Contact GDC http://www.gdc.com

GENERAL DATACOMM

Revised:
February 2006

Author:
George Gray - CTO

How Secure is Your Network?

General DataComm
The Best Connections in the Business

The ENEMY Within *[your]* NETWORK

In recent years, network planners have been providing robust and more widely shared voice and data communication throughout their environments. Such flexible, transparent boundaries between central and remote sites are vital enhancements for day-to-day business operations.

They also open the door to a greater vulnerability. In today's security conscious world, network operators must be focused on the recognition of, and the response to, attacks and threats from outside the network.

Regardless of the approaches taken to identify and protect against attacks from outside the network, there remains a larger and perhaps more insidious threat that can occur from within the network itself.

Attacks can come from hostile employees, from persons with access to a particular location, or from many other sources.

Scope of this Document

Network access products, selected for their proven reliability, performance and comprehensive built-in security features, are the best protection from hostile or illegal attempts to access your network. This document will discuss the General DataComm security solutions that can protect your network from malicious or unwanted traffic.

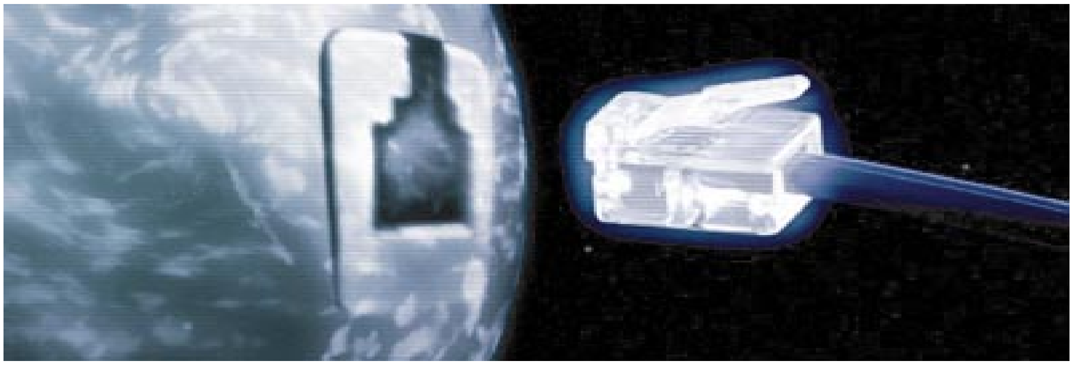
> *"... A larger, perhaps more insidious threat can occur from within the network itself..."*

Most people consider Ethernet as the "secure" access interface to their network. Because of the pervasive use of Ethernet throughout today's networks, unwanted or hostile traffic occurring at an Ethernet port can cause irreparable harm.

To keep unwanted traffic off the network at the point of origin, GDC has developed "IronGate," a security strategy that guards these entry points throughout your mission-critical network. Irongate Security stops illegal WAN and LAN port access before serious network damage or interruptions can occur.

IronGate Security is part of a comprehensive suite of security features designed into the GDC family of SpectraComm IP and SpectraComm Ethernet Switch products. IronGate Security allows operators to identify valid and invalid users by the MAC address detected at the specific port being accessed. To accommodate complex network topologies, operators can tailor IronGate Security to deliver the least or the greatest restriction at access points anywhere in the network. To best understand the IronGate features, it is necessary to briefly describe GDC's SpectraComm IP (SCIP) and the SpectraComm Ethernet Switch (SCES).

General DataComm IronGate, SteadFast and Dial-In security solutions protect mission-critical enterprise and provider networks.



Typical Implementation: SCIP and SCES

General DataComm's SCIP device is an integrated CSU/DSU and Ethernet device aimed primarily at providing transparent LAN extension. (Alternatively, the SCIP can be configured as a static router. A static router-based network has an inherent security advantage over a dynamic router-based network, in that static routers can be added and routes discovered without operator intervention.) The SCIP has one WAN port and two Ethernet (LAN) ports. The SCES is a high performance Ethernet switch available with nine or eighteen ports.

