A WHITE PAPER FROM ENCORE NETWORKS

Migration Of Legacy Systems & Applications to Broadband IP VPN Infrastructure

September 2003 © Encore Networks, Inc.

Specifications are subject to change without notice.
Encore Networks, Inc. • 45472 Holiday Drive • Dulles • Virginia • 20166
Tel: 703-318-7750 • Fax: 703-787-4625 • Email: info@encorenetworks.com • Web:

encore!networks™

A WHITE PAPER FROM ENCORE NETWORKS

Migration Of Legacy Systems & Applications to Broadband IP VPN Infrastructure

What does "legacy" mean, and why are legacy protocols important?

Several characteristics of a protocol suggest the term "Legacy" should apply to it, particularly if the protocol was:

- Designed for leased line or TDM networks
- Organized as "master/slave" rather than "peer-to-peer"
- Not intended for "routed" networks (as were IPX/SPX, Vines, etc.)

More simply, they are older than the mass popularity of the Internet: all legacy protocols were in wide use before 1990.

Legacy protocols began as part of financial, business, and manufacturing systems built around mainframe computer;- with their proprietary communications methods. Businesses have long relied on these systems for mission-critical functions. In many cases up to the present, the custom software and specialized hardware deployed in these systems have no counterparts in off-the-shelf components based on IP; they can't be replaced easily.

Financially, many companies cannot afford to replace legacy protocols with IP because that step requires buying a large number of devices to replace equipment that isn't fully depreciated. Despite the reduced operating costs that an IP network might offer compared to leased lines, the savings don't match the capital expense and resulting depreciation for replacement hardware.

Examples of some widely deployed legacy protocols include:

- SNA (mainframe computers to terminals)
- BSC, Uniscope, Poll/Select, etc. (banking equipment, cash dispensing machines and ATMs)
- Airline Link Control and AX.25 (travel reservations, passenger records)
- SCADA (Utility operators, manufacturers/production lines).
- X.25 and Polled Async (lottery networks, Point Of Sale applications)

Everybody wants to update their computers and networks to IP--if there were no cost to do so it would be done by now. But conversion does carry costs. Even if the dollar cost of a new network is not a barrier to change, there are intangible costs. Operators of highly developed business systems understandably may not want to give up a legacy protocol that offers:

- High availability of proven, reliable technology for mission-critical transactions;
- Security against eavesdropping that private lines offer;
- Immunity from hacking and denial of service attacks on a private network;
- Low protocol overhead for efficient use of narrow-bandwidth links.

Their reluctance is under increasing pressure from the market, from equipment vendors, and from carriers--all are moving to IP-based equipment and services. As a result, enterprises and other end users increasingly find IP offers advantages over legacy protocols and leased lines:

- Lower monthly cost per site or for a given access bandwidth
- More accessible by new applications software
- Supported by all new hardware products.

Geographical coverage no longer favors any particular protocol. A site that can get a dedicated local loop from a local exchange carrier could as easily access IP services and use that loop for one end of a dedicated circuit. Almost any site served by plain old telephone service (POTS) can use it or ISDN for Internet access.

As part of carriers' migration strategy, for years they have increased the cost of leased lines to encourage customers to change to public networks--first ATM and Frame Relay, now IP. That trend will continue.

The large numbers of layoffs at every local and long distance phone company have removed many of the experienced technicians who installed and maintained leased lines--the time to provision new leased lines and to repair their faults will only increase.

Making the Move:

The remainder of this paper will address the problems of changing legacy systems from proprietary or older protocols on private networks to IP-based transmission services on public networks--with practical solutions that will:

- Overcome the cost issue of making the change;
- Eliminate intrusion threats from the Internet;
- Prevent disclosure of information (financial records, etc.).

To the question of what can best replace a private network, the short answer is a *Virtual* Private Network (VPN). The essence of a VPN is that one customer of a public network isolates its communications from all other users of that network in one of two ways: logical separation or encryption. Frame relay and Asynchronous Transfer Mode (ATM) have long offered VPN service based on virtual circuits. Each VC is logically isolated in each switch. Many IP-oriented networks offer similar isolation based on Multi-Protocol Label Switching (MPLS) or Generic Routing Encapsulation (GRE).

