OBM (Out of Band Management) Overview

With the growth of IP, routers deployed into an IP network must not only be accessible by the network operator for maintenance and configuration purposes, but secure according to today's exacting standards. Once the IP address is configured, the router becomes manageable via the IP network. Should at any time, the router become inaccessible due to a network fault, the VF28.8 modem will provide the dial management path to the router.
Fig. 1 illustrates how a General DataComm VF28.8 modem is used for the network operator to dial into the router and configure an IP address.

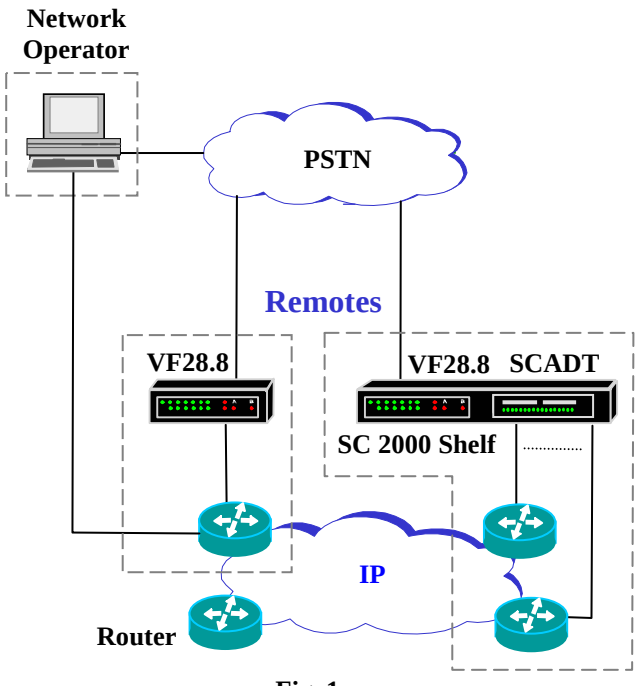

Fig. 1

OBM Modem Security

The simple OBM solution shown in Figure 1 supports the following modem security features:

–With On-line security, a password is stored in the VF28.8 modem and, upon handshake, the modem sends a password prompt to the network operator. The password sent by the network operator will be validated by the VF28.8 modem.

–With callback security, the network operator's telephone number is stored in the VF28.8 modem. Upon connection, the modem drops the call, retrieves the telephone number and calls the network operator back.

–Handshake security is proprietary to General DataComm and requires VF28.8 modems at both ends. A password is stored in both modems and embedded into the handshake. The password is validated at both ends and the connection is made.

–AES encryption requires VF28.8 modems at both ends and uses an encryption key of up to 32 characters stored in both modems to encrypt and decrypt the data.

Although traditional OBM solutions provide protection to remote devices, they do not fully comply to the specifications of SAS 70. The specification defines security measures that must be taken to protect data. Audit findings of the traditional OBM solution determine that:

–There is no proper authentication, authorization and audit trail.

–A simple password is used to block access to a cluster of remote devices.

–The user names, passwords, and stored telephone numbers are widely published and distributed.

In order to meet the requirement of SAS 70, General DataComm became part of a joint development effort to develop a security system known as the "Secure Access Controller System."

SAC Overview

Figure 2 shows a more secure OBM solution using the Secure Access Controller system (SAC). The SAC provides users with secure and authenticated dial access to remote network devices. The solution also provides compliance to SAS 70.

Figure 2 illustrates all the hardware components that are required to build a SAC system. Following is a description of each component:

–The client software is loaded onto the network operator's computer and is used to call the authentication server to obtain a public key. The public key is required to set up a secure tunnel to the Secure Access Modem (SAM) and ultimately establish a communication session to the router.

–The VF28.8 modem is upgraded with SAC software and becomes a SAM. The SAM protects the router from unauthorized users. The SAM may also be deployed into a SpectraComm 2000 shelf with a SpectraComm ADT providing the network operator with access to multiple routers. The SAM will also call the authentication server and obtain a private key that is required when the client software sets up a secure tunnel to it.

