Engage Communication

Secure Communication

The exponentially accelerating use of public networks to facilitate private communications is exposing vital information to eavesdropping, tampering and regulatory compliance violations. In addition the conversion of Voice and Video to IP reveals intimate details of an enterprises telecommunication, perimeter surveillance and video conferences to easy observation with shareware packet sniffers.

Then there is the false sense of the security of Private Networks. Private Network Service provider networks, such as Metro Ethernet and Telco WANs, have unmanned facilities or minimal security at manned locations. Access to interconnecting circuits can be obtained at Telco Switching locations or at a multi-tenant building's common phone closet. Network service providers utilize collocated common equipment that is maintained by un-vetted technicians. Increasing innovative industrial espionage among highly competitive businesses requires that extensive security measures are employed.

Enterprises are experiencing network attacks that seek to obtain the most important or profitable sources of information including:

· Customer Records

· Employee Files

· Source Code

· Intellectual Property

· Accounting Forecasts

· Formulae

· Marketing Plans

· Sales Strategies

· Financial Spreadsheets

Stringent information security standards are mandated by a variety of legislative actions, including the Health Insurance Portability and Accountability Act, Sarbanes-Oxley, California Database Security Breach Act, the Gramm-Leach-Bliley Act, EU Data Protection Directive and the Federal Information Security Management Act.

"With the threat of a data breach looming large over every corporation that handles sensitive information, encryption has become the No. 1 answer to the question, 'How do I protect myself?' Then there are the mandates -- the Health Insurance Portability and Accountability Act, Graham-Leach-Bliley, Sarbanes-Oxley, the Payment Card Industry data security standard, and other regulations -- that require data protection, for which encryption is again the obvious answer." – Network World (10/2007)

Encryption is the key to ensuring confidentiality, data integrity, and accountability. Advanced Encryption Standard is the government approved solution for protecting Data, Voice and Video transmissions. AES, specifically using 256 bit keys, offers the enterprise network a secure method for transmission of confidential and secret corporate and government information.

AES encryption meets the new security requirements for:

- **Highly Competitive Businesses**
- **Department of Defense - Air Force, Army, Navy, Marines**
- **National, State and Local Governments**
- **Public Safety Networks**
- **Homeland Security**
- **Law Enforcement**
- **Multi-Site Commercial Enterprises**
- **Banking and Financial Institutions**
- **Health Care Industries**
- **Natural Gas & Electric Power Utility Companies**
- **Transportation Agencies**

Encryption

The Engage **Black·Bond** and **Black·Door** products ensure the confidentiality and integrity of Intranet and Internet networks with the strongest commercially available cryptography that provides a secure and cost-effective solution for voice/video/data encryption that is compatible with VoIP, Video over IP, Multicast and other latency-sensitive applications.

Despite the importance of encrypting sensitive or confidential information over a network many business and governmental organizations send information in clear text. A company's formal policy may demand encrypting sensitive or confidential information in transit but managers routinely fail to comply with this mandate. The most typical reasons are:

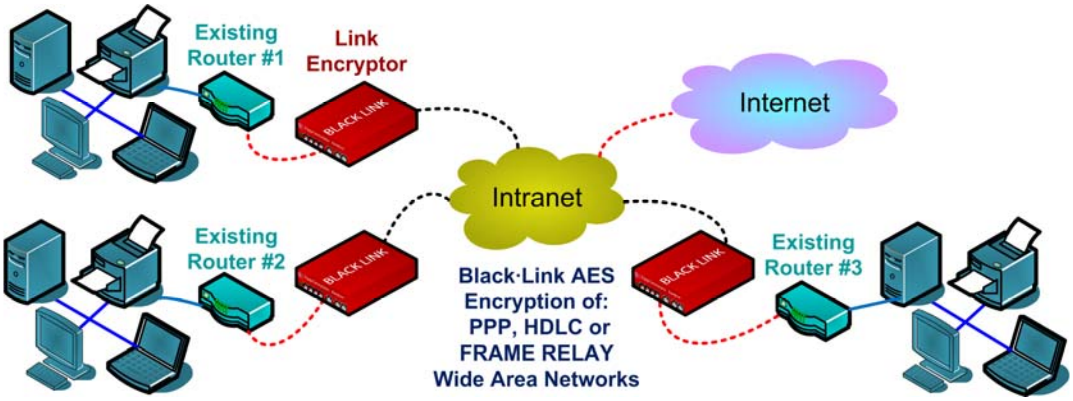
- Encryption methods are too complex to use properly
- Encrypting and de-encrypting information impacts productivity
- Managing of encryption keys
- Lack of qualified resources
- Cost to implement the required Encryption

Engage Communication's packet and circuit Encryption solutions are purpose built encryption appliances that take the **cryptic** out of cryptography.