Both SCIP and SCES devices are NEBS Level III-certified; as such, they are extremely reliable, rugged, and deployable in most environments - even those with extreme temperatures between -40º C. to +75º C. (-40º F. to +167º F.).

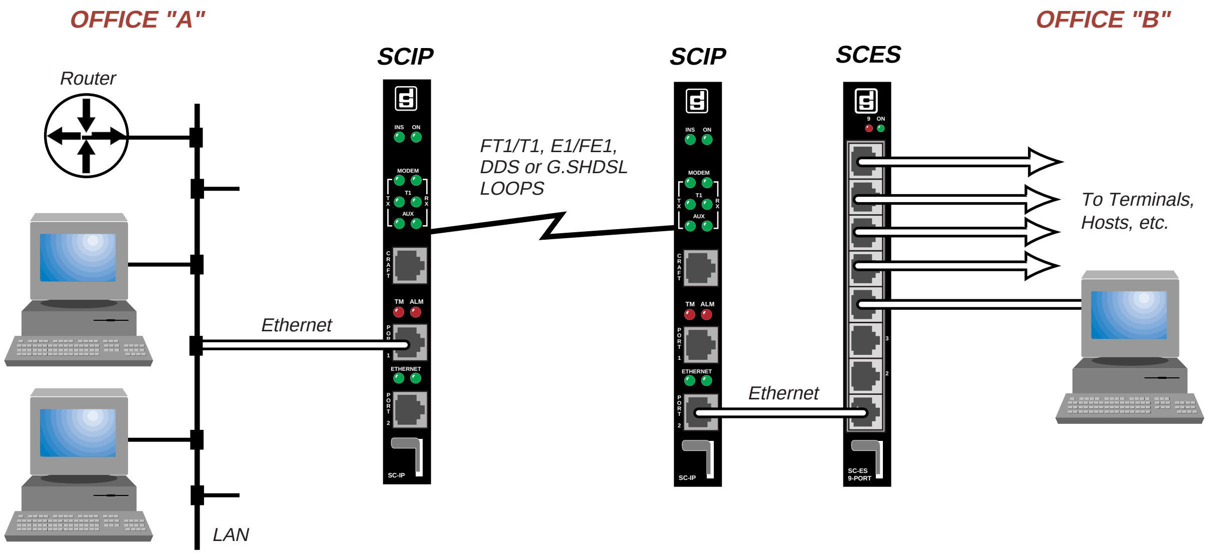
SpectraComm IP with IronGate Security

SCIP uses a MAC address table to apply IronGate security screening at its Ethernet (LAN) ports. Up to 100 valid MAC addresses can be defined in a table for the Ethernet interface, thereby filtering traffic onto the network from only those addresses permitted at the associated port. Up to 100 valid MAC addresses can be defined at the SCIP's WAN port. Both the LAN and WAN interfaces can be implemented with IronGate Security for simultaneous in-bound and out-bound traffic validation.

Figure 1:
SCIP devices extends the LAN between two sites across the T1, E1 or G.shdsl network.

Figure 2 and Figure 3:
Irongate Security protects SCIP's LAN and WAN ports (at central or remote sites) from unauthorized in-bound or out-bound traffic.

FIGURE 1



IRONGate Security at Central Site

Every access attempt at the central site SCIP's LAN or WAN ports are screened by Irongate Security. Valid MAC addresses are recognized and traffic is allowed to progress normally, whereas unknown MAC addresses are detected, denied ingress or egress traffic and are reported via SNMP alarms. SNMP alarms are also generated if a disconnect is detected at SCIP's WAN port or Ethernet ports. These SNMP events alert network operators to a potential intrusion. Since only valid users with high-level access privileges can execute MACL commands, the MAC address table itself is protected from unwanted manipulation by users at SCIP's WAN, LAN or dial-up access points. For secure and centralized management of usernames and passwords throughout the network, SCIP supports TACACS+ Authentication.