A "separation VPN" of permanent virtual circuits, GRE tunnels, or MPLS paths, often provides sufficient security for commercial traffic. However, they still hold at least the potential for interception of readable messages. With increasing concern about privacy, legal requirements to safeguard personally identifiable information, and various other threats, many organizations are seeking better security from encryption.

Ways to Go:

Most network services, new applications, and the latest hardware cater to VPNs for the Internet Protocol (IP). That leaves a large class of network users to face the problem of securing legacy protocols without the same universally offered services that exist for IP.

Public data services are optimized for just a few protocols: X.25, frame relay, cell relay, and IP packet forwarding. These networks do not support directly the full range of legacy protocols.

To use today's public data networks for a legacy protocol, the enterprise customer typically adapts the old protocol to the new network in customer premises equipment. Table 1 summarizes the available ways to perform adaptation. Each solution solves the problems of migrating between networks, but with various tradeoffs. Enterprises can choose solutions with different impacts on remote terminal equipment and central site hosts.

Table 1: IP VPN Options for Legacy Protocols

Legacy Protocol Handling	Features
1. Full Encapsulation	• Simple • Retains all protocol features • Polling protocols use lots of bandwidth
2. Encapsulation with Spoofing	• CPE participates in legacy protocol • Reduces WAN traffic (no Polls on WAN) • Can reduce response time, improve throughput
3. Protocol Conversion	• Allows old and new to coexist
a) At a remote site	• Confines legacy protocol to remote sites • Allows conversion of terminals on per-site basis • Permits update of central computer and software
b) At a central site	• Confines legacy protocol to central site • Lets legacy software operate with new terminals • Allows PCs to replace legacy terminals
4. Encryption	• Can combine with any of the above • Provides "secure tunnel" between end points • IP Security (IPsec) operates on any IP service • Compatible with IP/PPP on leased lines, IP/Frame, and IP/ATM

Protocol Encapsulation:

In this solution, the new network carries all of the legacy protocol's messages--transmission units, or characters--end-to-end (Fig. 1). The legacy equipment remains at both central and remote sites as they continue to operate as previously. The hosts and terminals cannot tell that there has been a change in the transport network.

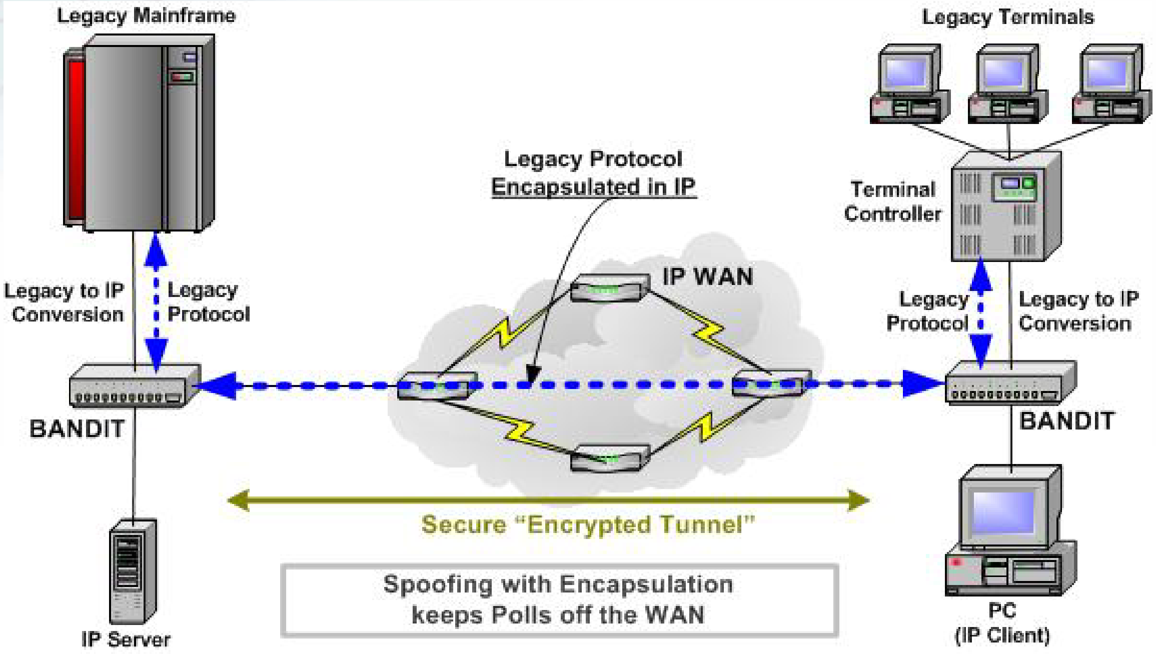

Fig. 1: Legacy Protocol Encapsulated in IP, with Optional Spoofing.

