As shown in Figure 1, most corporate backbone networks have expensive routers. Understandably because these routers are very robust, their capable of handling large amounts of traffic, have advanced security features and hold all the information pertaining to the network.

If only these routers needed to be maintained, network administrators would save themselves substantial amounts of time that translates to significant labor savings. Unfortunately each remote location require additional routers than need to be maintained. By implementing additional routers, network administrator must deal with the following issues:

1. Higher capital expenditures because they must purchase these full-featured expensive routers and the CSU/DSU's if not integrated into the routers.

2. IP issues especially sub-net because each remote location must be treated as a separate network using up additional IP resources.

3. Increased recurring support costs in maintaining these remote routers that require configuration setup, monitoring and upgrades.

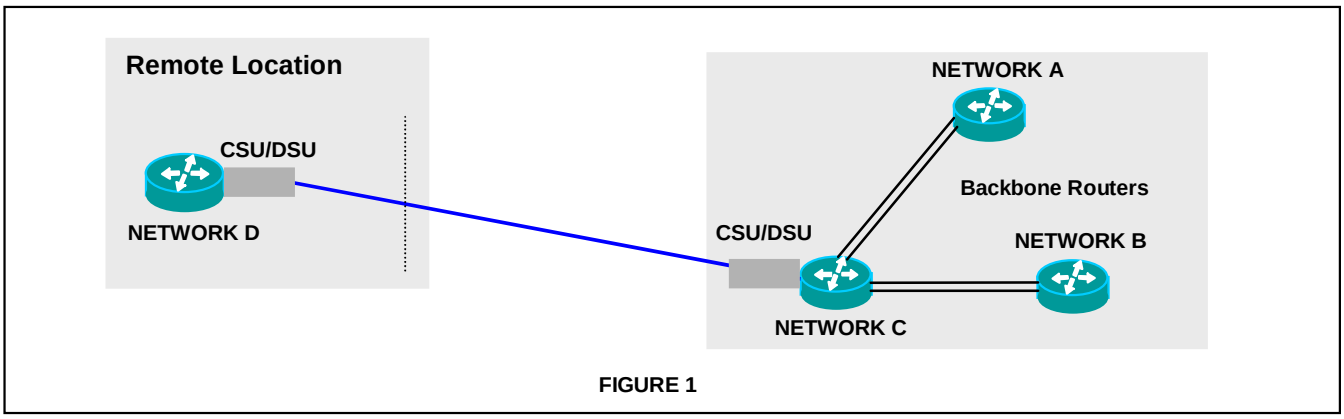

FIGURE 1

As shown in Figure 2, General DataComm's Transparent Ethernet Extension solution changes the dynamics of the network and eliminates these problems. The SCIP's, essentially function as router eliminators and extend the LAN to remote locations by passing data at the MAC layer. Network administrators can reduce their recurring support costs for the following reasons:

1. Only the central router needs to be configured. It is not necessary to maintain two sets of configuration, one for the central and one for the remote router.

2. There is no need to monitor the remote routers thus freeing up operations personnel and other infrastructure requirements associated with system setup for monitoring.