Typical Configuration

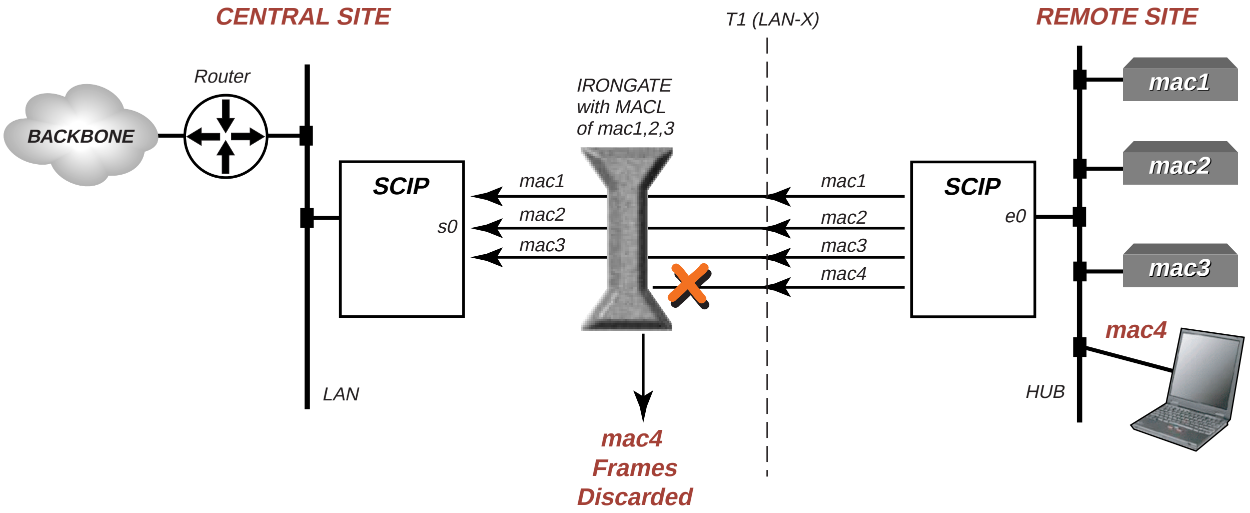
Ethernet equipment is attached at the remote SCIP site. Two devices may be connected directly to the SCIP ethernet ports or an external hub or switch (i.e., SCES) may be connected to support more ethernet equipment. The central SCIP device has MAC security enabled on the serial0 interface. The Media Access Control List (MACL) for this interface is configured with the addresses mac1, mac2, and mac3. The MACL also has the MAC addresses for the remote SCIP. If a managed SCES device is at the remote location, its MAC address should also be entered in the MACL. Likewise, the MAC addresses of remote SCIPs must also be entered in MACL of the central site SCIP. The remote-site equipment with addresses mac1, 2, and 3 will be allowed to send traffic towards the backbone.

Typical Scenario

The 'hacker', shown in Figure 2 as a laptop at the remote location, has entered the site and connected to the ethernet segment. Since this MAC address (mac4) is not in the MACL, this traffic will be discarded before reaching the customer's backbone.

The net effect is that legal traffic will be able to pass through the IronGate demarc, while hacker traffic will be detected, dropped and reported.

FIGURE 2



IRONGate Security at Remote Site

Every access attempt at the remote SCIP's LAN or WAN ports are screened by Irongate Security. Valid MAC addresses are recognized and traffic is allowed to progress normally, whereas unknown MAC addresses are detected, denied ingress traffic and are reported via SNMP alarms. SNMP alarms are also generated if a disconnect is detected at the SCIP's WAN port or Ethernet ports. These SNMP events would alert network operators to a potential intrusion. Since only valid users with high-level access privileges can execute MACL commands, the MAC address table itself is protected from unwanted manipulation by users at SCIP's WAN, LAN or dial-up access points. For secure and centralized management of usernames and passwords throughout the network, SCIP supports TACACS+ Authentication.

