The Critical Messaging Gateway (ITS-LX) Application

The Critical Messaging Gateway (ITS-LX) is the Nucleus of American Messaging Service's Critical Messaging System.

The Internet Telephony Switch – Linux (ITS-LX) is basically a modern version of what in the messaging industry is called a "Paging Terminal" or "Paging Switch". It's a messaging application platform that runs on a Linux OS based server that allows for inbound messages, using various messaging protocols, e.g., SNPP, WCTP, Email, TAP and Telco Trunks via SIP or (T1 or POTS), and converts them to an output protocol.

Typically, American Messaging Service's uses Telocator Network Paging Protocol (TNPP), which is a standard messaging protocol, for output to the messaging encoder systems. Messages can be sent to the local messaging encoder, the wide area messaging encoders or both for dual frequency pagers.

The diagram below (Fig.1) shows the different input and output protocols:

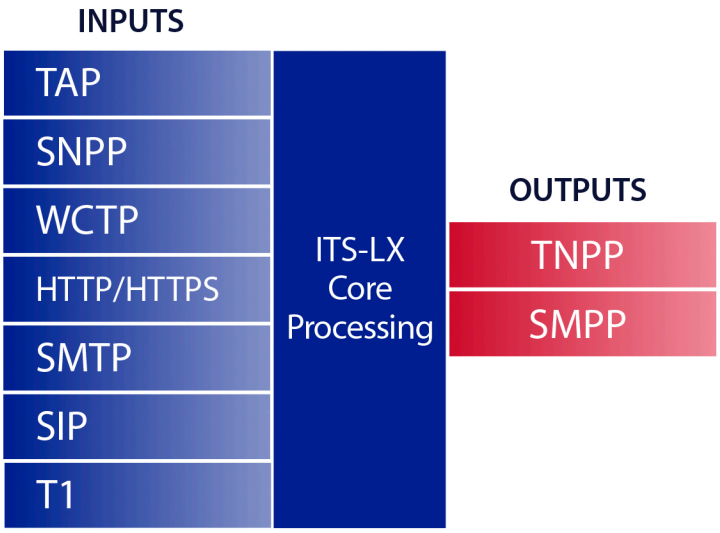

Fig.1: American Messaging Service's input and output protocols.

The ITS-LX switch is a modern day replacement for the Glenayre (GL-3000) messaging terminal/switch. It provides improved functions as well as new functionality:

- Standard server/hardware platform
- Smaller footprint; 1 to 2 rack units per server (1 ¾" to 3 ½" of rack space)
- Hardware can be easily scaled depending on system requirements
- Provides SIP/VoIP functions
- Provides for encryption to accommodate advanced clinical system integration capabilities

Benefits:

- Easier to maintain and support
- Redundancy which provides high reliability
- VoIP capable for improved network interconnection reliability and efficiency
- Uses modern network and server technologies

The Critical Messaging Gateway is the nucleus of American Messaging Service's Critical Messaging System. The diagram below (Fig. 2) shows a critical messaging system and how it is connected to the American Messaging wide area network and the local network:

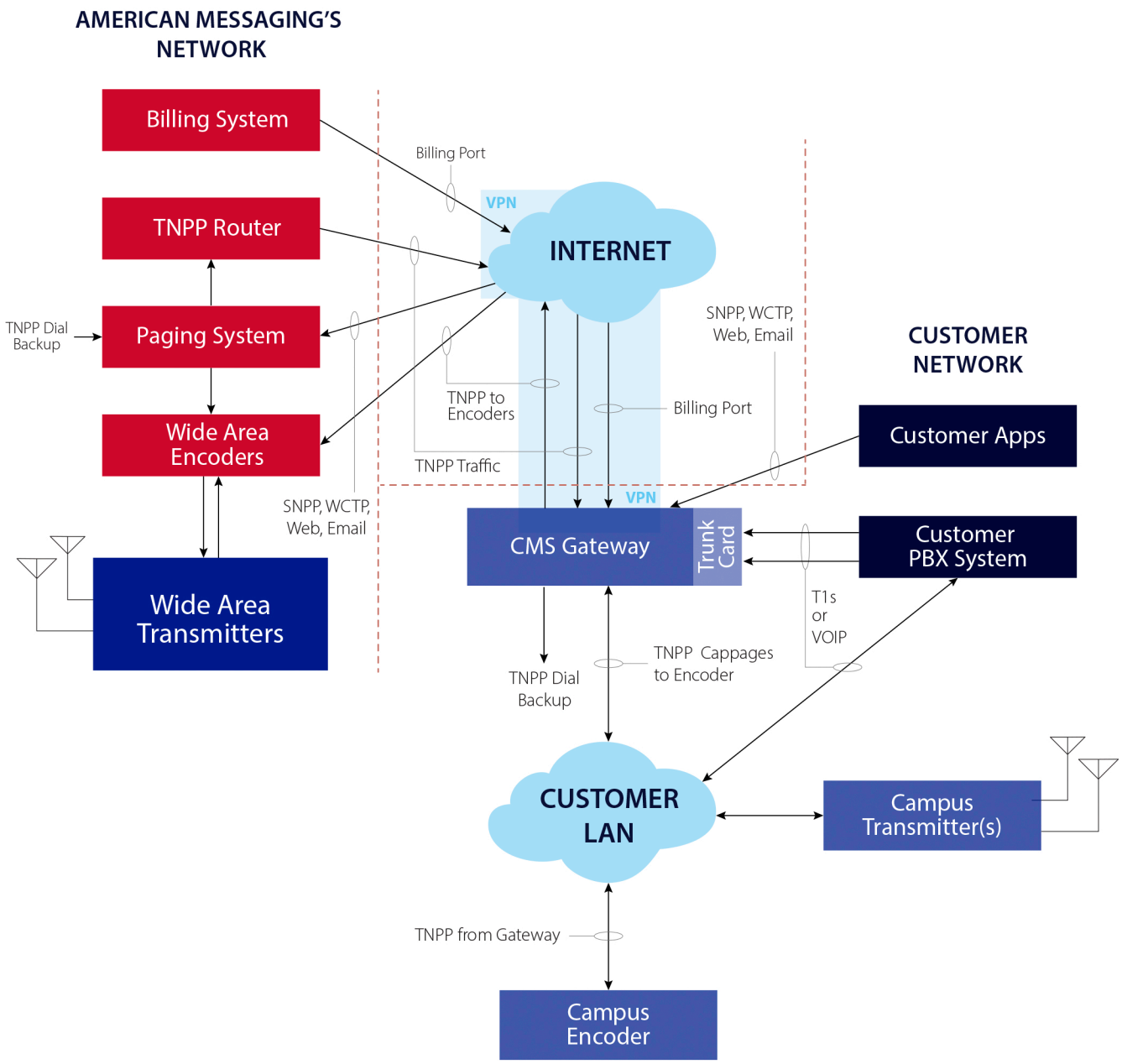

Fig.2: An example of a Critical Messaging System connected to the American Messaging wide area network and the local network.

While not shown in the above diagram, there is a VPN Firewall located between the internet and the Critical Messaging Gateway (ITS-LX) that is used to connect the Critical Messaging System to American Messaging's network over the internet using a secure connection.

The American Messaging billing system is used to provision the Critical Messaging Gateway, however once provisioned, the Critical Messaging System becomes a standalone campus messaging system.

The system can also be configured for redundancy by using separate Critical Messaging Gateways with separate internet connections.

Referencing the above diagram (page 2), and from a customer's perspective, the Critical Messaging Gateway provides the following on-campus interfaces for messaging functionality:

- Interfaces, via SNPP or WCTP, to client applications for SPOK, ISS, InfoRAD, PageGate, Amtelco
- Email (SMTP) input from the customer's email system
- Webpage that allows integration into the customer's employee/intranet website providing a custom "Send-A-Page Webpage" for sending critical messages
- Telco interfacing to the customer's PBX system via T1 or SIP connections
- TAP protocol for use with legacy messaging systems
- Converts open messages to encrypted messages
- Customer administrative interface for configuring address books and listing message history

The Critical Messaging Gateway application, using standard server hardware, and operating under the Ubuntu Linux OS, utilizes all the benefits of Linux, including security and reliability. The application is designed with modularity, which allows easy expansion and redundant configurations and was designed using multi-threaded asynchronous processes, which allows for the most efficient use of hardware and software resources.

All system hardware is comparable with US data center power systems, operating between 100 to 240 VAC, and are 19" rack mountable. Webpage access is compatible with most browsers.

It is also highly recommended that the system be physically located within a data center and configured for redundancy as well as using a UPS and a backup power generator (if available) for the power source.