General DataComm
The Best Connections in the Business

SteadFast Solutions

Securing Your Network Assets

Network security is a high priority for any enterprise and information network that stores or provides access to critical assets.

General DataComm's SpectraComm family of systems and network devices support SteadFast Security® solutions that protect your network assets from attacks by illegal users and malicious hackers. GDC systems and products are designed with rigorous security solutions that meet the requirements of mission-critical network applications, such as service provisioning, banking and financial communication, transportation and governmental agencies.

GDC's proven "telco-tough" SpectraComm SteadFast Security® solutions give network administrators a suite of protection options for their large or small network environments, including Security, Authentication, Encryption and Disaster Recovery. SteadFast Security® solutions protect network assets by blocking disruption of service due to data theft, data corruption, illegal intrusions, shutdowns, line failure and component failure.

Fig. 1: SpectraComm SteadFast solutions offer cost-effective security and authentication strategies for your network requirements.

LAN RADIUS

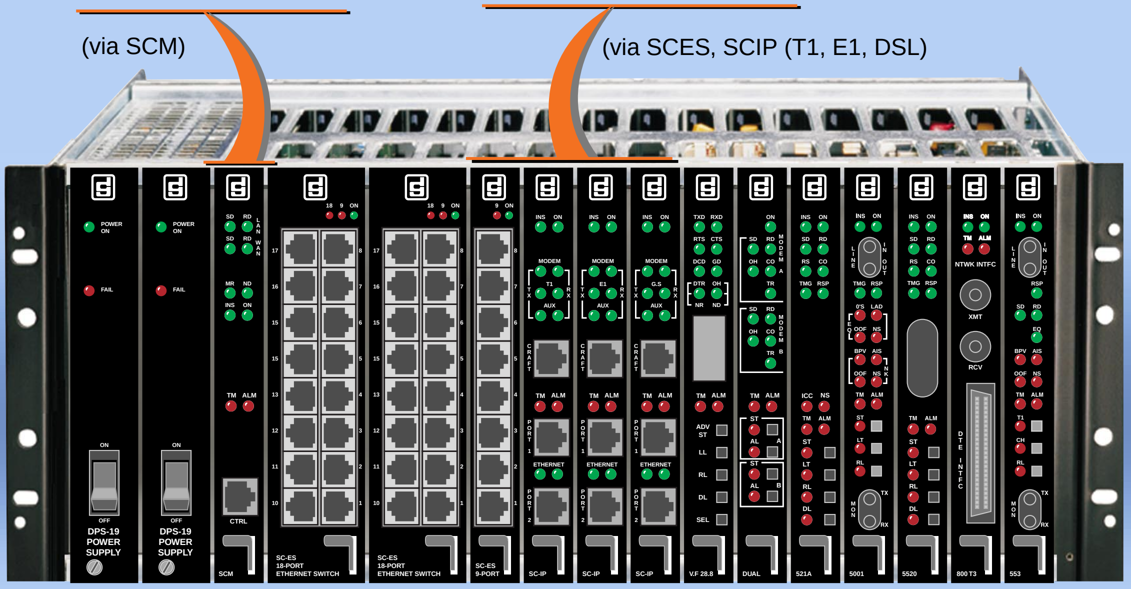
Authentication and Accounting

(via SCM)

IP Password Security

TACACS+ Authentication

(via SCES, SCIP (T1, E1, DSL)



(via SCES)

Ethernet Security

(via SpectraComm V.34 Modems)

RADIUS Authentication and Accounting w/Challenge

AES Encryption

Secure Access Modem

Handshake Security

On-line Password Security

Callback Security

DISASTER RECOVERY

Safe T1 Redundancy...........	via SC 5001
Management Redundancy..	via SCM
Power Redundancy.............	via SC Shelf
RADIUS Redundancy	via SCM/V.34 modems
Remote Management	via SCM
Dial Back-Up	via V.34 modems
Safe LAN-X	via SCIP
Out-of-Band Management	

SteadFast V.34 Modems

For dial-up applications, GDC's SteadFast V.34 modems can employ one or more SteadFast solution to meet your network's security requirements:

- SteadFast Handshake Security (transparent to users) (uses a cell password stored in the modem)
- SteadFast On-line Password security (uses cell passwords stored in the modem)
- SteadFast Callback security
- RADIUS Authentication and Accounting with Challenge (via V.34 modem, SCM and RADIUS server)
- AES Encryption (transparent to users) (uses encryption key stored in the modem)

SteadFast Handshake Security

GDC's exclusive Handshake Security is built into SpectraComm V.34 modems for multi-level security protection. As part of its handshake, the initiating GDC modem sends the receiving GDC modem a cell password previously stored in both modems. After more than ten years in the field, SteadFast Handshake Security has never been breached!