Avoiding any impact on installed equipment and computers, encapsulation also preserves all features of the legacy protocol and the system it runs on. This approach replaces leased lines with an IP service, nothing more. Everything else remains the same.

Spoofing:

Polling protocols (SNA, UNISCOPE, and others) use all of the bandwidth available on a line. If not transmitting data, the host computer is asking remote stations if they have anything to send or if they are ready to receive data. Most of this traffic is simply overhead as it carries no user information.

Smarter CPE not only encapsulates, it also understands polling protocols and can participate in them to prevent the overhead traffic from reaching the wide area network (WAN). The process, called spoofing, lets the mainframe in Fig. 1 think it is communicating with the remote terminal while, in fact, it is the CPE at the computer site that responds. (Actually, the central-site CPE pretends to be *all* of the remote terminals).

When the mainframe sends a poll to ask a specific terminal if it is ready to receive data, the co-located CPE answers immediately. At each remote site, the CPE independently generates polls to the terminals or controllers to assure them the connection is functioning and to gather information they have to send.

When the mainframe or terminal actually sends data, the CPE at that end of the connection encapsulates the data in a packet and forwards the packet to the other site. The CPE that receives the packet removes the data from the packet and injects the data into the polling cycle at the next appropriate point.

Neither end of a spoofed connection realizes that the polls are not crossing the network. Suppressing polls often saves significant amount of bandwidth.

Protocol Conversion:

Many commercial software applications originally were written for a specific legacy protocol. Remote terminals often had that protocol hard-wired into their circuit boards. Adding a TCP/IP protocol feature to the central application software doesn't require a new mainframe computer, but often there is no way to add IP to the remote hardware.

In these situations, the optimum solution for a migration to an IP network lets the mainframe speak native IP to the (IP) WAN. On IBM systems this technique bypasses the Front End Processor (FEP) that ran the Network Control Protocol, and so is called "NCP bypass." At the remote sites, an inexpensive protocol converter interprets the legacy protocol in IP terms, so the old terminal hardware (3274 cluster controllers, for example) continues to work with the new version of the mainframe application software, now communicating over IP (Fig. 2).

