Total Control STGe

Enhanced Integrated Dial, IP Access Transaction Platform for Small, Medium & Large Transaction Volumes

OVERVIEW

NewNet's Total Control Secure Transaction Gateway version 5.0e (STGe) enhanced, integrated Dial and IP Secure Transaction system is the path breaking, newer generation, market leading solution for carrier class transaction network solution for acquirers, processors, carriers, financial institutions, payment service providers, network service providers etc. This specialized software suite can enable fast transaction transport of credit card authorizations, debit card fund transfers, health benefit authorizations, electronic benefits transfers, and other communications involving single-session transfer of small and large amounts of data. The Total Control STG system is a high density and high session capacity secure transaction transport system designed to run on industry standard, highly reliable, high performance 2U rack mount hardware.

Globally, electronic transactions have increased in volume and dollar value over the previous years and continue to grow. Worldwide ecommerce spending is estimated to exceed $1Trillion in a few years and over 12.5% of all ecommerce transactions will be conducted over smartphones soon. Close to 1Billion handsets with contactless capability including NFC etc. is expected to be in use in the next few years and it is estimated that significant proportion of all POS terminals will have contactless capability in the same timeframe. All these estimates point toward a huge increase in mobile, broadband IP transactions, which is expected to cross over 45 Billion transactions and be, valued over $10 Trillion in the next few years. Meanwhile the dial based transactions are still continuing to be the highest transaction volume drivers today globally and holding significant potential to maintain that for a long time. This increased volume growth for IP and Dial transactions can be efficiently handled with the future ready Total Control STG system version 5.0e which leverages the functional capabilities of legacy systems together with the advanced processing prowess of the newer generation system architectures, operating systems and microprocessors.

The Total Control STG 5.0e is designed to handle electronic payment transaction transport of highly sensitive transaction data associated with payments and ability for future expansion to cater to the market growths. These systems comprises of two Intel Sandy Bridge processors onboard that support emerging technologies and applications with advanced high speed modem processing, DSP capabilities and advanced crypto processing for security. This secure transaction aggregation and intelligent routing & switching solution offers capability to support payment transactions from dial, broadband/mobile IP, internet/mobile internet browser based POS terminals/POI devices, which need to be completed rapidly and economically with highest security.

Modern day payment system network architecture is driving payment processing and the industry to have a convergence of mobile and broadband IP-centric products and services, together with the legacy dial based services. Increasingly, more financial institutions, insurance companies and businesses around the world are using the mobile and broadband internet to offer products and services and enhance an expanded suite of communications based services to its consumer's customer base. Internet based transactions have many obvious advantages over traditional telephone line based transactions. These include the potential to reduce the transaction costs, improve transaction time, and an increase in the payload size is regarded as a major driving force for financial institutions to switch over to the internet. Security becomes a major concern with modern day payments and Total Control STG systems addresses this by intelligently constructing newer solutions on top of the advancements that NewNet payment transaction transport systems have built over the years.

For Dial Traffic handling Total Control STG provides high density modem span capability with E1/T1 support with expandable options in 2U form factor and can be stacked for handling thousands of transactions.

Total Control STG 5.0e solution is designed to transport millions of mobile, broadband IP based POS transactions, m-commerce and e-commerce payments transactions, internet payment transaction, mobile wallet payments etc, while delivering the fundamental security capabilities needed to enable safe and reliable transport of financial transactions, security verification, and also for any data which requires high levels of data encryption over many network types.

STG in The Network

The Total Control STG 5.0e system connects transaction Dial and IP based POS terminals to a host authorization system using TCP/IP protocol or with legacy protocols like X.25, SNA with optional modules. As seen in the below figure, the Total Control STG 4.0i acts as an intermediary, aggregating POS traffic securely and routing these transactions to the Host servers and thus performing the vital network access, transport and routing role.
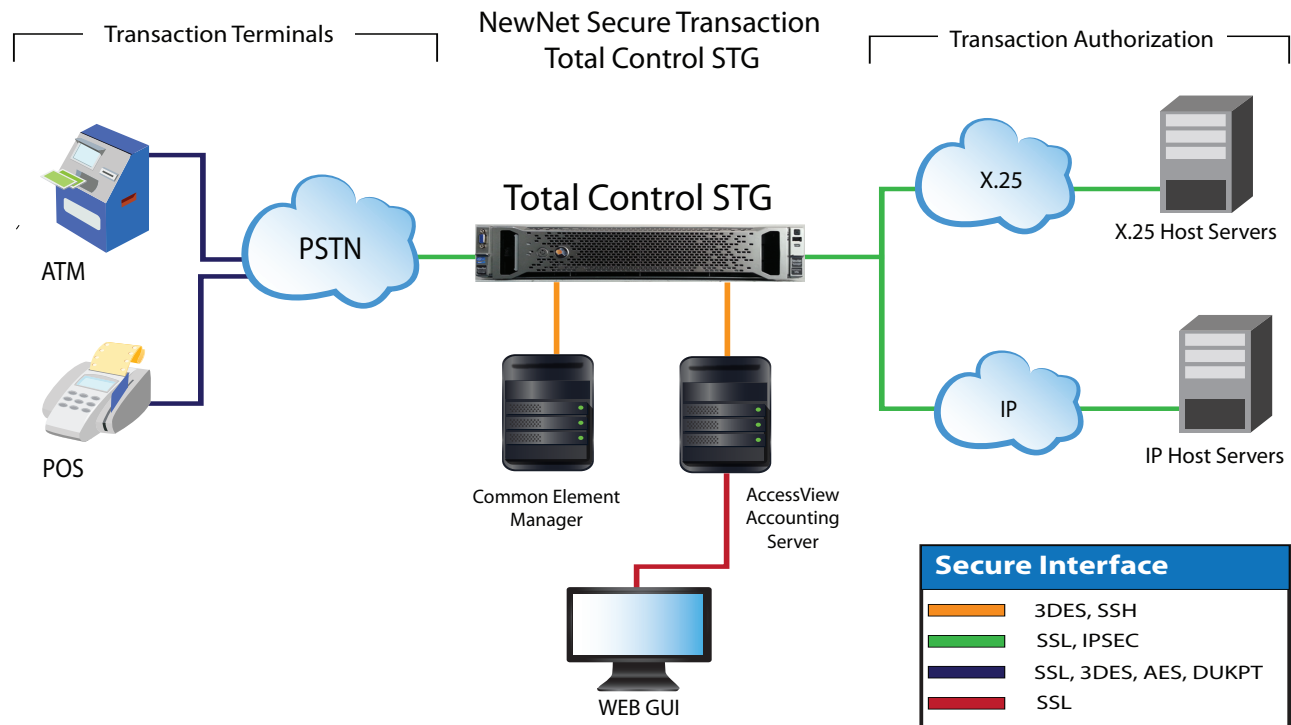