3. Only the central routers need to be upgraded. Upgrades usually take form in new features and heightened security.

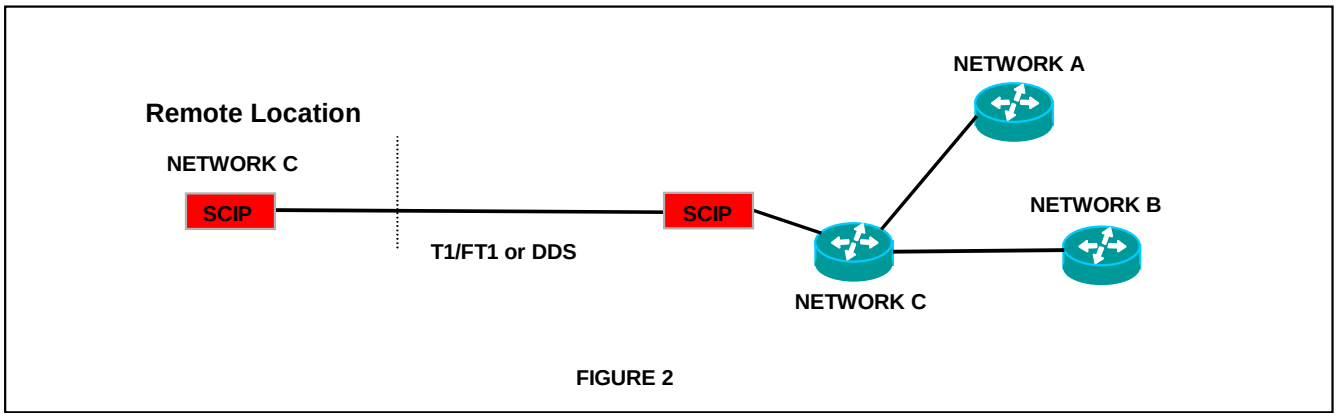

FIGURE 2

Figure 3 illustrates the traditional method of accessing remote IP and Legacy devices for maintenance purpose. Typically Service Providers will deploy a router based overlay network within their internal network for transmission of Primary Network Management traffic. Secondary "Out Of Band" Management traffic is through an external physical data connection such as a dial up.

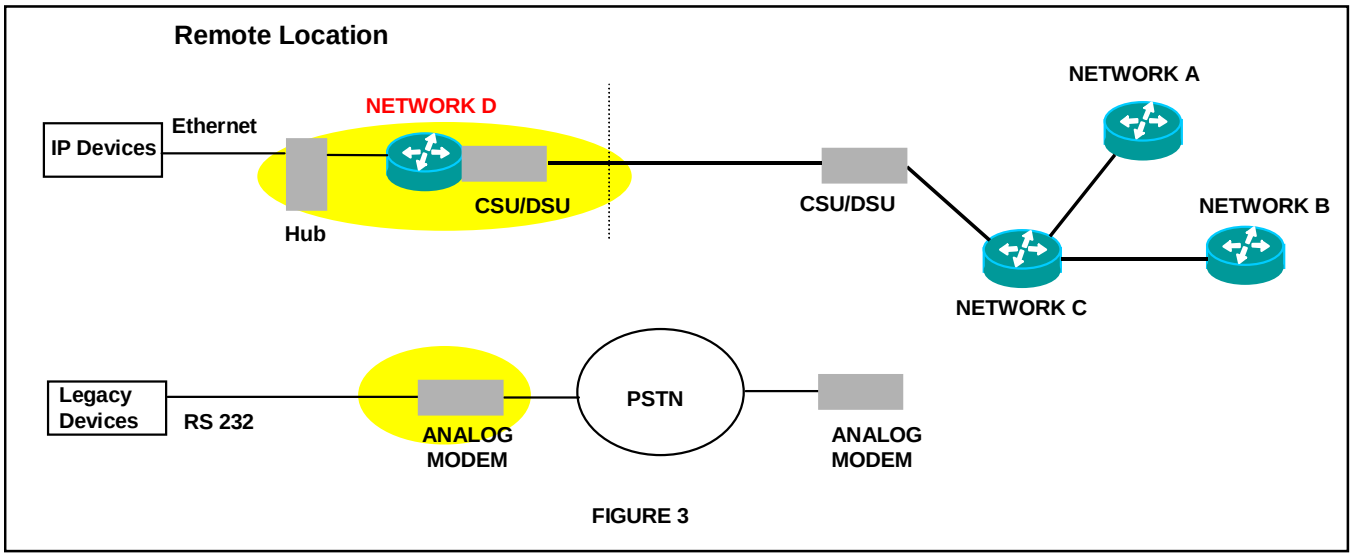

FIGURE 3

A much more effective method of accessing the remote IP and Legacy devices is shown in Figure 4. To summarize the benefits:

1. Network Administrators will significantly reduce their capital expenditures. The Remote Router, CSU/DSU, Hub and Analog modem as shown in the traditional method are replaced with a SpectraComm 2000 shelf equipped with a SCIP and SCES.

2. General DataComm's solution uses only one rack unit of space and integrates both Primary and Secondary Management traffic onto the same platform.