In applications that require authentication, V.34 modems can be configured for SteadFast Handshake as fail-safe security when RADIUS or TACACS+ servers are out-of-service/unreachable. This eliminates truck-rolls and restores service quickly, saving time and capital expense.

On-line Password Security

When a remote user initiates a call to a GDC V.34 answering modem configured for On-line Security, the modems handshake and the caller is prompted to enter a valid cell password within 20 seconds. If the answering modem can make a match with one of the ten stored cell passwords, the call is directly admitted. If not, the call is disconnected.

Adding SteadFast Callback Security

After an online password is accepted, Callback Security causes the V.34 modem to disconnect and call back the modem that placed the original call. The V.34 modem can be configured to use stored callback phone numbers, to prompt for callback phone number, or to deny a callback.

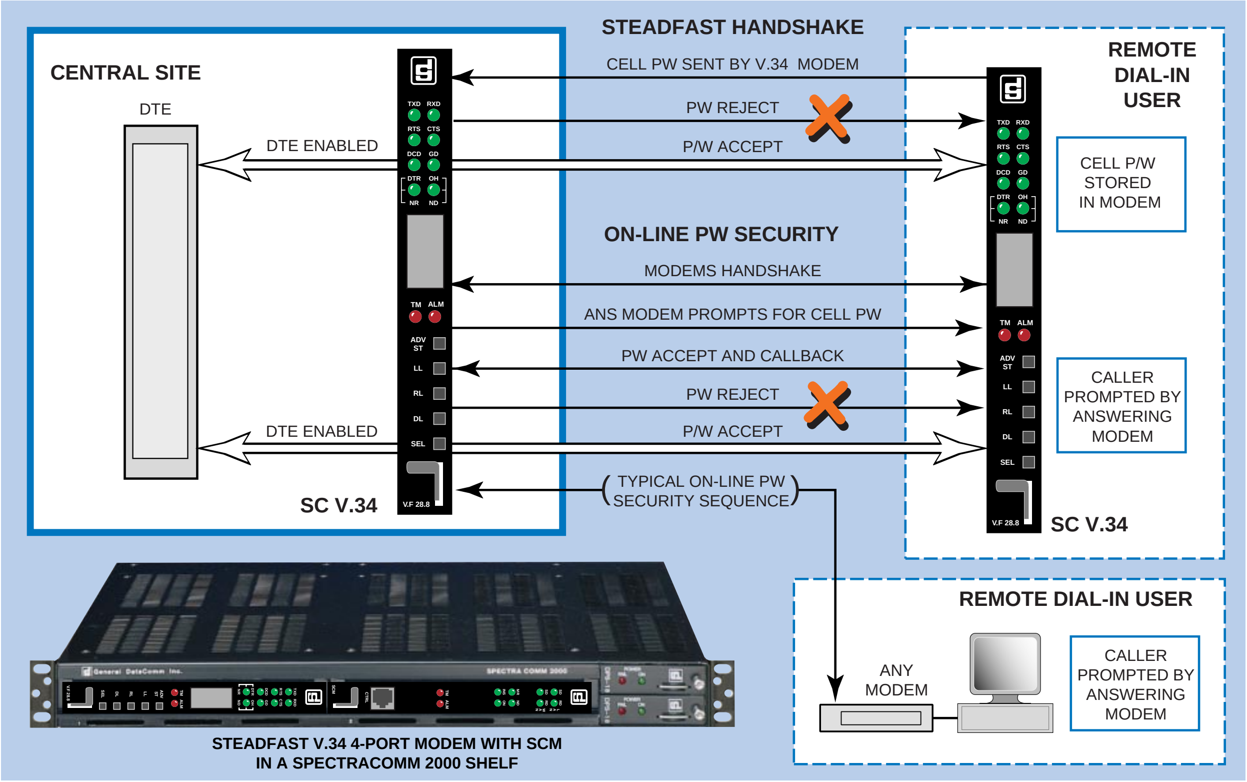
Adding Roving Callback Security

After an online password is accepted, Roving Callback security causes the V.34 modem to prompt the caller for a callback phone number. Once the phone number is supplied, the answering modem disconnects the call and then places a return call using that number.