Figure 1: Total Control STG 5.0e Aggregates Transactions From POS Terminals & Routes to Transaction Authorization Servers

Supported Protocols

Total Control STG 5.0e uses DNIS number, IP Address, transaction data fields like TPDU NII to route debit, credit, POS, healthcare, and EBT transactions to the host server over IP networks. This system support multiple protocols with a variety of capabilities to perform several types of intelligent transaction routing with routing decisions made on the fly based on data received from terminals including tokens in place of card data. The system offers security while connecting to POS and Host Servers with SSL/TLS and IPsec; handles secure TCP/IP and HTTPS transaction transport; performs advanced IP routing for network traffic using network routing protocols of RIP, OSPF; supports transaction protocols like VISA I, VISA II, ISO 8583, TPDU (Transport Protocol Data Unit), and several custom protocols.

Network Management Agent

Total Control STG 5.0e Network Management Agent provides complete SNMP-based remote management capabilities including the following:

• Robust system HW/SW event and alarm reporting
• Configuration management
• Software downloads without service interruption
• System parameter storage
• Rapid response to pre-configured system events

System Statistics

Total Control STG 5.0e system interworks with the element management system from NewNet - CEM (Common Element Manager) for providing the system statistics, configuration, network management information in a centralized manner. This offers flexible client-server architecture and easy-to-use graphical interfaces that allow network operators to view system status at a glance. In addition, the CEM solution provides a common look and feel across all NewNet systems service environments as well as open XML interface and scripting application interfaces, enabling network operators to rapidly develop and deploy new customized applications.

Wide range of system statistics is available from STG system on CEM including transaction statistics, network protocols statistics, security protocol statistics, transaction protocol statistics, modem and IP connection statistics, ingress/downlink and egress/uplink statistics etc. STG also generates traps and syslog for events and allow the operators to effectively address these events and take actions in a timely manner.

High Processing in Small Form Factor

The STG supports E1/ T1 spans for Dial POS traffic routing together with IP POS traffic routing with SSL, HTTPS (with future options to increased capacities) in a 2U rack mount form factor and can linearly expand E1/T1 capacity or IP Sessions capacity with additional servers.

Clustered Architecture

Multiple STG systems can be deployed in a clustered architecture with load distributed across these systems along with high availability and redundancy. All the deployed systems can be managed from one location by a single web based management GUI. This provides for easy scalability – scaling up is simply a matter of adding new systems.

Multiple Transaction Types

Total Control STG 5.0e system is designed to ensure no single point of failure for maximum uptime and higher availability. This modular platform is based on redundant modem and transaction routing applications on stackable rack servers. The system combines digital signaling processor (DSP) technology, secure transaction processing (switching and routing), SSL over TCP/IP processing, HTTPS transaction routing and management software to provide fast, reliable connectivity using today's most advanced communication technologies.

Broader Markets

Internet and similar public network security is fundamental and necessary to the successful adoption of the new economy and markets such as Internet Banking, internet commerce, mobile banking, mobile commerce, mobile wallet payments, e- governance, and medical records transfer etc. NewNet"s security solutions can be used in the following markets to provide secure financial transactions, data collection and custom applications over the public networks and internet.