3. General DataComm's solution also provides management access to both IP and Legacy devices on the same platform.

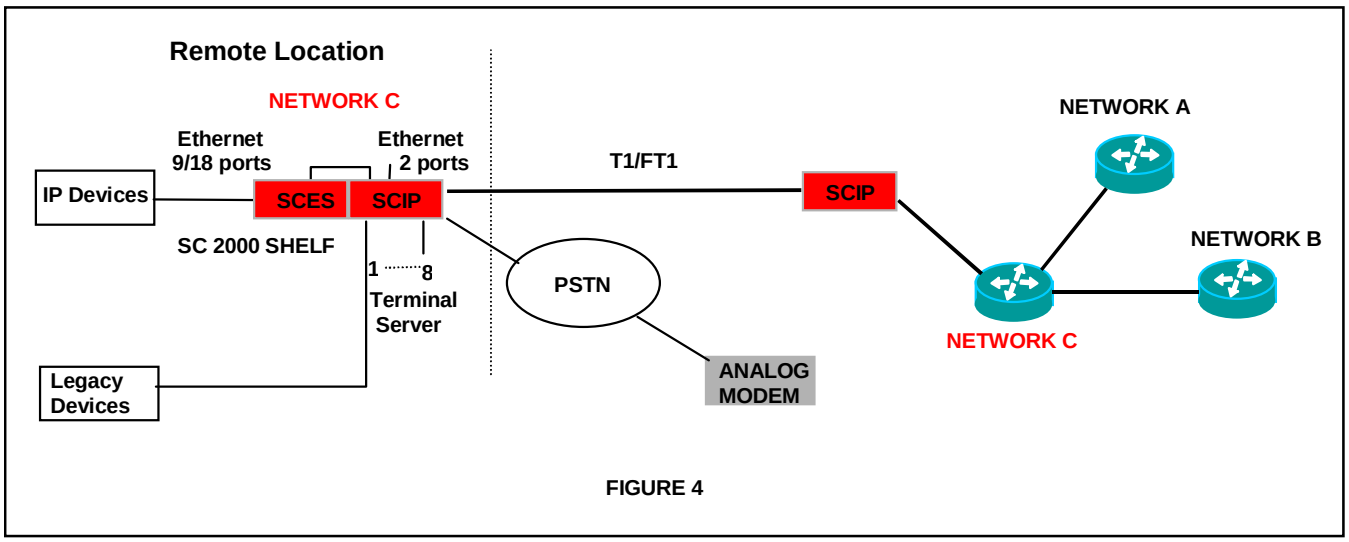

FIGURE 4

To keep unwanted traffic off the network at the point of origin, General DataComm has developed "IronGate", a security strategy that guards these entry points throughout the network. IronGate Security is part of a comprehensive suite of security features designed to allow Network Operators to identify valid and invalid users by screening MAC addresses at the port being accessed. Up to 100 valid MAC addresses can be defined in a table for the Ethernet interfaces. Both the LAN and WAN interfaces can be implemented with IronGate Security for simultaneous in-bound and out-bound traffic validation. For secure and centralized management of user names and passwords throughout the network, SCIP supports TACACS+ authentication.

In Figure 5, the central or remote SCIP devices could have MAC security enabled on either s0 for central or e0/1 for remote interfaces. The Media Access Control List (MACL) for these interfaces are configured with the addresses mac1, mac2. The intruder is shown as mac3 and has connected to the Ethernet segment from either one of the SCES port or from one of the SCIP port. Since this mac address is not in the MACL of either interface, this traffic will be discarded.

When an invalid MAC address is detected at a port, one of the following three configurable modes of security can be applied:

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

2. Permanent port shutdown works identical to the temporary shutdown but the port is only restored by operator intervention. SNMP alarms are also generated as a result.

3. Ignore Traffic allows legal user traffic to proceed, but leaves the hacker disconnected. This is applicable when legal/illegal traffic from up to eight mac addresses is being “hubbed” to a single SCES port.