Adding Cell Callback Security

After an online password is accepted, Cell Callback causes the V.34 modem to prompt the caller for a memory cell number. Once the cell number is supplied, the V.34 modem disconnects the call and then places a return call using the phone number stored in that memory cell.

Fig. 2: Access to central site protected by SteadFast Handshake and/or On-line Password Security.


CENTRAL SITE
DTE
DTE ENABLED
DTE ENABLED
SC V.34
STEADFAST HANDSHAKE
CELL PW SENT BY V.34 MODEM
PW REJECT
P/W ACCEPT
ON-LINE PW SECURITY
MODEMS HANDSHAKE
ANS MODEM PROMPTS FOR CELL PW
PW ACCEPT AND CALLBACK
PW REJECT
P/W ACCEPT
TYPICAL ON-LINE PW SECURITY SEQUENCE
REMOTE DIAL-IN USER
CELL P/W STORED IN MODEM
CALLER PROMPTED BY ANSWERING MODEM
SC V.34
REMOTE DIAL-IN USER
ANY MODEM
CALLER PROMPTED BY ANSWERING MODEM
TXD RXD RTS CTS DCD GD DTR OH NR ND TM ALM ADV ST LL RL DL SEL V.F 28.8
General DataComm Inc.
SPECTRA COMM 2000
STEADFAST V.34 4-PORT MODEM WITH SCM IN A SPECTRACOMM 2000 SHELF

SteadFast RADIUS

RADIUS Dial-In Authentication with Challenge and RADIUS Accounting

As dial-in modems are added to communication servers on a corporate network, that network becomes more vulnerable to security breaches. Network managers are left with serious security problems. To answer many of the Internet's security needs for a standard protocol, RADIUS was accepted as the de facto standard for Remote Authentication Dial-In User Service. RADIUS brought a client-server architecture to ISPs, enabling efficient, secure authentication of dial-in users. RADIUS servers manage a database of users, provide authentication that allows/denies dial-in user access, and define the type of service to deliver to the user.

GDC's V.34 Modems Provide SteadFast RADIUS Solutions

The SpectraComm Manager (SCM), Dual V.34, V.34 and V.34 4-Port modems support RADIUS Security. The V.34 modems prompt the dial-in user for a name and password and forward this information to the RADIUS server. The RADIUS server authenticates the user and returns a message to the modem to grant or deny access. The RADIUS server may also Challenge the remote user and request additional information before granting access. A typical RADIUS-protected network is illustrated here.