Financial: Electronic Fund Transfer, Electronic Data Interchange, Electronic Benefits Transfers, Electronic Trade Confirmations

Insurance: Data Collection

Health: Medical Records Transactions

Airline: Reservations

Security: Pin Encryption and Verification for Transactions, ID Verification, Security Verification

General: Data Collection, Custom Applications

Figure 2: Total Control STG 5.0e System

DIAL POS HANDLING

Traditionally, POS based transactions are initiated by POS devices dialing into the PSTN, which then transfer data via standard V (modem modulation standards V.32, V.90, V.x), series modulations using VISA I, VISA II and similar protocols. While the industry makes efforts to move to all IP architecture and POS devices convert to mobile or broadband IP only devices, the legacy Dial devices are still continuing to form a major part of the transaction initiating devices. The volume of transaction is increasing, the Dial POS continues to remain active, and the transaction volume on the Dial POS devices is even growing in several geographies as the card usage in increasing in several fast growing economies. Even with GPRS/3G POS devices, Dial remains as a backup option so as to fall back in the event of the traditional mobile data network being unavailable.

Multi Span E1/T1 Card

The advanced design of the E1/T1 multi span card enables multiple modem sessions ISDN processing on a single DSP, delivering high-level functionality in a small space. The card set can process multiple E1/T1 within each PCI-e slot.

The Total Control STG E1/T1 modem card features a fully reprogrammable DSP engine that can allow administrators to reconfigure the system to implement new technologies and applications. The multi span card supports a full range of trunk and communications standards, including V. everything, V.92, V.44 error correction, and many variations of PRI.

Switching & Routing Engine

The Total Control STG's modem card processes the packet contents of all digital and analog connections and routes E1/T1 transaction calls to the hosts. The rack server that hosts the application provides Gigabit Ethernet interfaces. Total Control STG system implements various transaction protocols like VISA I and VISA II. As an example, for asynchronous VISA transaction processing, this system supports the VISA configuration modes like Full Emulation, Full Emulation/No Acknowledgment, ENQs Only, ENQs Only No Framing, and Transparent. This routing engine offers NII based routing of transaction data for TPDU protocol based transactions.

Faster Transaction Routing

Generally, in industry standard transaction routing systems if two modems are using different baud rates, the faster modem will step down to the lower rate. Total Control STG supports fast-train protocol to retrofit lower rate modems and allow for them to communicate with higher baud rate modems at enhanced speeds. Fast train protocol significantly reduces the training times of 1200-bps and 2400-bps modems. Originating 2400- bps modems must support the proprietary fast-train protocol to receive 2400-bps fast-train benefits.

IP POS HANDLING

When evaluating systems for transaction transport, Financial Institutions will look for which technology or solutions best suit for their needs. When replacing the legacy systems with new technology, payment service providers must evaluate interconnecting and integrating their existing system with new services. There is a significant business risk and costs associated with discarding the legacy system and replacing it with brand new systems.

For example, in financial transactions where legacy hosts work on X.25 network moving the transactions to over the internet requires the host server to support all the security requirements of a generation IP infrastructure. Since the mobile, broadband internet is a public network and the basic IP protocol lack the most basic mechanisms for security, such as authentication, message integrity, and data confidentiality, the network infrastructure that these payment service providers choose must have uncompromised performance, be highly secure and safeguard the information it collects in order to avoid a security breach and costly surprises.

The solutions from NewNet deliver fundamental security capabilities to enable safe and effective means of conducting financial transactions, data collection, security verification and custom applications over the internet any day, any time.

Mobile and Broadband Internet Based Transactions

As mobile data access becoming increasingly prolific world over, newer POS/POI devices are increasingly geared towards the usage of 3G/4G mobile data technologies for wireless network access. Also the usage of Internet both over broadband and mobile for business and financial transactions are also on the rise. This increased usage with the lack of built-in security has become more and more problematic. Additionally, global mobile subscriber base is expected to touch 6 billion in the near future. Mobile phones have advanced far ahead from being a basic voice communication device to a multi-purpose device with an appealing form factor which enables internet access, streaming videos, multimedia messaging, discount coupons, airline check-ins, mobile banking, mobile payments and even as a true mobile wallet. The volume of transactions, once these mobile devices could be enabled to make mobile payment transactions is estimated to be huge in the years to come. Contactless payments with NFC technology together with Host Card Emulation (HCE) modes on user devices is expected to fast drive the emergence of mobile POS terminals with the ability to enable mobile wallet payments with increased potential to avoid card swipe based transactions in the longer term and save the consumer from carrying multiple payment cards in the wallet. For these transactions, security becomes an even bigger concern to ensure that all electronic information related to payment cards is safe and transported securely.

Any security product portfolio for financial services over the internet should address the following fundamental security issues:

- Authentication (Person's identity is ensured)
- Authorization (Person is allowed to have access to data)
- End-to-end Encryption (data confidentiality)
- Digital Signatures

In addition to the fundamental security services, in depth knowledge of each transaction application may be critical in order to provide a cost effective solution. For an example, in Point of Sales (POS) networking, it is common for some of these systems to require specific standards and protocols implementation and customization. Due to this, a generic product that provides only Internet security may not be suitable for secure routing and transport for all financial transactions. Here is the true value of the NewNet Total Control STG solution with ability to handle mobile and internet broadband based transactions with the highest level of security compliant to PCI standards and supporting a wide range of transaction protocols.