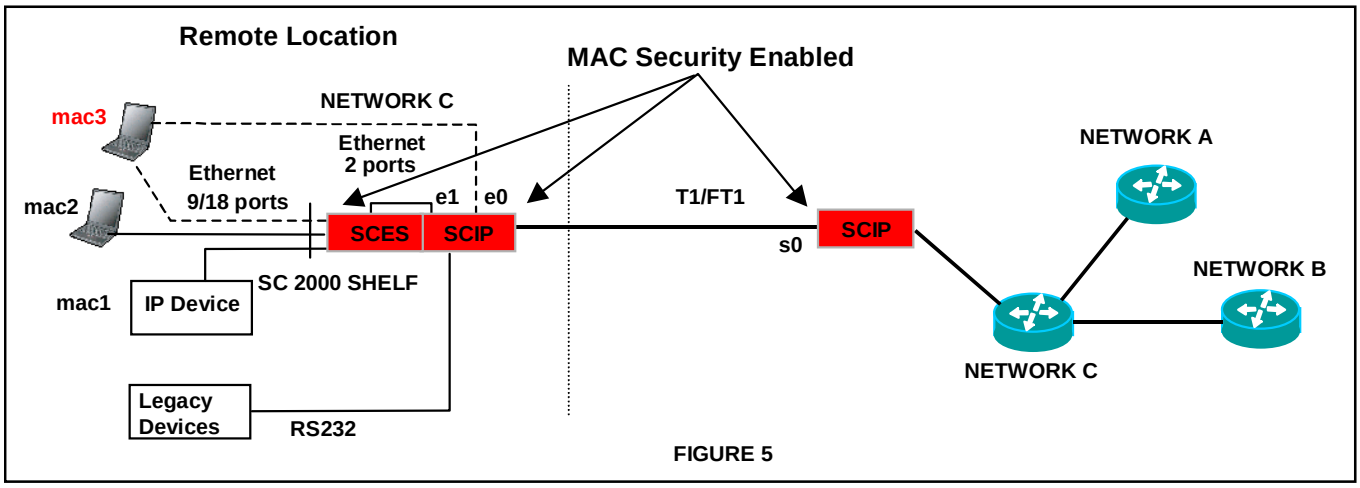

FIGURE 5

While security in the network is paramount, network operators must also consider reliability. General DataComm has introduced Safe LAN-X to protect the network from structural failure such as hardware or facility. Figure 6 demonstrates a typical Safe LAN-X network. SCIP can detect and eliminate loops so that there is no more than one active data path. When there is a failed device or line, SCIP automatically reconfigures the active topology of the LAN. Traffic proceeds on the alternate path and communication is uninterrupted.

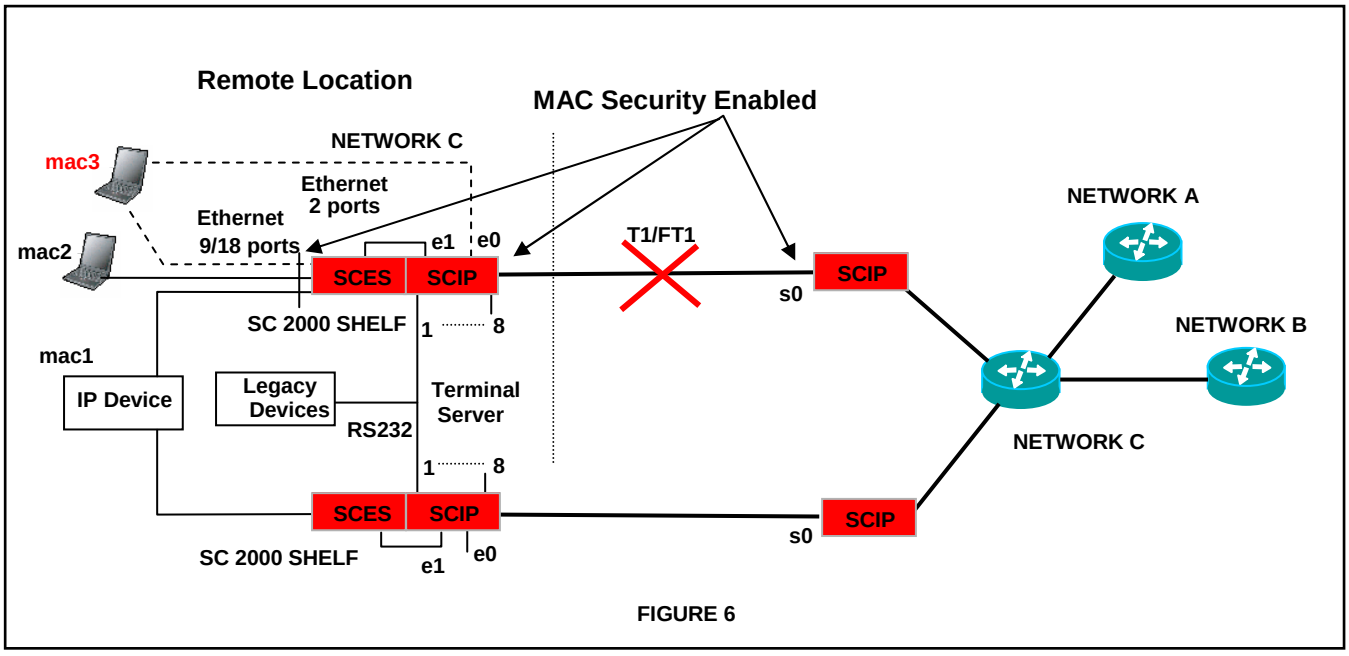

FIGURE 6