Unique Approach to Wide Area Network Encryption

The **Black·Link** splices in an AES hardened payload encryptor between an existing WAN Router/Bridge and the egress point of the Circuit. The configuration of the Router/Bridge does not require modification.

The **Black·Link** is also able to operate at the Network Layer 3. The **Black·Link's** integrated Router can be configured to only encrypt the Routes to Intranet Sites. The packets that default to the Internet are not encrypted.For point to point layer 2 Wide Area Networks the **Black·Link** installation is a cable swap and connect. Ease-of-implementation there is no need to reconfigure routers or other network devices.



The **Black·Link** eliminates major hurdles to implementing encryption especially in contrast to the overhead, latency, and complexities of implementing a VPN encryption configuration in the WAN Router. The cost of reprogramming a WAN router can easily exceed the cost of the **Black·Link**.

The **Black·Link** is a Serial Data Link AES Encryptor that encrypts serial protocols such as SDLC, HDLC, BDLC, LAPD/PRI, SS7, X.25, Point to Point Protocol and Frame Relay. The Encryption is done at the Data Link Layer 2 or at the Network Layer 3. The **Black·Link** has models with T1, E1, RS232, RS530, RS449, V.35 or X.21 interfaces.

Ethernet Encryption

Every aspect of public and private communications security needs to be under scrutiny. From private infrastructure to shared public networks, the considerations for security are essentially the same.

- Is the Data, Voice or Video transmission secure and protected?
- Is compromised encryption technology being relied upon such as DES or 3DES?
- Does the encryption solution marginalize the capabilities of the primary equipment?
- What are the consequences?

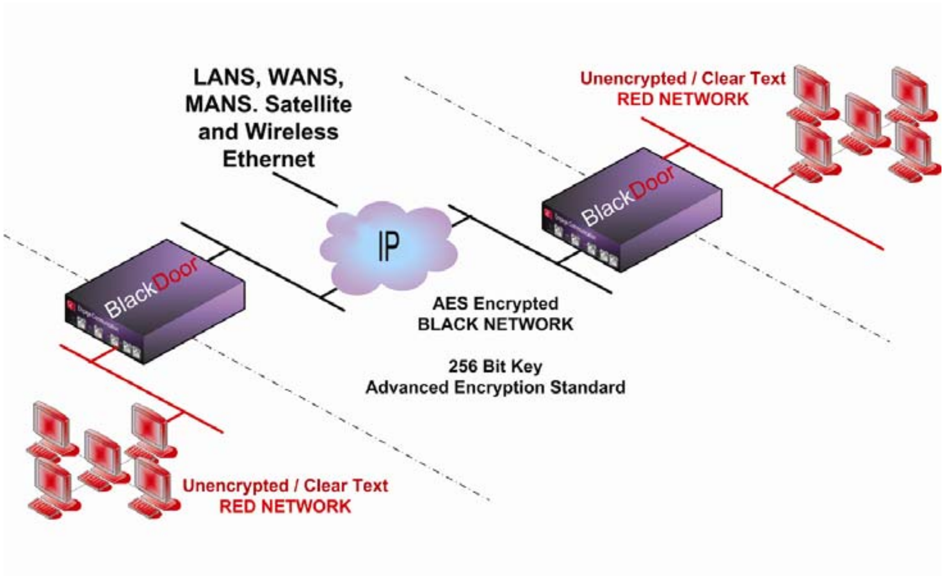
Engage's **Black·Door** transparently AES encrypts Ethernet Voice, Video or Data packets. The **Black·Door** operates in transparent bridge, VPN, tunnel or route modes.

As a transparent bridge all but the MAC layer is encrypted. This mode of operation is well suited for shared wireless networks such as Wi-Fi, or in LAN environments where the layer three protocols may not be IP. Bridging mode also protects network segments within an organization such as separating accounting from marketing.

In tunnel mode a LAN segment is "tunneled" through a public or private network allowing a transparent bridge through any IP cloud. In route mode, individual encrypted routes are built to allow traffic flows over public or private IP networks. The unencrypted LAN segments at each end point can have unique keys to other remote peer networks. This method of operation has many applications in private enterprise as well as the public sector.