SteadFast LAN RADIUS

Authentication and Accounting with Challenge for Telnet Users via the SCM

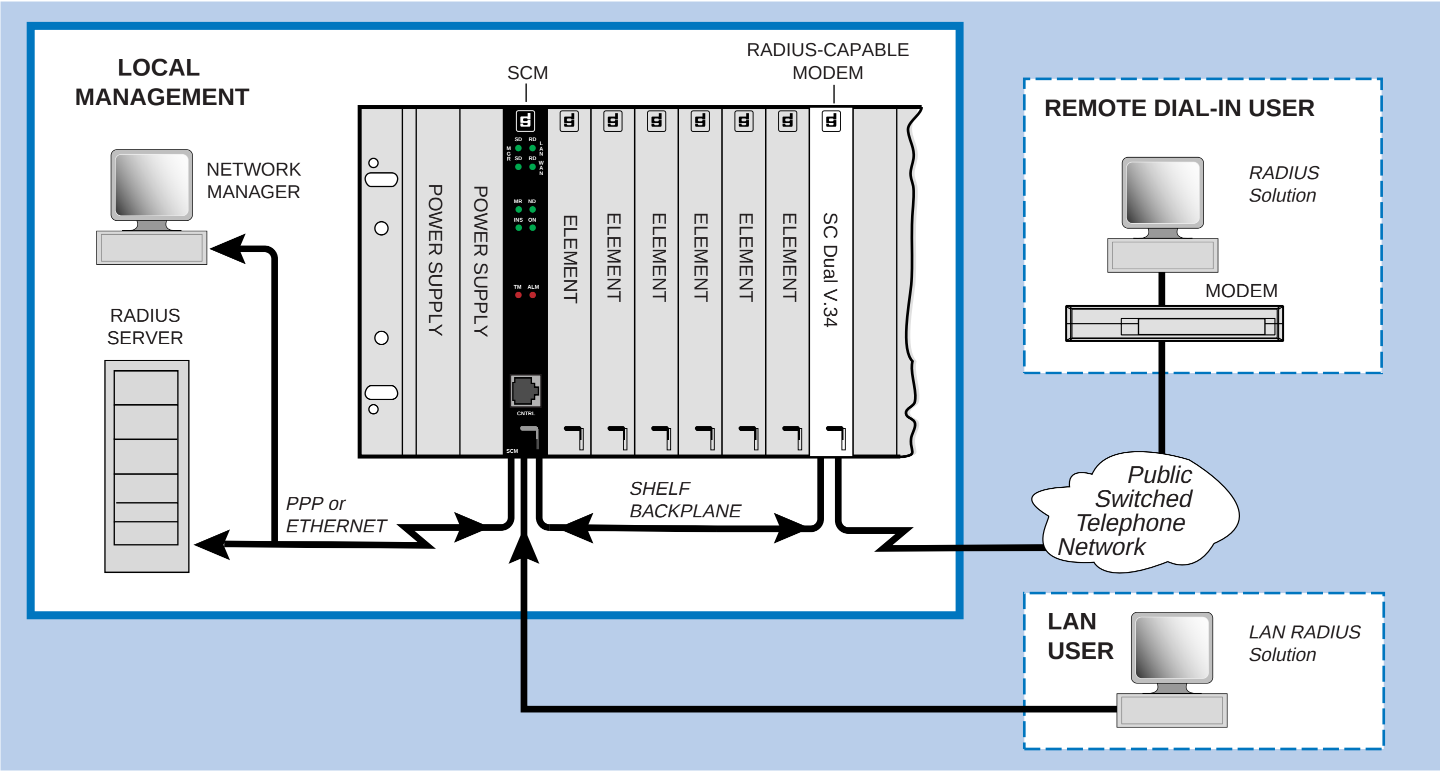
SteadFast LAN RADIUS provides users with authenticated Telnet management access to network elements in an SCM-managed SpectraComm shelf. By using the same RADIUS server that provides Authorization and Authentication for dial-in users, SteadFast LAN RADIUS allows you to eliminate the requirement for a separate server. SteadFast LAN RADIUS migrates Telnet management onto a high-security platform while saving hardware and software capital expenses.

Certified and Compliant V.34

GDC's SteadFast V.34 modems are the only analog V.34 NEBS III certified modems with RADIUS Authentication for Secure Dial-In Access. Supported RFCs are as follows:

- 2865 RADIUS
- 2866 RADIUS ACCOUNTING
- 2618 RADIUS Client MIB
- 2620 RADIUS Client Accounting MIB

Fig. 3: Communication between SCM and RADIUS servers can be conducted along LAN, WAN, Dial Backup WAN ports or the SCM CTRL port.



SteadFast RADIUS Authentication

Industry Standard Authentication
The SCM operates as a client of RADIUS to pass user identification information to designated RADIUS servers and acts upon the response. RADIUS servers receive connection requests and authenticate the users.

Network Security
Authentication occurs through a "secret" that the SCM and RADIUS server share but never send over the network. User passwords are encrypted, preventing hackers from determining passwords. Server redundancy for up to six RADIUS servers is supported by the SCM.

Flexible Authentication in Legacy Applications
SteadFast RADIUS can authenticate user access to legacy equipment via craft ports or X.25 pads.

Easy Maintenance & Management
Centralized password storage in the RADIUS Server simplifies password provisioning and maintenance.