Typical Configuration

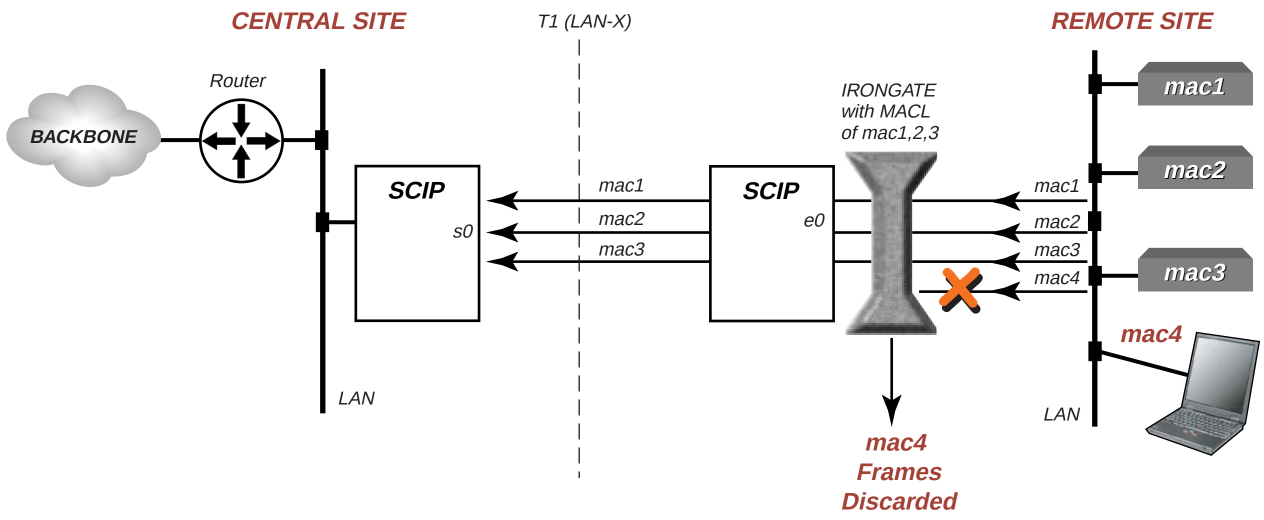
At the remote site, the SCIP device has MAC security enabled on the ethernet0 interface. The MACL for this interface is configured with the MAC addresses mac1, 2, and 3. If a managed SCES device is installed at the remote location, its MAC address should also be entered into the MACL. SCIP facilitates MAC address configuration with a MAC address "auto-learn" feature for each interface. When this feature is enabled, the source MAC address is learned from each packet received on the specified interface. If not already in the MACL, the MAC address is automatically added for that interface, up to the limit of 100 MAC addresses per MACL.

Typical Scenario

The 'hacker', shown in Figure 3 as a Laptop at the remote location, has entered the site and made a connection to the ethernet segment. Since this MAC address (shown as mac4) is not in the MACL, this traffic will be discarded before reaching the customer's backbone. In this scenario, this traffic will be discarded before traversing the T1 towards the backbone.

The net effect is that legal traffic will be able to pass through the IronGate demarc, while hacker traffic will be detected, reported and dropped right at the remote site.

FIGURE 3



Port-By-Port IRONGate Security

GDC's SpectraComm Ethernet Switch (SCES) employs IronGate MAC address filtering for port-by-port control of access to the network. Up to eight valid MAC addresses can be added to address tables created for each port (9 or 18 ports per device, depending on model). To facilitate port configuration, SCES provides a "snapshot" feature which can automatically learn legal MAC addresses.

