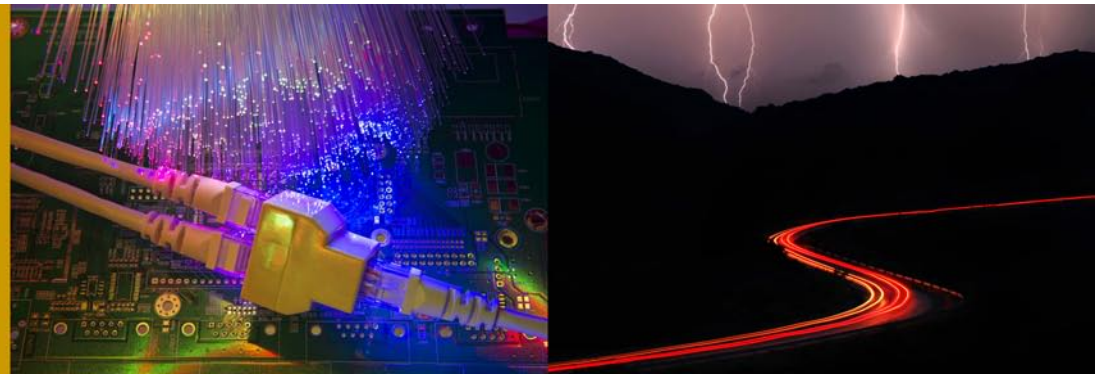
CONNECT

PROTECT



SECURE

Engage Communication

Communication, Networking and Security Solutions for Defense

Engage Communication provides **Defense**, **Homeland Security** and **Intelligence Communities** with innovative and cost effective solutions that connect network elements, protect critical circuits, and secure network traffic and cryptographic keys. We have a quarter-century of experience developing, manufacturing, and supporting solutions that are critical to our customers' operations.

CONNECT Migrate from Circuit-based to Packet-based Networking

- Interconnect PBX, Channel Bank and T1 MUXes with Ethernet packet networks
  - Serial -RS232 - 4-Wire - T1 - E1

CONNECT Type 1 Bulk Serial Data Encryptors over IP/MPLS Networks

- Convert KIV-7, KG-84 Serial Interfaces into Ethernet

CONNECT Seamlessly Transition from End of Life ATM to IP

- Interconnect PBX, Channel Bank and T1 MUXes via IP packet networks
- Convert Synchronous and Asynchronous Serial connections to Ethernet

PROTECT Protect Mission Critical T1 Circuits and Serial Connections with Automatic Failover Switch

- Missile Defense Connection Protection
- UAV Serial Control Redundancy
- Backup Land Mobile Radio (LMR)
  - 4G cellular data networks - MPLS - Metro Ethernet

SECURE Voice, Video and Data Encryption

- COTS encryption for securing sensitive military and government telecom and packet networks.
  - T1 Circuit - Ethernet Packet - RS232 Serial

SECURE Implement FIPs Assured Cryptography

- Secure cryptographic keys for provisioning encryption, decryption, authentication, and signing
  - Expedite Regulatory Compliance Audits - VPNs - Certificate Authority

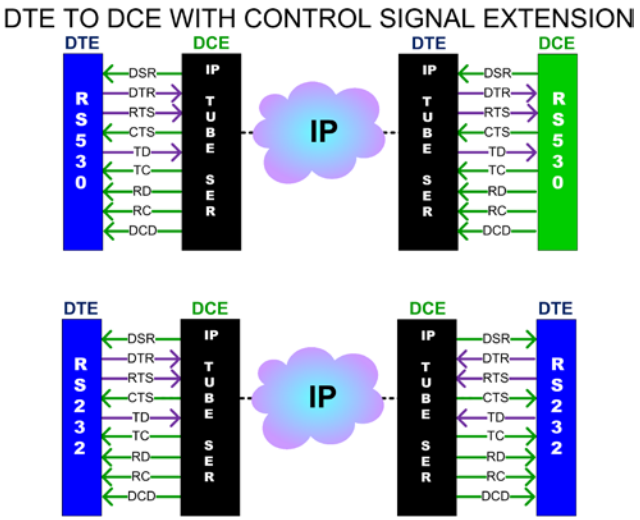
SECURE Secure Computing Platform

- Handheld FIPS pending Application Processor with Integrated Trust Path
  - 2-Factor Authentication - Tamper Reactive: Die Shield, Temp & Voltage - Touch Screen

CONNECT SERIAL DATA EXTENSION over PACKET SWITCHED NETWORKS

SITUATION

C4 Communications and Computers use Serial Data connections, transported over telecommunication circuits, for Command and Control of military systems. Increasingly, these connections are being replaced by IP packet networks due to the End-of-Life of ATM and other technology / availability changes. Thus, defense organizations are required to develop new networking strategies while managing overall cost, reliability and operational disruption.