TEAM Network Management

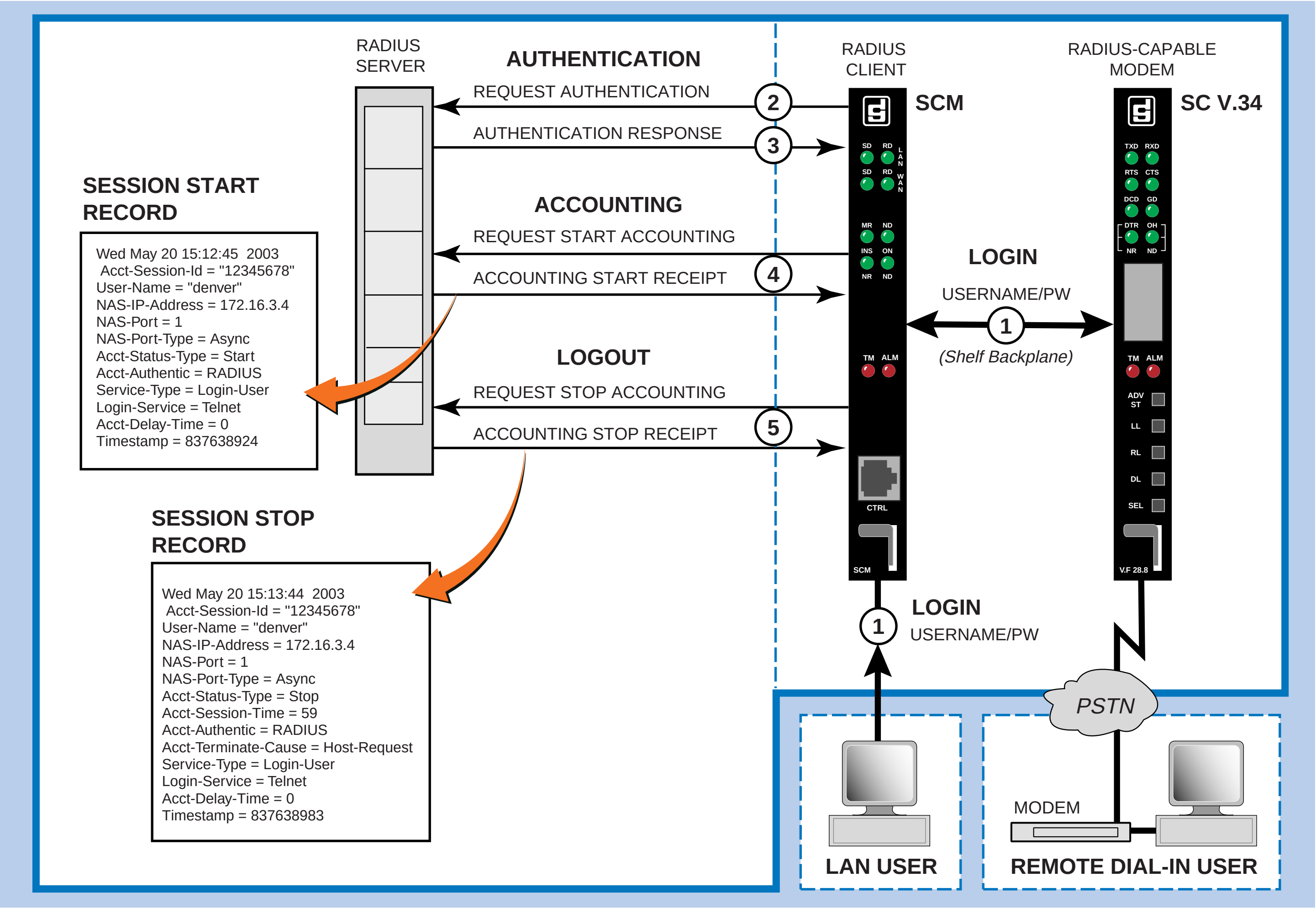
TEAM can configure RADIUS (except for secrets), and also display RADIUS Authentication and Accounting status.

SteadFast RADIUS Accounting

RADIUS Accounting is an extension of RADIUS Authentication for both dial-in and Telnet users. Administrators use RADIUS Accounting to track network usage for auditing and billing purposes. RADIUS accounting consists of a customer-supplied accounting server and the SCM as the accounting client. As transactions occur, they are recorded to a file on the RADIUS accounting server. RADIUS Authentication and RADIUS Accounting may be conducted on the same server or on separate servers.