Similar to the SCIP devices, SCES can "close the circle" by providing TACACS+ Authentication, which prevents unauthorized access to SC-ES MAC address tables and any configuration information. When an invalid MAC address is detected at a SCES port, one of the following three configurable modes of security can be applied:

Temporary Port Shutdown

Temporary Port Shutdown will disable the port for 5 minutes upon detection of an invalid MAC address. The port will be restored automatically without operator intervention. SNMP alarms will be generated as a result of detection of an invalid MAC address.

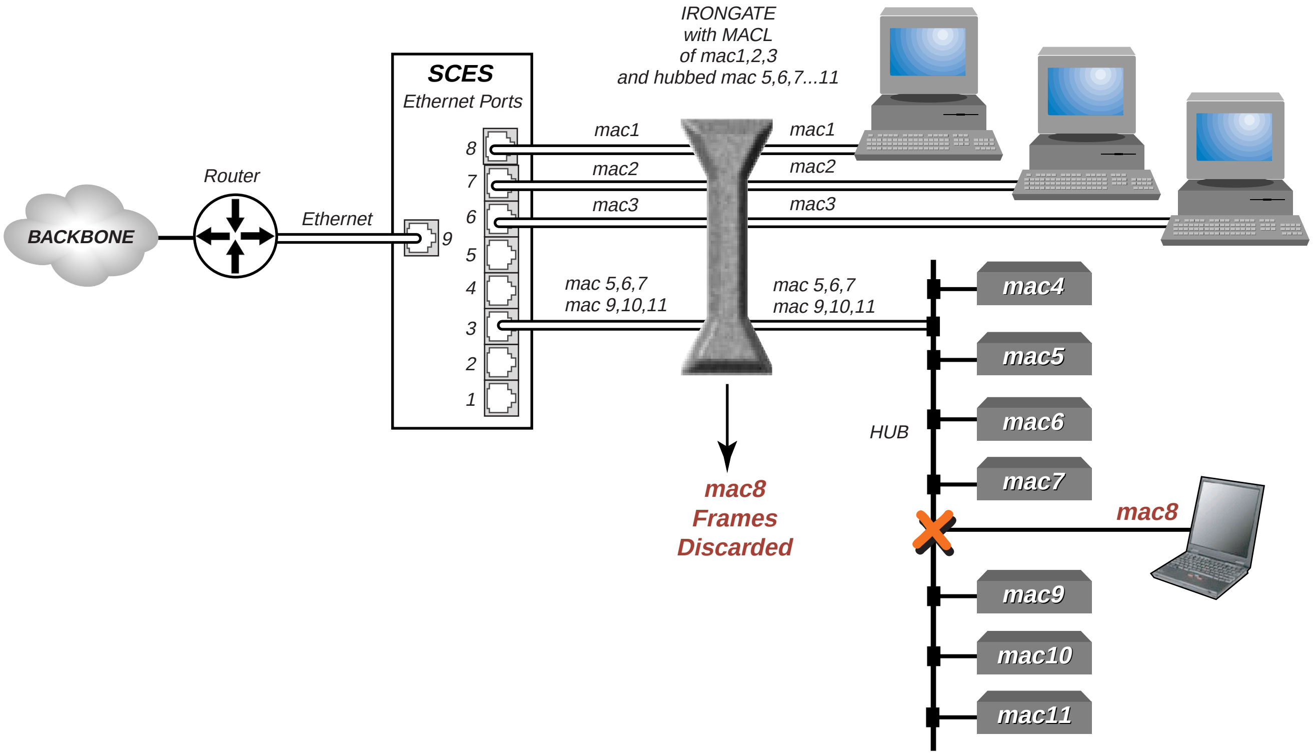
Permanent Port Shutdown

Permanent port shutdown works identically to the Temporary Shutdown described above, but the port can only be restored by operator intervention. SNMP alarms are generated as a result.