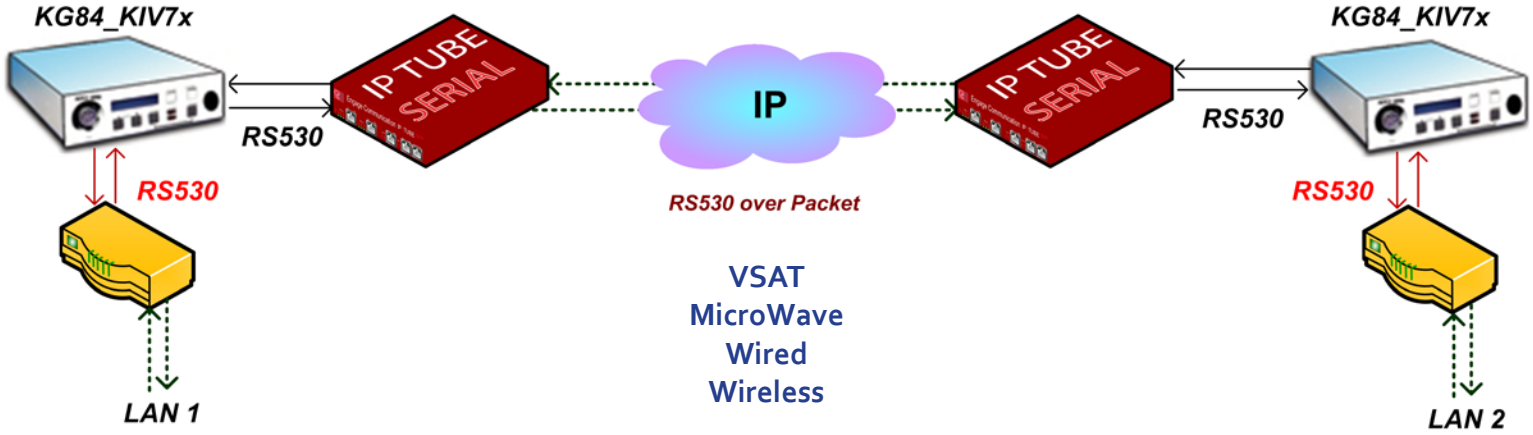


SOLUTION

One of the primary areas of focus is enabling Serial Encryptors to communicate over IP networks. Engage's **IP•Tube SER** product line seamlessly converts Type 1 encryptor traffic to IP without change to the cryptographic boundary or SOP. The **IP•Tube SER** supports a wide variety of applications including RS232, RS530, RS422, and V.35 data and control interfaces, sync and async operation, and data rates from 75 bits to 16 megabits per second.

RESULT

- Migrate from DISA End of Life ATM to IP Packet
- Transport Legacy Serial Connections over ubiquitous Packet Services
- Convert Type 1 Serial Bulk Encryptors into Ethernet
  KIV7, KG84 & OMNI to Ethernet Packet Converter
- Redundant and diverse connectivity for **Serial** communication

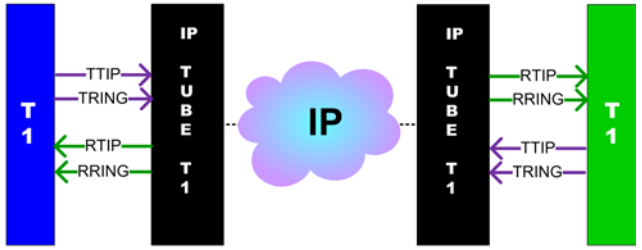


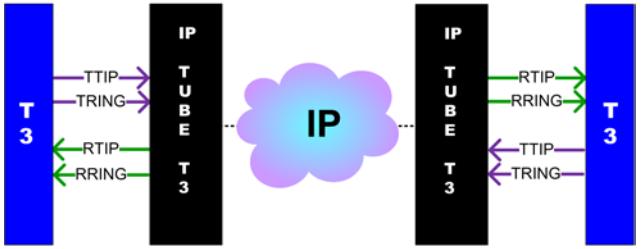
CONNECT TRANSITION TDM CONNECTIONS to PACKET NETWORKS

SITUATION

T1, E1, E3 and **T3 T**ime **D**ivision **M**ultiplexed circuits are utilized to interconnect voice, video and data systems between remote locations. TDM telecommunication services providers, such as DISA, utilize ATM technology to provide the connectivity.