–The admin server is the web server interface that allows the network administrator to add SAM configurations and user accounts into the database.

–The authentication server authenticates the users and SAMs calling in by retrieving their information stored in the database. The authentication server also generates the SAM public and private keys required to set-up a secure tunnel between the client software and the SAM.

–The SpectraComm MS-2 shelf equipped with regular VF28.8 modems deployed at the central site provides the authentication server with an interface to the PSTN and all the users and SAMs dialing in. An SCM card deployed in the shelf allows the network administrator to access and configure the VF28.8 modems through an IP network.

SAC Communication Session

The SAC system uses a sequence of three secure dial-up calls to establish a successful communication session between the network operator and the router.

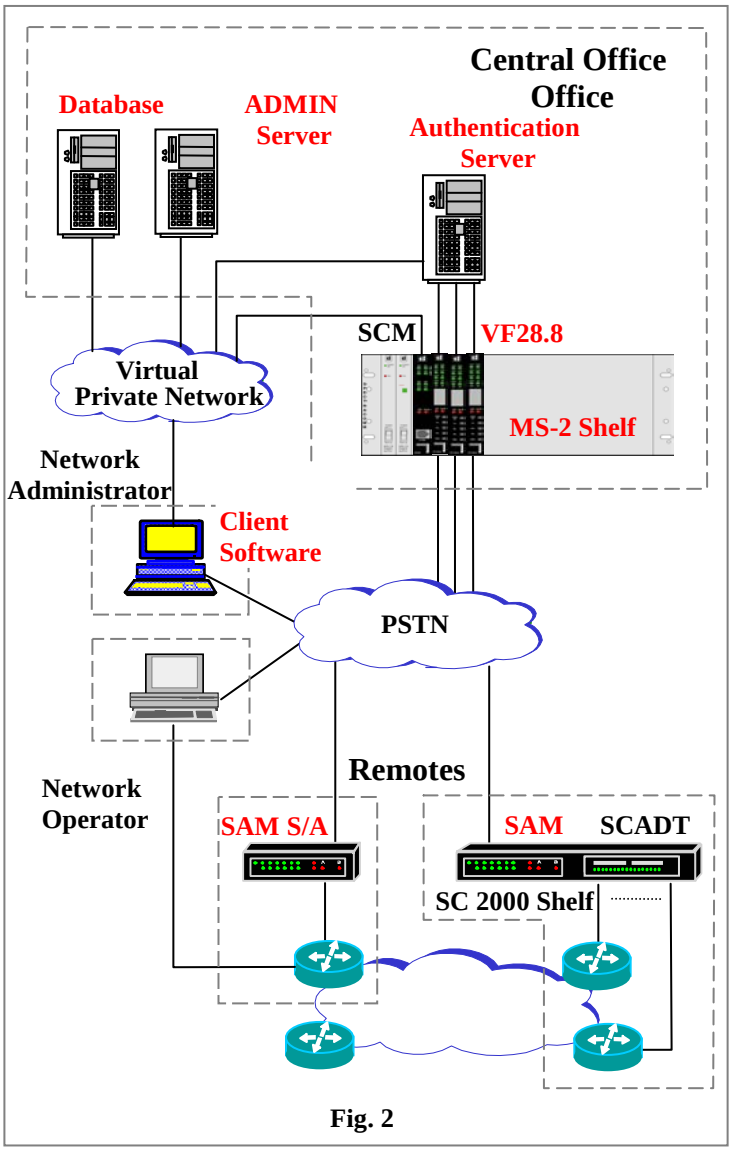

Fig. 2

The following describes the sequence of events that take place to establish a successful communication session.

1. The SAM supports the "remote configuration" feature. This feature allows the network administrator to remotely dial into the SAM and configure a SAM ID, SAM PIN, and the primary and secondary telephone numbers of the authentication server.