Ignore Traffic

The third method allows legal user traffic to proceed, but leaves the hacker disconnected, even when illegal/legal traffic from up to eight mac addresses is being "hubbed" to a single SCES port.

FIGURE 4



Today's Networks: Secure, Reliable and Recoverable

GDC has taken the lead in offering IronGate for point-of-access MAC filtering and TACACS+ Authentication as standard and fully configurable features on all SCIP and SCES devices. Any combination of these features can be implemented (or disabled) by a network operator to suit the security requirements for a specific site, interface or access port in the network.

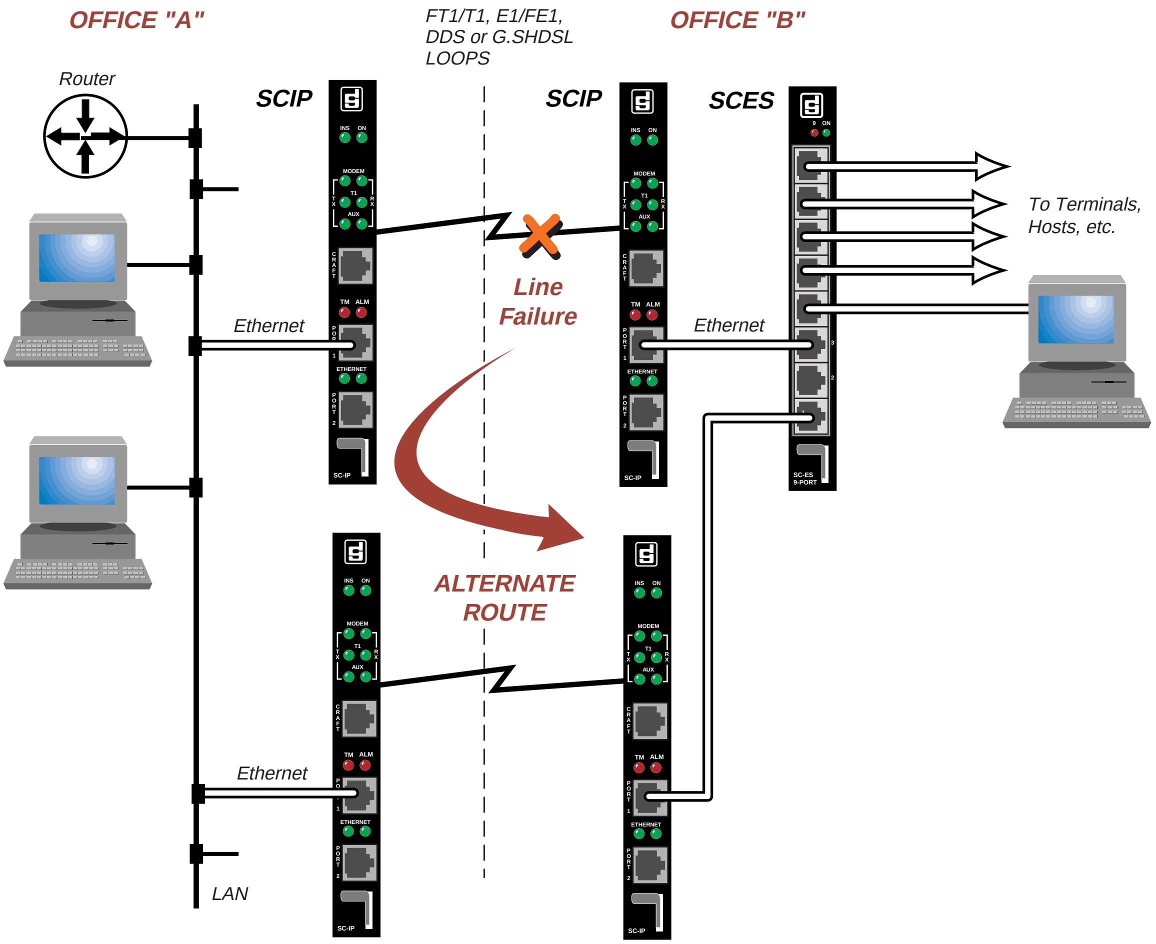
While security in the network is paramount, operators must also consider reliability. Network outages caused by major structural failure, such as hardware or facility (T1, E1, G.shdsl) failures, can have a serious impact on day-to-day business. Analysts have calculated the cost in millions through losses in revenue and productivity. GDC has introduced Safe LAN-X to protect the network from such costly failures.