Security For IP Payment Transactions

Transport Layer Security (TLS)/Secure Sockets Layer (SSL)
TLS/SSL is a cryptographic protocol which provides secure communications over the Internet. The protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. Total Control STG system employs the powerful mechanisms of security by utilizing the SSL/TLS protocols. SSL involves a number of basic phases:

- Peer negotiation for algorithm support
- Public key encryption-based key exchange and certificate-based authentication
- Symmetric cipher-based traffic encryption

Encryption Algorithms
The most widely used encryption algorithms for SSL are AES, 3DES and RC4.

Advanced Encryption Standard (AES): Advanced specification for the encryption that supports 192, or 256 bits.

Triple DES (3DES) : Version of DES that encrypts a message three times using the DES 56-bit key, which is effectively 168-bit key encryption.

DES: Block cipher algorithm developed by the National Institute of Standards and Technology (NIST) Data Encryption.

RC4 : Stream cipher developed by RSA Data Security, Inc. The key-length is variable but typically used is 128-bit.

Key Exchange Algorithm

Symmetric key cipher requires a key to be used to encrypt the communications. When two parties have no prior knowledge of each other, they must jointly establish a shared secret key for encryption over an insecure communications channel.

The most widely used algorithms for exchanging or generating shared key at both ends of the communications link are RSA and Diffie-Hellman. Diffie-Hellman is a key agreement protocol, where the algorithm generates a shared secret at both ends of the communications link. RSA is a public-key cipher, which works as a key transport protocol, by which the algorithm sends out a secret key to the other end of the communications link.

Digital Certificate

Key agreement or key transport schemes are vulnerable to man-in-the-middle attacks. A solution to this problem is to send the public key over the communication link using a signed certificate. Certificate contains, along with the public key of the sender, the name of the certificate holder as well as the digital signature of an independent and trusted third party, called certification authority (CA), to ensure the validity of the transmitted information.

The certificate format is usually based on ITU-T recommendation X.509. During TLS/SSL negotiation, certificates are exchanged for public key information. These certificates are validated during SSL handshake phase.

Mobile/Broadband Payment Routing

With increased industry movement to all IP architecture and as POS devices convert to mobile or broadband IP only devices, the need to aggregate and securely transport the transaction information from these IP POS devices to a central server is on the rise. The NewNet Total Control STG is designed to meet this specific market, as it will provide a secure means of connecting mobile or broadband IP POS devices, mobile data devices like Tablets and smart phones with card readers etc and securely transporting the information to hosts over the insecure internet.

In this next generation network, a merchant has one or more mobile, broadband IP enabled POS devices sharing a high-speed public internet link (Wireless, Cable, or DSL modem). Total Control STG supports transaction protocols like VISA I, VISA II, ISO 8583, TPDU (Transport Protocol Data Unit), and Custom Protocols, which expedites the financial transactions. Total Control STG terminates SSL sessions that are originated from the IP supported POS. In this model, the acquiring bank host system continues to operate in the same model as it was operating with the legacy transaction mode with STG system performing a crucial role on interconnecting modern day protocols on the POS/POI devices with legacy Host servers.

Mobile Internet Payment Routing

Total Control STG offers a wide variety of service options for enabling multiple types of mobile payments, mCommerce and mobile wallet services. The supported mobile payment interfaces on Total Control STG includes:

• Mobile Browser Based Payments (HTTPS)
• Mobile Application Based Transactions (TLS/SSL over TCP/IP or HTTPS)

Total Control STG inters woks with these payment methods by interfaces to mobile data networking systems and HTTPS interface to the mobile payment devices for the mobile browser or mobile application based transactions. These payment transactions from mobile devices are processed on the Total Control STG and sent to the banking or financial institution servers for the payment approvals and authorizations.

Total Control STG seamlessly enables the payment transactions for the two broad mobile payment service categories which are the retail merchant location based mobile POS based payment transaction and subscribers' mobile device initiated mobile wallet based payments.