2. The network administrator then adds the SAM's configuration into the database via the admin server. The admin server supports an Ethernet interface allowing the network administrator to add user and SAM configurations through an IP network.

3. When the SAM is enabled, it will automatically call the authentication server. If authentication is successful, the authentication server will send the SAM a private key and the first call is dropped.

4. The network operator launches the client software and enters a user name, password, and the SAM ID of the SAM that the client will connect to. The network operator instructs the client to call the authentication server and send the information. If authentication is successful, the authentication server sends the client the SAM ID, a public key and the telephone number of the SAM. The second call is then dropped.

5. Using the telephone number it just received, the client automatically calls the SAM and sends the SAM ID. If authentication is successful, the call is maintained and a communication session is established between the network operator and the router through a secure tunnel.

At this point the network operator can assign an IP address to the router.

SAC Secure Tunnels

Each secure dial-up call uses RSA and AES encryption algorithms for authentication and data transfer. RSA algorithm uses two asymmetric keys: a public key to encrypt the message and an associated private key to decrypt the message. AES uses a symmetric key to encrypt and decrypt the information.

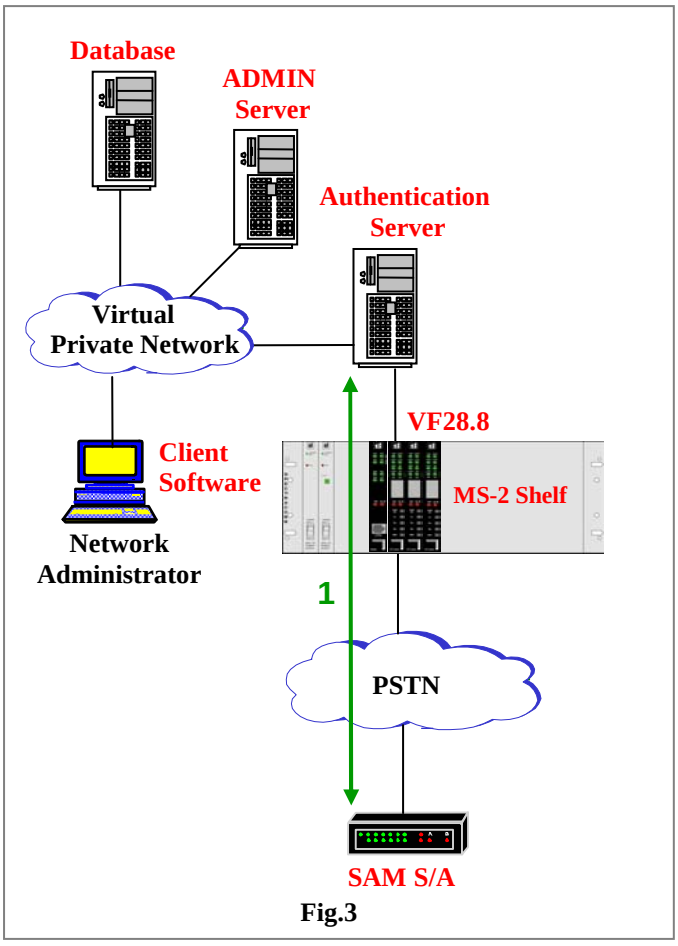

Fig.3

Fig. 3 shows the first secure dial-up call. The SAM generates a symmetric key that will be used to set up an AES tunnel. Both the symmetric key and the SAM ID are sent to the authentication server through an RSA encrypted tunnel. If the SAM ID is successfully authenticated, an AES tunnel is established and the authentication server sends the SAM a private key.

Fig. 4 shows the second secure dial-up call. The client calls the authentication server and sends a user name, password and the SAM ID that it wants to connect to through an *RSA encrypted tunnel*. If authentication is successful, the authentication server sends the client the SAM ID, a public key and the SAM's telephone number also through an *RSA encrypted tunnel*. In this call, all messages between the client and the authentication server are sent through an RSA tunnel only.