RADIUS Process

1. A Telnet or Dial-in user logs in with a username and password.
2. SCM and RADIUS server exchange encrypted authenticating information.
3. An authenticated user is granted access to the shelf.
4. When the user session begins, a Start Accounting record is stored on the server. *(Sample shown below.)*
5. When the user session ends, a Stop Accounting record is stored on the server, including disconnect cause and session time in seconds. *(Sample shown below.)*



SESSION START RECORD

```
Wed May 20 15:12:45  2003
 Acct-Session-Id = "12345678"
User-Name = "denver"
NAS-IP-Address = 172.16.3.4
NAS-Port = 1
NAS-Port-Type = Async
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Login-User
Login-Service = Telnet
Acct-Delay-Time = 0
Timestamp = 837638924
```

SESSION STOP RECORD

```
Wed May 20 15:13:44  2003
 Acct-Session-Id = "12345678"
User-Name = "denver"
NAS-IP-Address = 172.16.3.4
NAS-Port = 1
NAS-Port-Type = Async
Acct-Status-Type = Stop
Acct-Session-Time = 59
Acct-Authentic = RADIUS
Acct-Terminate-Cause = Host-Request
Service-Type = Login-User
Login-Service = Telnet
Acct-Delay-Time = 0
Timestamp = 837638983
```

AES Encryption Option

AES Encryption employs the Advanced Encryption Standard which is a symmetric 128-bit block data encryption technique. AES Encryption takes plain-text data and encrypts it according to the AES algorithm to generate cipher-text data. AES is an approved FIPS-140-2 and FIPS-197 U.S. Government encryption standard that works at multiple network layers simultaneously.

SpectraComm Dual V.34, V.34 and V.34 4-Port modems support the AES (Rijndael) encryption standard. The user configures the modem for AES Encryption by entering an encryption key via AT commands at one of the modem's management interfaces (Telnet connection through the SCM, the SCM craft port, or the modem's DTE interface). AES Encryption allows each modem to take transmit/receive asynchronous data and encrypt/decrypt it on a dial-up or private line network.

AES Parameters

AES Key Size

The AES key size is user-selectable as a 128, 192 or 256 bits character string.

AES Modes

AES Encryption is implemented in SpectraComm modems with three encryption modes:

- Electronic Code Book mode (ECB)
- Cipher Block Chaining mode (CBC)
- Counter mode (CTR)

Combined Security Options

A modem optioned for encryption is required at either end of the communication link and with the same encryption key entered in both modems. AES Encryption can be configured to operate in combination with SteadFast Security and/or the RADIUS Authentication option.

Secure Access Modem Option

The Secure Access Controller (SAC) system employs a factory-optioned GDC V.34 modem to authenticate remote users attempting to access protected network equipment, such as switches, routers, multiplexers, etc.

SpectraComm V.34 and Dual V.34 modems support the Secure Access feature. The modem is user-configured via extended AT commands typed at one of the modem's management interfaces (Telnet via the SCM, the SCM craft port, or a terminal connected to the modem's DTE connector).

SAC System Components

The SAC system consists of five principal components:

- SAC Administration Server
- SAC Database (with Backup)
- Authentication Server (AS)
- Secure Access Modem (SAM)
- Client desktop software

The Authentication Server connects to the PSTN by a modem bank. Authentication data obtained from the SAC Database allows the server to permit only authorized personnel to control the network equipment. The server generates the private key exchanged by the modem and server, and the public key exchanged by the modem and remote user's client software. Client software initiates calls to the SAM and the AS, sets up secure tunnels between those devices, and functions as the user interface to protected network equipment.

Access privileges to network equipment are determined by an administrator who operates the SAC Administration Server, typically located at a service coordination center. Remote users must make a request of the administrator for authorization to particular network equipment. User data is then entered in the SAC Access Database for retrieval by the Authentication Servers.

Each connection sets up a secure tunnel that passes AES-encrypted data to the authorized user. When a user terminates a management session, the Secure Access Modem requests a connection to the Authentication Server to obtain another new private key, thus preventing further access from the previous remote user or intruders.

Combined Security Options

A modem optioned for Secure Access can be configured to operate in combination with or without SteadFast Security.

SteadFast IP Security

GDC's SpectraComm IP products provide IP connectivity to LAN-attached devices over standard T1, E1, DDS or xDSL circuits. SCIP routers (SCIP-T1, SCIP-E1, SCIP-DSL) and SCES ethernet switches (9-Port or 18-port) are all equipped with SteadFast IP Security solutions as follows:

- User- and Supervisor-level passwords stored in the device authorizes every access attempt.
- Inactivity logoff prevents hacks through 'left on' equipment.
- Disabling of SNMP, HTTP, and TFTP services will deter hacking through these protocols.
- TACACS+ protocol provides secure, centralized authentication over IP networks.
- MACL (Media Access Control List) Security detects unauthorized users by their MAC address.