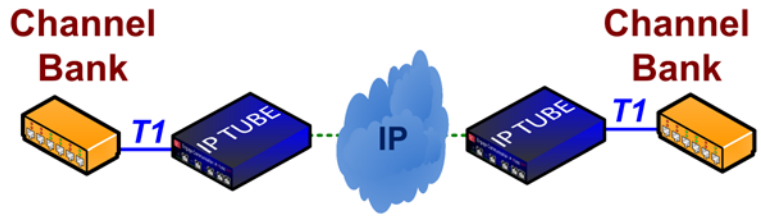
The broad availability of Ethernet / IP networks, ease of connectivity with MPLS and VLAN services, and predictable performance enabled by higher speeds and quality of service, have allowed packet networks to push ATM to the brink of extinction while displacing an increasing number of SONET networks.

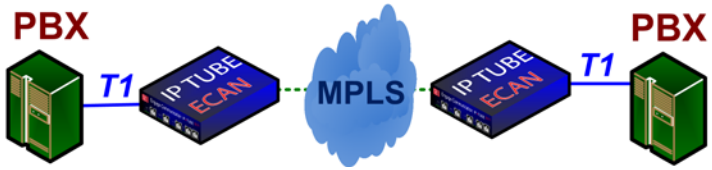




SOLUTION

When migrating to packet networks, continue to utilize existing circuit-based equipment with Engage **IP•Tube T1** and **T3** circuit to packet conversion solutions. The **IP•Tube** converts **T1/E1** or **T3/E3** signals from a wide variety of telecommunication equipment to packet format, while maintaining the integrity and timing of the original circuits across the packet network.





RESULT

- Continue to use existing Telecommunication equipment
  - **PBXes** - **Channel Banks** - **Multiplexors**
- Seamless transition to future-proof connectivity
- Inherent support for Diverse Path Redundancy
- Eliminate leased lines charges: ROI measured in weeks
- Reduce reliance on 3rd parties for network availability
- Maintain current operational procedures

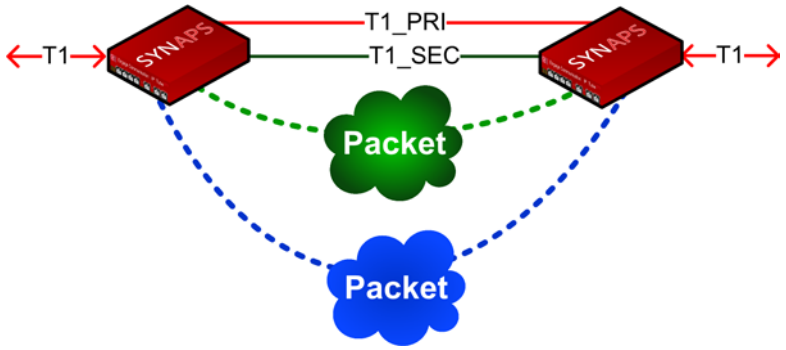
PROTECT PROTECTION of MISSION CRITICAL T1 COMMUNICATION

SITUATION

T1 circuits that provide Mission Critical connectivity require automated redundancy to ensure uninterrupted communications.

SOLUTION

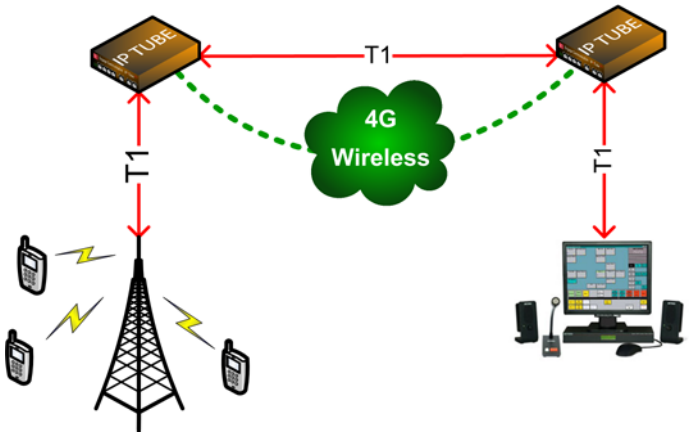
Keep critical T1 Voice, Video and Data systems fully operational when the primary path fails with Engage network protection solutions. Upon detection of a network fault, traffic is automatically switched to a redundant circuit or packet network. Multiple backup networks are supported.