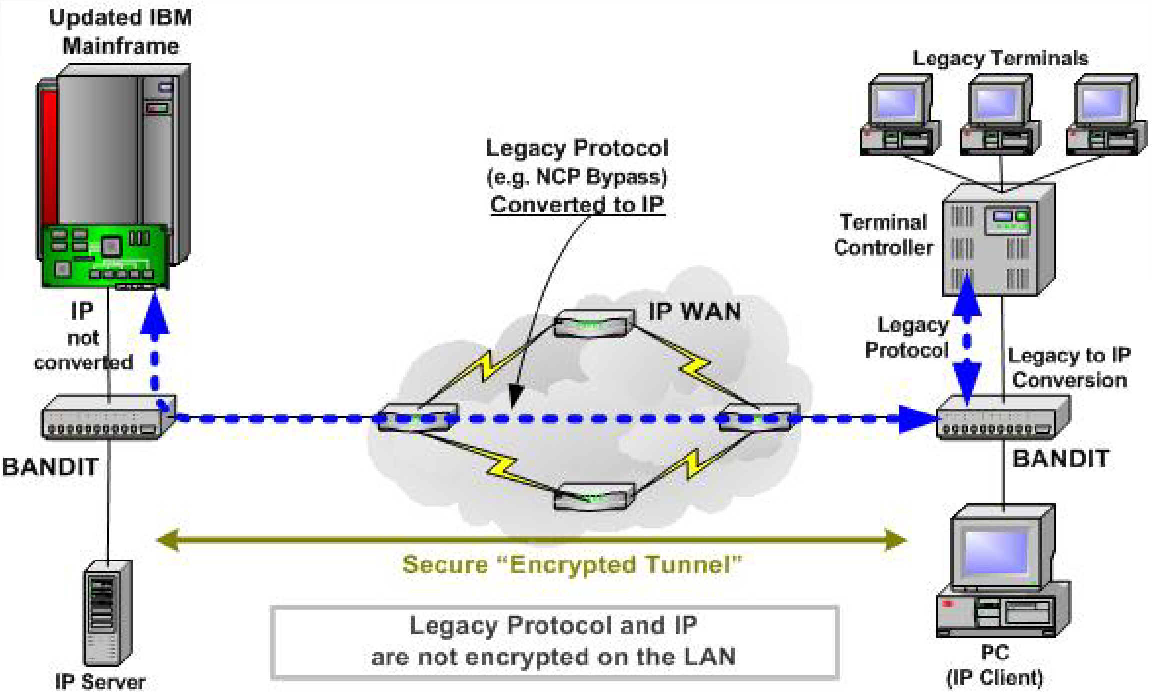

Fig. 2: Protocol Conversion at Remote Terminal Sites.

Conversion of a legacy format to IP format near the remote legacy terminal hardware confines the legacy protocol to specific remote sites. Once the central computer is moved to the newer IP protocol, the enterprise may convert each of the remote sites, or even each remote terminal, individually and only as needed. The enterprise can continue to draw on the satisfactory performance of existing terminals and specialized devices such as check proofers, reservation terminals, and industrial controllers. There is no need to replace a large number of remote devices at one time.

Some organizations turn this example around. They retain a mainframe, existing business software, and a legacy communications protocol at the central site. A protocol conversion platform transforms WAN traffic into a standard IP-based format, compatible with the Internet and any IP network service. The standard IP capability for the host computer is put in place before changing any remote terminals, which continue to operate over a private network or leased lines. Once the central protocol conversion is ready, remote terminals can give way to new equipment (typically personal computers), again on a per-site basis when convenient or affordable.

Encryption:

To keep communications private while transporting information on a public network, the certain solution is encryption, which affords greater privacy than a leased line. The standardized process and format for encryption on the Internet is "IP Security" (IPsec). It is flexible enough to support various algorithms and key handling methods.

By virtue of the encryption applied to an IP connection, that connection becomes a "secure tunnel" between sites. That is, encrypting the legacy protocol (only the parts that pass over the WAN) before encapsulating in IP makes any IP service--public or private, including the generic Internet--a secure VPN for any legacy system.

Hiding the content of the payload means there is no need for isolation on a virtual circuit. Any IP network that delivers IP packets can support an IP VPN based on encryption (Fig. 3). Until all IP networks offer assured quality of service, some users will continue to want a virtual circuit to carry IP packets because the VC can be configured with a guaranteed throughput, priority level, or other desired performance characteristics.

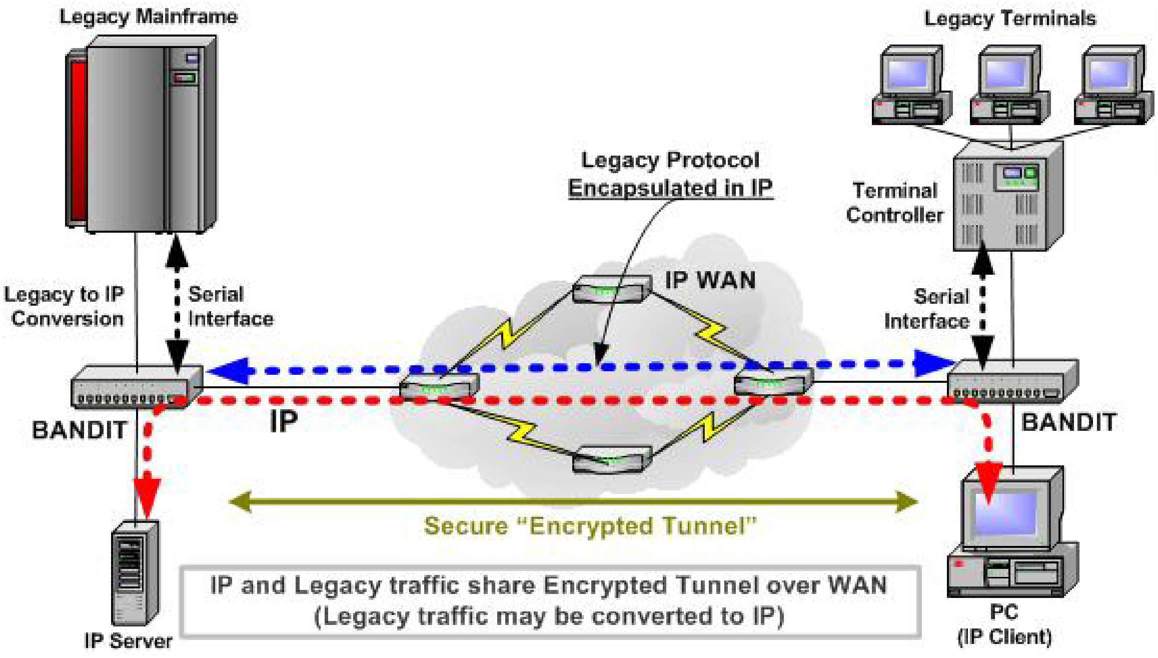
Legacy Mainframe
Legacy Terminals
Legacy Protocol Encapsulated in IP
Terminal Controller
IP WAN
Legacy to IP Conversion
Serial Interface
Serial Interface
BANDIT
IP
BANDIT
Secure "Encrypted Tunnel"
IP and Legacy traffic share Encrypted Tunnel over WAN (Legacy traffic may be converted to IP)
IP Server
PC (IP Client)