TACACS+ Authentication

Each SCIP and SCES device can be configured for TACACS+ authentication. This capability supports the Cisco TACACS+ protocol for secure, encrypted authentication between the SCIP or SCES device and its TACACS+ server.

When TACACS+ is enabled in the SCIP or SCES, the TACACS+ server becomes the central point for managing network-wide usernames and passwords. This is especially useful when provisioning usernames and passwords for devices in large networks. TACACS+ usernames and passwords are authenticated for all access methods: craft, Telnet, and HTTP.

Added SCIP Features

When equipped with the optional V.34 modem, or when installed with an external V.34 modem, SCIP devices can provide emergency management access over a dial-in connection. In extended LAN applications, SCIP devices support the standards-based Spanning Tree Protocol for full network redundancy and loop elimination.

Added SCES Features

Assuming that password-protected hosts and network equipment are present in the customer's network, the SCES devices can be configured to provide Ethernet Security to heighten network protection. Protected ports can detect access attempts by an illegal user or by a hacker attempting to make an illegal cable connection into the port. SCES responds to a security breach at any port according to the following pre-set Ethernet Security modes and options:

Port-based Ethernet Security Mode

Protected ports are disabled permanently or for 5 minutes whenever SCES detects a cable disconnect at the port. When optioned for a permanent disable, only an authorized administrator can re-enabled the port.

MAC-based Ethernet Security Mode

Each protected port is configured with up to eight legal MAC addresses. The port is disabled permanently, for 5 minutes or is filtered whenever an illegal address is detected. When optioned for a permanent disable, only an authorized administrator can re-enabled the port.

Enforcement Protection

If power cycles after a port- or MAC-based security violation occurs, SCES will continue to enforce security on the port. Disabled ports will come up disabled.

STEADFAST IP DEVICES, SCIP AND SCES 9-PORT IN A SPECTRACOMM 2000 SHELF

Disaster Recovery

Your Worst Network Nightmare

Network outages, natural disasters, and other events in recent years have prompted a surge of interest in redundancy and disaster recovery. When government, law enforcement, financial, enterprise and other networked repositories experience downtime caused by outages and security breaches, vital information and assets are vulnerable. Millions of dollars in worth, damage and lost revenue can ensue.

A recent survey in IT Week reveals IT managers' worst nightmares:

> *“... two-thirds admit to lying awake at night worrying about security or downtime."*
>
> *"Most IT managers feeling that money is draining from the company coffers every time a server crashes, an Ethernet switch flashes yellow and then goes dark, or a service provider sends a courteous email a week after a T1 went down.”*

According to analyst, Infonetics Research, network outages and degradations cost some firms as much as one per cent of total annual revenue - up to $74.6M through lost productivity. In-depth case studies of six large organizations across various industries found companies losing up to $96,632 per hour of network downtime. Most administrators don't know where the network is vulnerable, or how to deploy strategic and effective protection.

SteadFast to the Bottom Line

Reliability and performance with high security built in is a necessity; savings and ease of use is a must. Through excellence in engineering, testing and innovation comes GDC’s reliable SpectraComm line of integrated network access cards, management software and housing products.

With 'SpectraCommonality' each SpectraComm device can integrate into a unified, flexible, managed shelf environment that is scalable to your network's changing needs. This integrated design means flexible sparing requirements and seamless, secure coverage throughout the network. SteadFast solutions built in to SpectraComm products give you the control you need to secure your valuable network assets.

GDC SteadFast Disaster Recovery

GDC SteadFast Solutions not only provision Security and Authentication throughout the network, but can also prevent network downtime through strategic Disaster Recovery built into your GDC network products. Even with multiple security, service and hardware failures, links will be up and operational in a network provisioned with GDC equipment and its Steadfast built in solutions.

For more information on SteadFast Disaster Recovery solutions, refer to GDC literature at gdc.com or contact your GDC Sales Representative about:

- Safe T1 Redundancy
- SCM Redundancy
- Power Redundancy
- RADIUS Redundancy
- Remote Management / Out of Band Management
- Dial Back-Up
- Safe LAN-X

General DataComm
The Best Connections in the Business
http://www.gdc.com

SCSEC-AB03-070-EO_April 07