RESULT

- Proactively Protect Mission Critical T1 Circuits
- Switch T1 to multiple redundant circuit or packet networks
- Deliver on Stringent Service Level Agreements

PROTECT BACKUP CIRCUITS over 4G CELLULAR



SITUATION

T1 circuits used in Military Police, Fire, Medical Response and other defense based Land Mobile Radio (LMR) networks can experience outages and insufficient quality of service when needed most.

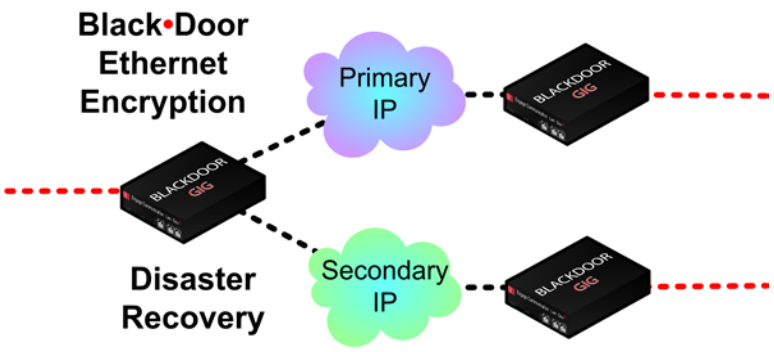
SOLUTION

Automatically switch critical T1 circuit from failed T1 connection to 4G cellular network with Engage **IP•Tube Link Protector**. Only pay for cellular bandwidth when in protection mode. Also supports redundant backup Satellite, MPLS and IP networks.

RESULT

- Ensures Warfighters have access to **critical circuit based infrastructure**
- Disaster Recovery for **T1** based **LMR** Networks
- Ensures communication after natural and man-made disasters

SECURE ENCRYPT ETHERNET VOICE, DATA, & VIDEO



SITUATION

Mission Critical information transported between Ethernet/IP based Networks must be secured. This information is often transported using wireless technology making it even more susceptible to interception and the need for encryption that much greater.

SOLUTION

Engage Black-Door Packet encryptors provide AES encryption for 10Mbps / 100Mbps / 1Gbps Ethernet carrying Layer 2 and Layer 3 Video, Data and Voice traffic. **Disaster Recovery** configuration automatically detects failure with the Primary connection and switches to a proactively monitored Secondary

RESULT

- Ethernet frames are kept Secret during transport
- Redundancy is proactively delivered
- Easy to implement End to End AES 256 Encryption Envelope

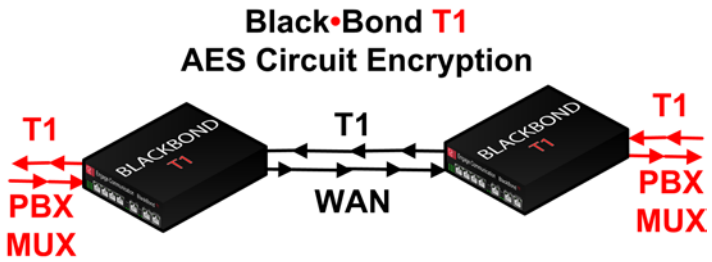
SECURE CIRCUIT ENCRYPTION

SITUATION

T1 and **E1** Circuits are used to interconnect data networks and phone systems. Sensitive and Secret information whose privacy is critical to the success of the mission is transported in the clear across easily tapped junctions.

SOLUTION

Encrypt T1 / E1 circuits using Engage **Black•Bond** link encryptor. Utilizes powerful AES encryption, with unique low latency / transparent capabilities to support voice, video and data traffic. Also allows for encrypting individual T1/E1 timeslots



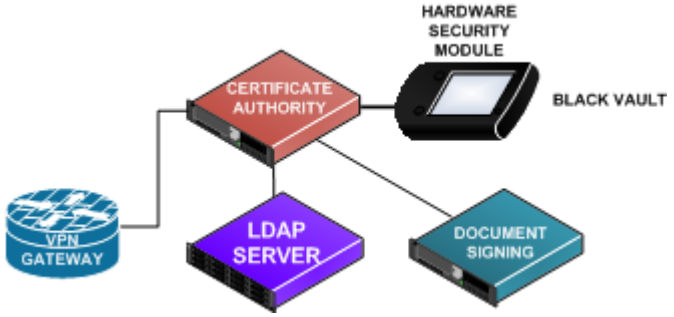
RESULT

- Sensitive and Secret Conversations are kept private
- Data in transit is encrypted at Layer 1
- Video Conferences restricted to "need to know" basis only

SECURE CRYPTOGRAPHIC KEY MANAGEMENT and SECURITY

SITUATION

Cryptographic keys are used for Virtual Private Networks (VPNs), Certificate Authorities, and critical information. Crypto keys are easily accessed and exploited on hard drives and OS memory since they are unique prime numbers of known length. Implementing encryption is for nought if the keys are accessible.