Fig. 3: Encryption Creates a "Secure Tunnel" Between End Points.

Encryption applied to the payload of an IP packet does not prevent that packet from operating on FR or ATM as well as over any MPLS or IP network. Where an encrypted VPN is the solution chosen, both native IP applications and legacy protocols converted to or encapsulated in IP can share the same secure tunnel.

The strong isolation provided by permanent virtual circuits on FR and ATM reduces the occasions when encryption is needed on those services. With the trend toward IP, most questions and the greatest interest in VPNs focus on pure IP transport. For example, the initiative to use Ethernet on local loops is a pure IP service.

Some business applications may not need high security. For them, legacy protocols may be transported whole (simple encapsulation). "Spoofing" and protocol conversion reduce the traffic volume on the wide area network by confining "chatty" protocols to end sites. Suppressing control messages that carry no new information thus reduces the encryption workload.

A VPN Solution from Encore Networks:

Encore Networks has in-depth experience with the full range of legacy protocols, general purpose and customized protocol conversion, and encapsulation devices for many years. Its Frame Relay Access Devices (FRADs), access routers, and protocol converters operate in many networks and customer sites worldwide.

The **BANDIT™ (**Broadband Access Network Device for Intelligent Termination) is the latest and most flexible platform Encore has produced. It combines routing, firewall, Network Address Translation, hardware encryption acceleration, and integral CSU with full capabilities for the entire range of legacy protocols. A flexible architecture permits almost unlimited configurations involving multiple encapsulations and encryption to solve the most unusual problems.

Complete remote management features support phased migrations between wide-area transport technologies. For example, to convert an X.25 network to IP, the BANDIT could first act as an X.25 switch, then transport X.25 over Frame Relay, or encapsulate the legacy protocol directly in Frame Relay. When the terminal changes, the same BANDIT can carry IP over Frame Relay, then IP over PPP on an IP network. All these functions are available via remote configuration, in the same software load, on a single hardware platform.

Encore has a long history of applying this flexibility to global reservation networks, state lottery networks, banking networks, SCADA-based utility networks, and most recently satellite networks.

The BANDIT solves several problems specifically associated with legacy protocols migrating to IP backbones:

- Low unit cost for the BANDIT justifies retaining legacy terminal equipment through its full useful life.
- "Plug and Play" features, customizable factory defaults, NAT, and Private AT (supports overlapping IP address ranges at both ends of a connection) simplify deployment
- SLE-based (Selective Layer Encryption) VPN solution that interoperates with different TCP accelerators to provide IP VPN services over satellite networks.
- Integral V.90 modem or BRI interface for dial backup and quick fail-over to alternate IP service ensure high level of survivability and availability
- Router functionality and integral CSU/DSU eliminate separate devices and cables to reduce costs and simplify maintenance
- Compatible with third-party large-capacity VPN IPsec devices at central sites; solution scales up to very large networks.
- Highly manageable from standard NMS over any link, including the integral modem (ideal for carrier-managed services)

Specifications are subject to change without notice.