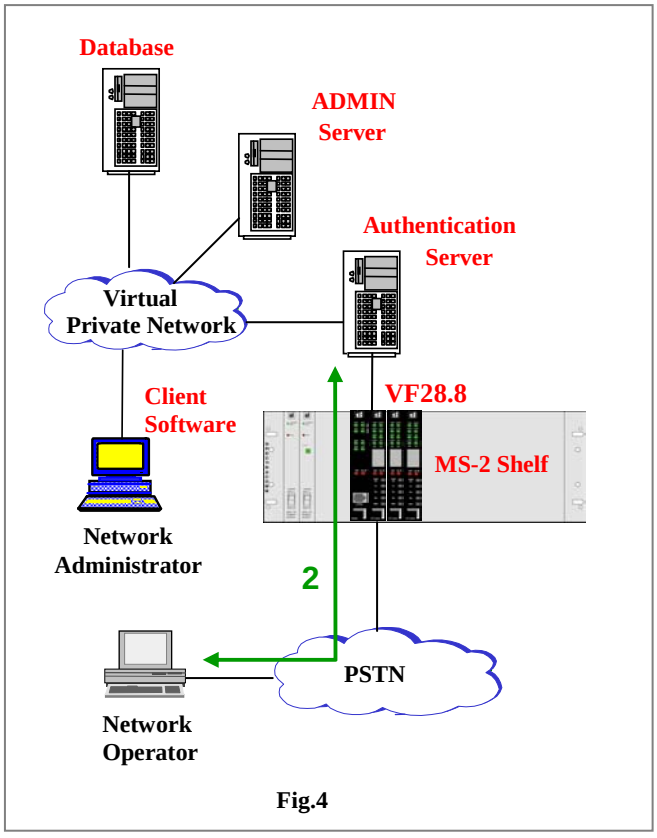

Fig.4

Fig. 5 shows the third and final secure dial-up call. The client also generates a symmetric key that will be used to set up an AES tunnel. The symmetric key and the SAM ID are sent to the SAM through an RSA encrypted tunnel. The client uses the *public key* received from the authentication server to encrypt the message and the SAM uses the *private key* also received from the authentication server to decrypt the message. If the SAM ID is successfully authenticated, an AES tunnel is established and all data traffic between the client and the SAM is AES encrypted and decrypted.

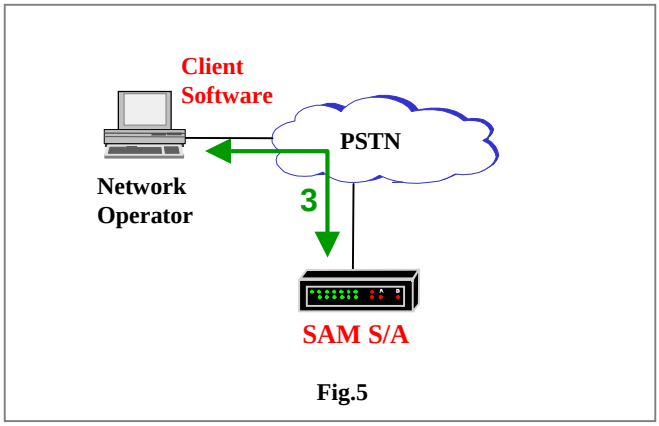

Fig.5

Radius vs SAC

Using the Radius Security System, the network operator calls into a VF28.8 modem and sends a user name and password. The user name and password are diverted to the radius server via the SpectraComm Manager Card (SCM). The radius server verifies the user name and password and instructs the SCM to advise the modem to either grant or deny the network operator access to the router. If access is granted, the communication session between the network operator and the router is *non secure. (unencrypted)*

With the SAC system, the authentication server generates the asymmetric keys required to set up a secure tunnel between the client and the SAM. With the use of these keys, the SAM authenticates the network operator. If access is granted, the communication session between the network operator and the router is *secure and encrypted.* Fig. 6 illustrates the OBM solution provided by both security systems.