Typical Scenario

Figure 5 demonstrates a typical Safe LAN-X network. SCIP can detect and eliminate loops so that there is no more than one active data path between any two workstations in that bridged LAN.

When there is a failed device or line detected, SCIP automatically reconfigures the active topology of the LAN. Traffic proceeds on the alternate path and communication is uninterrupted.

FIGURE 5



Secure Solutions for Dial-Up Data Services

GDC has been building secure network access products for 25 years and applies that knowledge in solving today's network security challenges. How secure are your Dial-Up data services? Securing the dial-in access points in the network can be especially difficult given their global exposure. General DataComm V.34 modems offer multiple security features which give network operators the choice of several levels of security protection for dial-in users:

GDC SteadFast Handshake Protection

For a higher level of dial-in security, GDC modems at both the originating and answering sites can be configured for GDC's SteadFast Handshake Security. As part of its handshake, the answering GDC modem sends the originating GDC modem a cell password that must have been previously stored in both modems. GDC's SteadFast Handshake Security is hacker-proof and will not permit unknown modems to communicate.

RADIUS Authentication & RADIUS Accounting

GDC modems can employ RADIUS (Remote Authentication for Dial-In Users) to authenticate users from a secure and centralized database of RADIUS usernames, passwords and challenges. RADIUS Authentication will accept, challenge and reject dial-in users via secure RADIUS servers. The RADIUS Accounting feature offers call tracking and billing information.

Modem Password Protection

GDC modems protect access with passwords stored in the modem.

Dial Backup Options

GDC modems offer several Dial Backup options that can be used with modem or RADIUS password protection.

Callback Security

GDC modems can be configured to respond to a dial-in user with one of three callback security responses. After the handshake, the caller is prompted to enter a password. If the password is accepted, the GDC modem disconnects and calls back only the specific modem associated with a valid user. Callback Security can be optioned to deny a callback, to call the original caller or to prompt the dial-in user for a callback phone number.

AES Encryption Option

For USA and Canada customers, AES data encryption encrypts async data sent across the communications facility via a dialup or leased line connection. Two GDC modems optioned for AES encryption are required, one at either end of the link. Modems perform all encrypt/decrypt functions without burdening customer applications, and without additional hardware. AES Encryption can be configured for ECB, CBC or CTR modes, and for 128-bit, 192-bit or 256-bit key sizes. Customers with SpectraComm V.34 modems in their networks can purchase the AES encryption feature as an upgrade.

Secure Access Controller System

For US and Canada customers, the Secure Access Controller (SAC) system employs a factory-optioned GDC V.34 secure access modem (SAM) to authenticate remote users Each authorized connection sets up a secure tunnel that passes AES-encrypted data between the remote user and the protected equipment.

Modem Security Combinations

SpectraComm V.34 modems optioned for the AES encryption or SAM feature can provide combined protection against unauthorized users. AT commands to the modem combine RADIUS, Steadfast, AES Encryption and/or SAM as follows, for security tailored to your needs:

- AES Encryption or RADIUS or Steadfast
- AES Encryption & Steadfast
- AES Encryption & Steadfast & RADIUS
- Secure Access Modem & SteadFast

General DataComm
The Best Connections in the Business

www.gdc.com

General DataComm WORLD HEADQUARTERS: Naugatuck, Connecticut, USA 06770 Tel 1-203-729-0271 Fax 203-729-3013