FEATURES, FUNCTIONS AND APPLICATIONS

Dialed Number Identification Service (DNIS) Based Dial Transaction Routing

The Total Control STG maps Dialed Number Identification Service (DNIS) digits from the PSTN into specific Host Servers for IP connectivity; maps DNIS digits to specific TCP host and port numbers. This allows transaction-processing centers to use the rich addressing capabilities of both the PSTN and the IP networks together. For example, a center may choose to
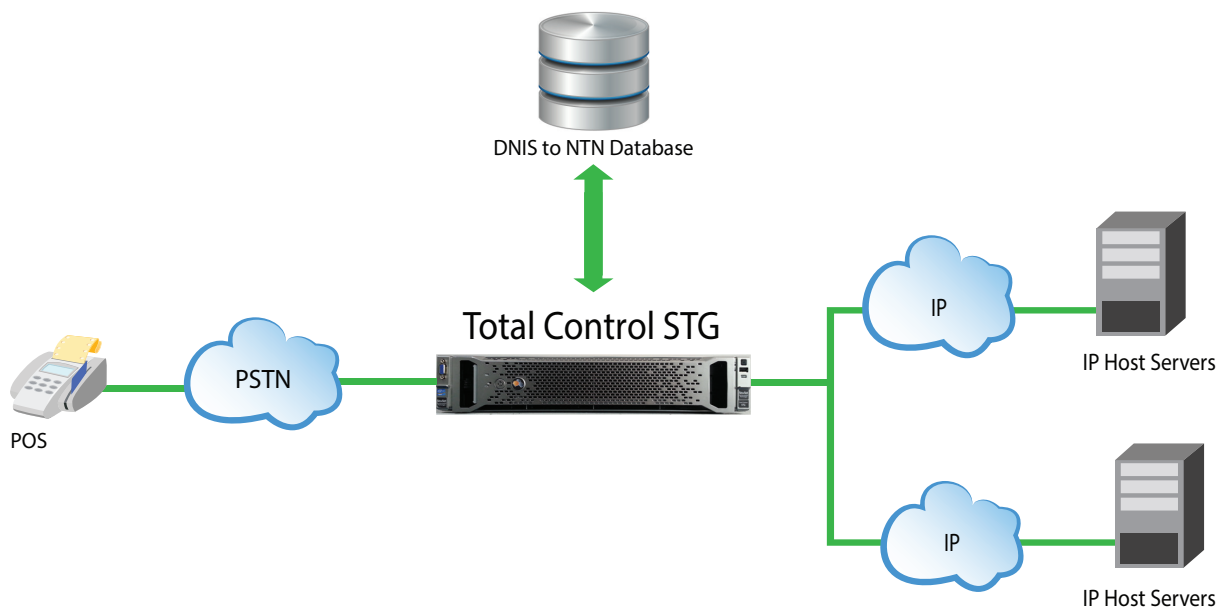
Figure 3: Dialed Number Identification Service (DNIS) with Total Control STG

As shown in above figure, if the transaction terminal dials a unique number identifying the credit provider, a Total Control system using the Total Control STG can map this telephone number (using DNIS Group) to a particular TCP host and port number.

With the Total Control STG configuration mechanism users may define a DNIS configuration which specifies each PSTN DNIS-to-TCP host/port number. The Total Control STG currently supports 100s of DNIS entries, which can be "mixed" so that some dialed numbers invoke specific TCP host for ISO8583 or TPDU or VISA transactions.

Multi-Mode Rules Based Routing for IP Payment Transaction Transport

Total Control STG, PCI DSS compliant Secure IP Transaction switching and routing system enables carriers, acquirers, processors and service providers the opportunity to route electronic payment transactions originating from any POS or transaction initiating device to an any authorization server based on, but not limited to the following criteria:

1. Least Cost Network Route
2. Network availability
3. Shortest path
4. Server availability
5. Server Traffic
6. Pending transactions

Apart from a network specific destination, the STG system offers the option to route transactions in real time, to specific acquiring banks, processing host servers or other financial institutions based on the transaction fees charged by the various entities. Depending on the fee charged by the acquiring institution, the STG will route the transaction to the lowest fee charging authorization server for a particular type of transaction. This includes varying fees for transactions like credit, debit, prepaid, mPayments, and peer to peer payments.

The Total Control STG will intelligently select the lowest fee charging destination based on the type of the transaction and specific card association, issuing bank or institution. These selections may be updated securely and dynamically via HTTPS, based on changes in the rates offered by these institutions, and the system will dynamically route the transactions real-time to the new destinations.

In addition to the direct selection of the lowest fee based destination servers, other possible secure routing may be applied in combination, with specific rules like:

1. Preferred server for specific type of transactions
2. Selected server for transaction values above certain ranges
3. Specific server for transactions from select locations
4. Designated server for low value transactions
5. Higher fee server for high risk, low security area transactions

In today's dynamic, volatile and fiercely competitive settlement of payment card and third party network transactions markets, secure and timely flexibility of routing and processing options insure minimizing fees and maximizing network processing efficiencies.

Managing Large Networks

The ability to configure all elements in the network from the same portal makes managing large networks a breeze. Once the desired configuration has been created for one Total Control STG system, it can be cloned onto every other Total Control STG in the network with a couple of clicks.

Most of the system parameters can be configured using the Common Element Manager or a modem template may be used to configure only those parameters that cannot be configured through the Common Element Manager. New Total Control STG configurations can be downloaded at any time after the Total Control STG has come online. Downloading a new configuration does not affect ongoing calls unless the X.25 frame or packet level parameters are changed.

Generic Functionalities

- VISA I/II transaction protocols and processing
- Synchronous Transaction Protocol (ISO8583/SDLC) and processing batched transaction processing
- Per-call configuration of modem parameters based on incoming DNIS
- Incoming calls at data rates from 300 baud to 56K
- TPDU Routing
- Secure Shell (SSH)
- ISDN T1, E1
- Auto detection of asynchronous versus synchronous transactions
- Faster modem training times using the proprietary "Fast Connect" negotiation
- Routing transactions over either an IP network or optional X.25/SNA networks
- Per-call configuration of transaction parameters based on ingress IP and port
- Performance monitoring of transaction statistics allowing early detection of possible T1 trunk problems
- Combination of transaction calls and dial/IP configuration selection on a per-call basis
- EIS standards 1051 and 1052
- Offline configurator CEM integration DNIS
- Transaction related SNMP traps
- Automatic shutdown due to high temperature
- Transaction related SNMP traps
- AC power

UNIQUE BENEFITS

Reduced Traffic

The transaction system can act as an intermediary, appearing to Point of Sale (POS) terminals as a host, but communicating to the host using far fewer packets required than if the POS terminal(s) connected directly to the host. This reduces TCP/IP network congestion and time spent by the host in handling responses, allowing the host to handle more calls per day. It also provides a means of connecting a wide variety of POS terminals to the same host by providing configurable protocol options on a per call basis.

