contact only).
DTE Interface	RS-232, V.35, X.21/V.11; strap selectable; uses DB-25 type connector
DCE Interface	RS-232, V.35, X.21/V.11; strap selectable; uses DB-25 type connector
Power Requirements	92-240 VAC, 47-65 Hz
Power Consumption	19 watts
Operating Temperature	32° to 122° F (0 to 50° C)
Physical Specifications	Height 2.7" (6.9 cm) Width 8.0" (20.3 cm) Depth 16.2" (41.1 cm) Weight 8.0 lbs. (3.64 kg)

Our policy of continuous development may cause the information and specifications contained herein to change without notice.

Racal, Racal-Datacom, Datacryptor, FastFrame, and CMS are trademarks of Racal Electronics Plc. All other logos and product names are trademarks or registered trademarks of their respective companies.

©1996 Racal-Datacom, Inc. All rights reserved. Printed in U.S.A.

3C1462 10/96 - 0874

Racal Data Group *Access to multimedia information networks*

RACAL

Americas
1601 North Harrison Parkway
P.O. Box 407044
Fort Lauderdale, Florida 33340-7044, U.S.A.
Telephone: 1-800-RACAL-55
Telephone: 1-770-279-9564 (outside U.S.)
Fax: 1-954-846-4942

Europe/Middle East/Africa
Landata House, Station Road
Hook, Hampshire, RG27, 9JF, England
Telephone: 44-1256-763911
Fax: 44-1256-764717

Asia/Pacific
Sun House 10th Floor
181 Des Voeux Road Central
Hong Kong
Telephone: 852-2541-2668
Fax: 852-2541-2823

Internet: <http://www.racal.com/rdg>