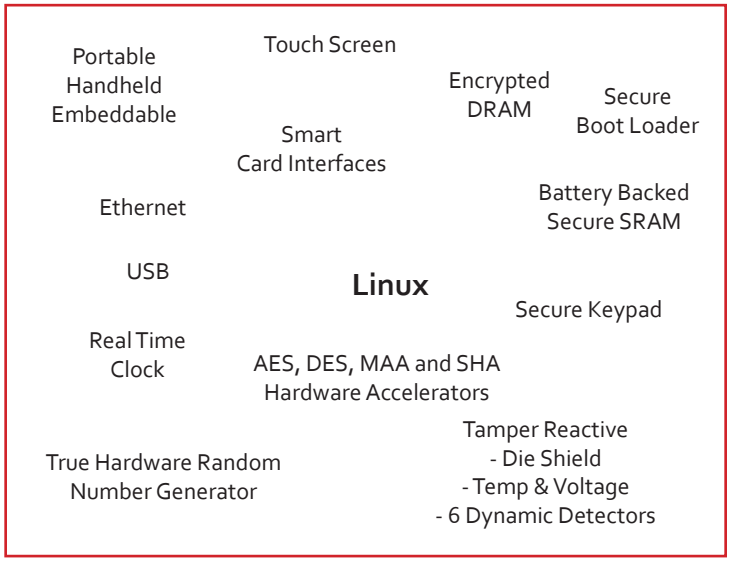
SOLUTION

Create, store, and manage cryptographic keys with the Engage **Black•Vault**, a hardend, tamper-reactive Hardware Security Module that performs secure cryptographic key protection, processing and management.

RESULT

- Cryptographic Keys are Secure
- Multi-Factor Smart Card authentication restricts access
- Centralizes the management of cryptographic keys, from distribution to termination and archival, in a highly secure hardware appliance

SECURE SECURE COMPUTING PLATFORM



SITUATION

Mission Critical applications are being executed on vulnerable computing platforms. Encryption keys are in the clear. Security routines are sharing resources with unvetted code. Insecure single factor authentication.

SOLUTION

Engage **Black•Vault** crypto processing ensures that critical security processes are secure. Critical Security parameters are encrypted within a Tamper Reactive Die shielded zeroizable memory.

RESULT

- Execute application code within a secure tamper reactive environment
- Mission critical applications are protected against unauthorized access, manipulation and theft..

CONNECT	PROTECT	SECURE
Convert Telecom Interfaces to IP	Mission Critical Infrastructure Circuits	Cryptographic Keys
KIV7 / KG84 to Ethernet Converters	Automatic Protection Switching	Critical Information
Land Mobile Radios to Ethernet	Land Mobile Radio Redundancy	Data in Transit
Transition End of Life ATM to IP	Satellite Packet Backup of Circuits	Voice, Video & Data

Focus on Customer ROI

Whether it is transitioning from ATM to IP, extending the life of military encryption gear, automatically protecting mission critical circuits with Ethernet services, or encrypting sensitive voice, video and data for secure communication, we help our customers meet their network, capital, and operational cost objectives.

We're an equal opportunity innovator; solving specific telecom, networking and network security problems for government, military, telecom, utility, enterprise, and first responders.

ABOUT ENGAGE

Since 1989, Engage Communication has developed innovative products and solutions that enable organizations across the globe to deploy and operate cost-effective, reliable, and secure communications.

We combine an experienced and responsive engineering team, highly scalable manufacturing resources, and a "whatever it takes" customer service philosophy to meet the demanding needs of our customers.

- **Over 24 Years of Expertise in:**
  Telecom, Networking and Security
  - Proven Products
  - Superior Support
- **Responsive to Customer Objectives:**
  Unique and Agile Adaptation
  - Optimized Solutions
  - Comprehensive Results

Engage Communication

1.877.ENGAGE4 • +1.831.688.1021
9565 Soquel Drive • Aptos, Ca 95003
sales@engageinc.com • www.engageinc.com

Designed, Fabricated, Assembled & Tested in America