Accounting and Network Management Support

The AccessView Accounting Server, which is an integral part of NewNet's Secure Transaction suite of products, captures accounting and network statistics from the Total Control STG System. The data captured by the accounting server supports subscriber billing, transaction recording, report generation, network performance monitoring, and system modeling and measurements. The Common Element Manager System provides flexible, centralized management for the secure transaction family of products. This powerful solution enables performance, fault, and configuration management of single and multiple STG chassis and their components in all NewNet based service environments.

Integrated Solution

The Total Control STG solution supports transaction transport, security off-loading and network routing in a single box. It can be used with the currently deployed point-of-sale (POS) terminals and legacy host servers.

Highly Versatile System

Single system for handling multitude of transaction types with the capability integrated into one system. Supported types include handling of different types of transactions like internet payment transactions, , Dial & IP POS transactions, NFC/contactless mobile wallet payments including HCE mode, mobile POS transactions etc.

Scalability and Reliability

System is designed to scale from supporting hundreds of dial, mobile, broadband IP payment terminal to supporting tens of thousands of terminals in a seamless fashion. The Total Control STG solution design also provides special attention to eliminate the single point of failure inherent in the IP environment.

Facilitates P2PE (Point to Point Encryption)

STG system interfaces with NewNet's AccessCert Security Server for Point to Point Encryption (P2PE) solution which is a FIPS certified HSM based solution that has the base key of all keys used with POS devices. STG systems would cryptographically generate the same key that terminal used for the encryption, working in conjunction with the Security Server. When the POS sends the encrypted payload it also sends meta data including terminal identifier and transaction counter which the STG systems passes to the AccessCert server and seeks the information to obtain the keys used for encryption by the POS. Based on information shared securely from the AccessCert, the STG systems can formulate the keys to decrypt the transactions. STG systems can also provide the encryption of responses in the reverse direction and can devise encryption options for entire payload or select fields in both directions - from and to the POS.

Low Cost Ownership

STG is built for delivering high call density in 2U of rack space which limits the space and power consumption together with limited system hardware thus lowering the cost of maintenance as well.

Leverages Years of Experience in Transporting Financial Transactions

The NewNet's Secure Payment Transaction Solutions have customer presence across the globe, with service and support responsibilities for over numerous customers across 50+ countries. NewNet's secure payment routing and transport solutions handles multi-billion transactions annually with major deployments at global acquirers, processors, carriers and banks. NewNet secure payment systems routes about 20% of the global annual transaction volume, with 1 in 4 transactions in North America, 1 in 3 transactions in South America and 1 in 4 transactions in the Asia-Pacific regions.

REDUNDANCY AND LOAD SHARING

E1/T1 Modem Redundancy and Load Sharing

The platform can be configured for redundancy or load sharing between the E1/T1 modem ports and PSTN. In the event of a specific modem span failure the platform can switch to the redundant pair. If preferred, additional modem spans may be used for load sharing.

System Fail-Over Redundancy and Load Sharing Mechanism

The redundant system offer the ability to have load sharing mechanisms and failover for redundancy in the event of failure of one of the systems. This model avoids a single point failure and ensures a fully redundant solution as would be required for a high available solution for transaction transport systems that may be transporting millions of transactions. The rack servers operate in a VRRP load shared and active- active mode for enabling load sharing and redundancy.

IP Redundancy

The TCP/IP configuration provides for multiple hosts. If the primary host does not respond within the specified configured time frame, information is sent to host with next lowest priority.

Equipped with multiple Ethernet ports, STG offers IP network connectivity busy out feature. In this mode, the application continuously pings the target host. If no response is received for a period of time, the host is marked as down and the POS interfaces (both Dial or IP) are busied out for Dial transactions and TCP listeners shut down for IP transactions.

Redundant AC/DC Power Supply

Redundant AC/DC power supply guarantee maximum system uptime with hot swap option to replace the part anytime with no service impact.