Ethernet Encryptor

*The **Black•Door** Ethernet Encryptor, which supports Point to Point and Multipoint information assurance configurations with unique dynamic keys, is specifically designed for real time wireline backbones and the full spectrum of Wireless WAN technologies including: Free Space Optics, licensed and unlicensed Radios.*


LANS, WANS, MANS. Satellite and Wireless Ethernet
Unencrypted / Clear Text RED NETWORK
BlackDoor
IP
BlackDoor
AES Encrypted BLACK NETWORK
256 Bit Key Advanced Encryption Standard
Unencrypted / Clear Text RED NETWORK

Self Configuring

Auto learning functions such as DHCP allow mobile use of the **Black·Door** permitting end user mobility and ease of use, ideal for road warriors, mobile operations, and temporary installations.

The **Black·Door** and the **Black·Bond** also have the sophistication to support complicated full-mesh point to multipoint layer 2, VPN or layer 3 topologies. Engage supplies configurations for each topology and also offers drop ship pre-configuration.

Circuit Encryption

The **Black·Bond T1** or **Black·Bond E1** circuit encryptors are truly transparent to the network users. As they are installed at either end of a high-speed circuit they appear like a standard CSU. They are designed to assure no loss of bandwidth and minimal latency. The **Black·Bond** products are suitable for real time applications such as broadcast, surveillance or conference video or voice. By providing the user a method for circuit encryption, the Engage products offer a unique alternative for T1 or E1 secure transmissions.

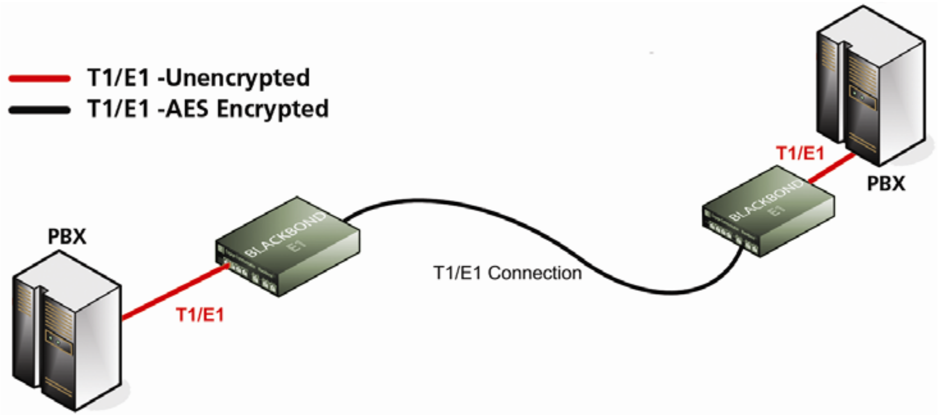
Engage's **Black·Bond** Link Encryptors support a full range of Telecommunication and Networking equipment:

- WAN Routers and Bridges
- PBX trunks, Codecs
- Multiplexers
- PBXs Phone Switches

TDM Circuit Encryptor

AES Circuit Encryption is employed to prevent interception, tampering and disruption of public or private communication channels.

*Engage's **Black·Bond** T1/E1 Link Encryptor utilizes the AES to secure secret and sensitive information transmitted over point-to-point or dial-up T1/E1 communication links.*



Note: The Black·Bond is a very unique solution for encrypting Voice

Voice Encryption

Black·Bond is inserted between the Phone System's T1/E1 interface and the T1/E1 circuit. The **Black·Bond** operates at the Layer 1 or Layer 2 or Layer 3. In Layer 1 mode the **Black·Bond** encrypts T1/E1 frames. Voice timeslots within the T1/E1 frames are AES encrypted. The signaling channel, which can be PRI, SS7 or Proprietary, is unencrypted.

Encryption of interoffice voice calls eliminates wiretapping at unsecured phone closets and telecom service provider monitor jacks. **AES Circuit Encryption** is employed to prevent interception, tampering and disruption of public or private communication channels. The need to employ end to end circuit encryption is a top priority for organizations that are aware of their vulnerability. Circuits from the Phone Company are commonly thought of as private and not accessible or requiring sophisticated equipment to tap.

Ready Access to Communication Channels

The vast majority of Telephone calls, Data networks and Video for Surveillance or Conferencing are interconnected over Time Division Multiplexed - TDM circuits from Regional Bell Operating Companies - RBOCs or Postal Telegraph and Telephone - PTTs.

Access to these interconnecting circuits can be obtained at the Telco Switching locations. There are numerous Telco switching centers that are unmanned and security at many of the manned locations is minimal and not in place 24 hours per day. Easily thwarted physical security provides ready access to the Telcos built-in TDM diagnostic circuit monitoring jacks.