To summarize the differences, the Radius solution authenticates and provides users with *non-secure access to manage devices. (unencrypted)* The devices are typically deployed *locally* to the radius server.

The SAC solution authenticates and provides users with *secure, encrypted access to managed devices.* The devices may be deployed *locally or remotely* to the authentication server.

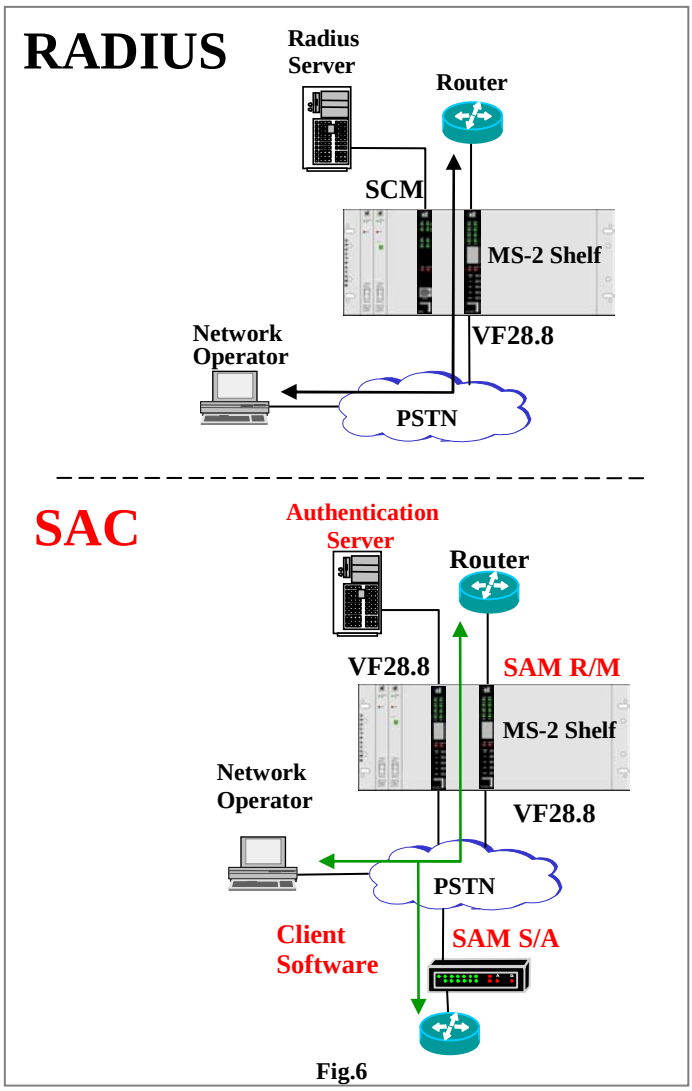

Fig.6

SAC Features and Benefits

The Secure Access Controller System provides the following features and benefits:

–The system supports authentication, authorization and accounting. Accounting referring to the database maintaining User and SAM logs. Every call attempt made by the SAM to obtain a private key from the authentication server is recorded with a time stamp that displays the result. As example, the result may indicate "success" or "wrong SAM ID". Every call made by the user to the SAM for authentication is also recorded with a time stamp that displays the result. The result may indicate "success" or "authentication error"

–The system generates private and public keys to set up a secure RSA tunnel between the client software and the SAM. What makes the system very secure is that new keys are issued for each secure tunnel established between the client software and the SAM.

–The system allows the data traffic between the client software and the SAM to be AES encrypted and decrypted.

–The system prevents the remote user of having knowledge of the keys or the SAM's telephone number. Only the SAM ID associated to the remote network device is known.

–The system allows the SAM to be periodically verified through private key requests. Remote modems in service for a long time may at some time become inaccessible due to the power being turned off or the telephone line being pulled out. Therefore, SAM private key requests act as an automatic circuit self test.