KEY FEATURES AND BENEFITS

Feature	Description	Benefits
Transaction Protocol Support	Designed to accommodate all POS industry standards and supports all major transaction protocols - VISA I/ II, TPDU, ISO 8583.	Maximizes interoperability between hosts and POS terminals through ubiquitous support of transaction protocols. Allows Total Control STG to provide intelligent routing of transactions with a variety of payment transaction services.
Transaction Routing	Transactions routed based on fields in packet headers and payload fields. Multiplex several transactions to host server on a single connection, maintained as persistent session.	Advanced routing ensures transactions are sent to correct destinations. Multiplexing balances transactions to avoid congestion, bottlenecks and diverts transactions
Secure Access	Supports SSL, IPsec, SSH and SCP cryptographic protocols to provide secure Internet access, transfers and communications	Cryptographic protocols ensure that access to the system is completely secure.
Network Routing	Supports a suite of routing protocols - RIP, OSPF and BGP-4.	Helps network administrators configure IP routing to maximize system availability.
Load Balancing	Load balancing criteria include default mechanisms of round robin, pre-defined preference values, outstanding traffic or active load, ability to process transactions swiftly or response to delays. Can be applied on multiple Host servers configured in a Host group, or destinations defined for specific packet traffic.	Load balancing can be combined with routing protocols to ensure the traffic is distributed across the available paths. Intelligent routing increases system efficiency.
Group Monitoring	Systems has the ability to track and display the status of all Host servers in a group tracking status "active" or "non responsive".	Used by the operators or NOC teams to restore services of servers out of action. Real time monitoring allows NOC teams to react to status changes in a timely manner, administrating alerts before they turn into problems.

KEY FEATURES AND BENEFITS

Feature	Description	Benefits
Virtualization	State of the art virtualization capabilities that allow for segregation of traffic into groups and allocation of resources based on virtual traffic groups. Groups are defined on traffic type (TPDU, ISO8583), IP address/port, remote IP ranges and VLANs etc. Intelligent resource allocation within virtualized groups ensures that a group does not starve other groups of system resources.	This enables acquirers, processors and carriers to offer differentiated services on the same systems to multiple customers and still maintain complete isolation of capabilities and access controls.
PCI Compliance	- Build and Maintain a Secure Network - Protect Cardholder Data - Protect stored cardholder data - Encrypt transmission of data across public networks - Maintain a Vulnerability Management Program - Implement Strong Access Control Measures - Restrict access to cardholder data by business - Assign unique ID to each person with computer access - Restrict physical access to cardholder data - Regularly Monitor and Test Networks - Track and monitor network resources & cardholder data - Regularly test security systems and processes - Maintain an Information Security Policy	Total Control STG insists on password protection for all users accessing systems including password control for system consoles and remote sessions. The system does not store any card data and all key information stored is encrypted. All data transmissions to and from the system are encrypted. System access is restricted with access control lists and various levels of access. All system access and configuration changes are logged and made available for audit trail. Fail-safe model, leaves no options for user to create non-compliant configurations, mitigating security risks to offer fully compliant systems.
Certificate Status	Verification on client and server certificates and provides information regarding the validity of Certificates	The certificate information can be listed and viewed and appropriate traps are generated when the validity expires or a configured
System Utilization	Detailed system resources utilization info including the processing resources, memory, interface status, traffic volume are available for tracking and monitoring	System management teams can proactively utilize this information for improving service.
Keep Alive Mechanism	Customized mechanisms for maintaining keep alive mechanisms between configured targets for status determination.	This feature is vital in ensuring the actual status to destination systems and making intelligent decisions on traffic re-routing.
Packet Filtering	Rules based packet filtering capability to filter traffic from avoidable sources or known/learned untrusted sources. Packet inspections for known patterns or signatures for early action to drop these before further forwarding.	Protects systems from known internet vulnerabilities and increase additional security layer over and above external firewalls.
Authentication	Radius, TACACS, LDAP based authentication.	Allows the use of a variety of external authentication servers.
DUKPT Encryption	Enables the terminal devices to offer advanced security capability for card data over and above the session security provided by the standard security protocols.	Enhanced security for card data which will still be secure over and above the session security.
DNS Resolution	Capability to rotate traffic incoming to STG groups among multiple STG systems by providing resolved IP addresses to DNS queries from transaction terminals. Based on run time identification in terms of traffic volume, processing delays, overall speed of transactions handled	Designated STG system can act as internal DNS server to intelligently distribute traffic across multiple AG.
Secure Shell	Authorized clients can connect to the internet via Ethernet interfaces on the Total Control STG system. This access is authenticated and secured via Secure Shell-2 procedures.	All user access to the systems remains over secure access mechanism only.
Configuration	Offers the ability to configure the system from the Common Element Manager tool (CEM) using graphical user interface or by CLI access to the system.	Full fledged capability to configure the systems in a carrier grade manner.

TRANSACTION STATISTICS & REPORTING

Access View is an integral part of the transaction-processing system. Access View captures accounting and network statistics from the Total Control STG, then processes and stores them in its database. Data captured by the accounting server can be used for the following operations:

- Transaction Accounting
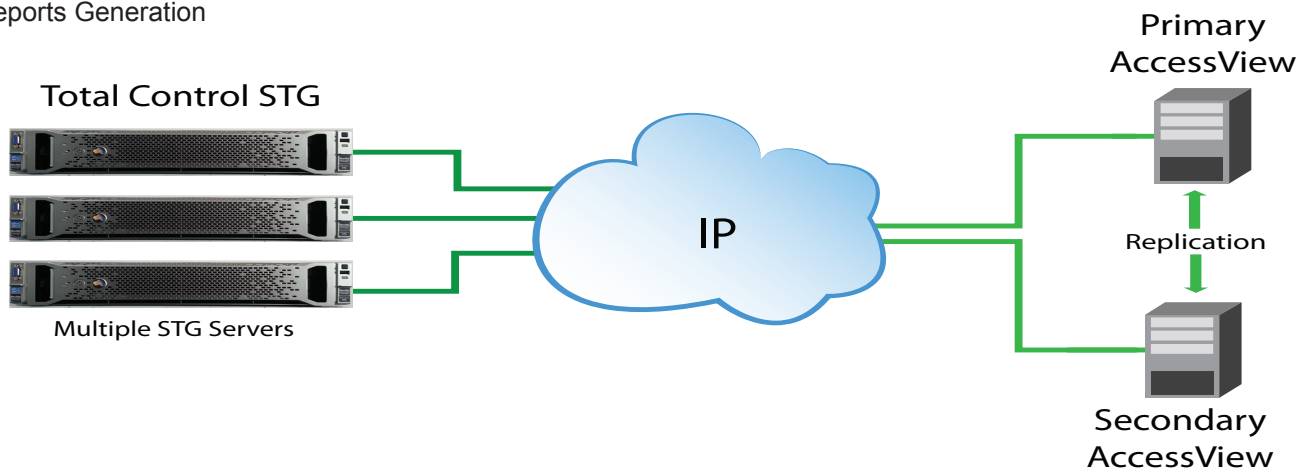- Transaction Monitoring
- Customer Billing
- Reports Generation

Figure 4: Multiple STG servers report to a redundant pair of Access View servers with live replication.

Real-Time Viewing of Data & Reports

Real-time data are recorded to Access View at the end of each call. Customers can monitor and build a custom summary table using the most recent data in real-time. On a system-wide basis, transaction statistics can be used for traffic analysis according to time of day, system components, offered load, and transaction routes.

Access View provides the convenience to generate various reports for planning and monitoring purposes.
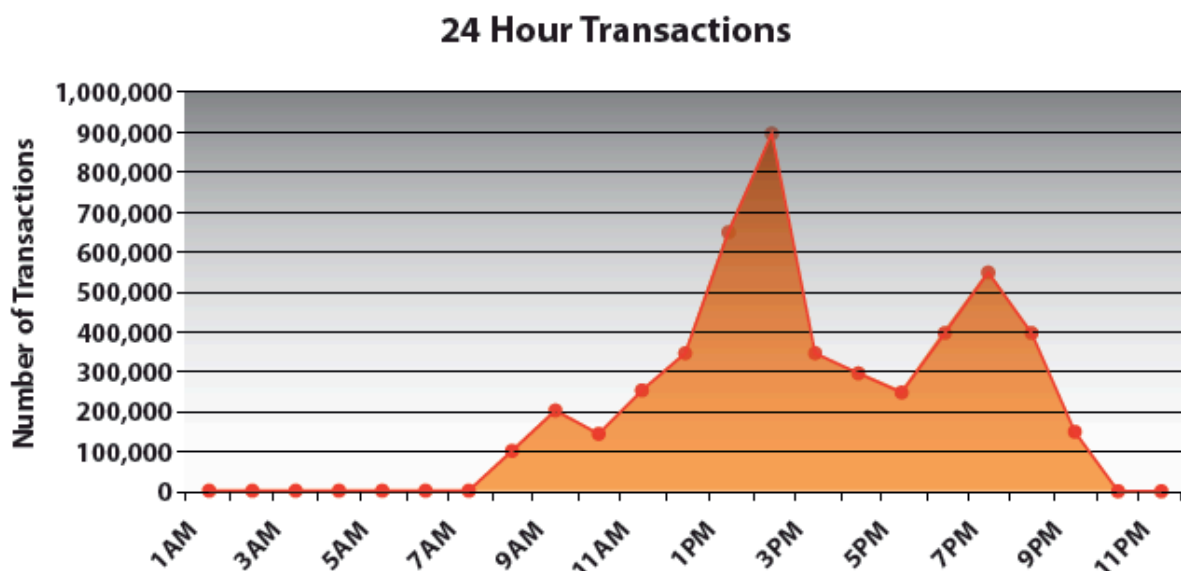

Figure 5: A graphical report from Access View, showing the number of transactions over a 24 hour

Summary

The Total Control STG version 5.0e (STGe) enables fast dial and IP transaction transport of credit card authorizations, debit card fund transfers, health benefit authorizations, electronic benefits transfers, and other communications involving single-session transfer of small amounts of data. Carrier class transaction network service providers can reduce CAPEX and OPEX by deploying Total Control STG for transaction transport over the next generation IP network or over legacy X.25 networks.

The rich features in the Total Control STG system provide new revenue generating opportunities for the network service providers.

Total Control STG Advantages

• Cost reductions of dial transactions

• Security to the insecure dial and IP POS terminals

• Interconnect legacy bank host computer with the next generation IP POS terminals & aggregate the connections for saving host's resources.

• Simplified solution

• CAPEX savings to avoid hosts replacement using the public internet

• Safeguard sensitive credit card data over the public internet

• Offer opportunity to provide more value add services

• Faster transactions using state of the art hardware accelerator options

• Highly scalable for location based growth

• Redundancy for network disasters with record recovery

• Integrated platform for dial broadband internet and mobile payment transaction routing

Contact Us
traxcominfo@newnet.com
www.newnet.com