

Telecommunications is an essential industry in our society. Imagine the world with no telephone, no cell phone, no pager, and no Internet — no way to communicate. Now imagine catastrophic events such as the terrorist attacks on Sept. 11, 2001 — with no communications. Carriers and governments increasingly are being required to address network security issues. They are challenged to develop tools and applications to prevent attacks on one of the most important and crucial infrastructures.

Tekelec provides the tools to detect service-denying attacks before they cripple the network. Sentinel also assists network providers in supporting the PATRIOT Act, a post September 11 legislation to combat terrorism. The Act increases the authority of law enforcement in conducting electronic surveillance and calls on providers to supply data and reports to law enforcement agencies.

### NETWORK ATTACKS

Network attacks take many forms. The best defense is early detection of network events fitting the characteristics of an attack. The Tekelec Sentinel has applications designed to provide early detection.

### Link Status Thresholding

Link status thresholding is a standard security feature within the Tekelec Sentinel. The carrier programs the system to notify network operators of a sudden increase or decrease in network traffic, indicating a possible attack. The user identifies normal link

utilization on specific links and, then, sets a threshold on the link monitor function.

When thresholds are exceeded, the system generates an alarm and displays it via the alarm manager function. The alarm manager provides a display identifying the source and type of alarm, or it can be interfaced with an existing network management system (NMS).

### Mass Event Detection

Also in the Sentinel security tools armory is the mass event detection feature. When larger than normal volumes of traffic are identified in the network, an alarm is generated and reported via the alarm manager. The alarm identifies the source of the message, the target of the message (i.e. affected point code), and the link where the message was discovered. A graphical user interface (GUI) displays each occurrence of the event found in the system in real time. The mass event feature is based on processing information as created by the call detail record (CDR) generator. The feature also includes threshold and timer features, alerting the operator when a specified number of alarms occurs.

### Calling Patterns Analysis

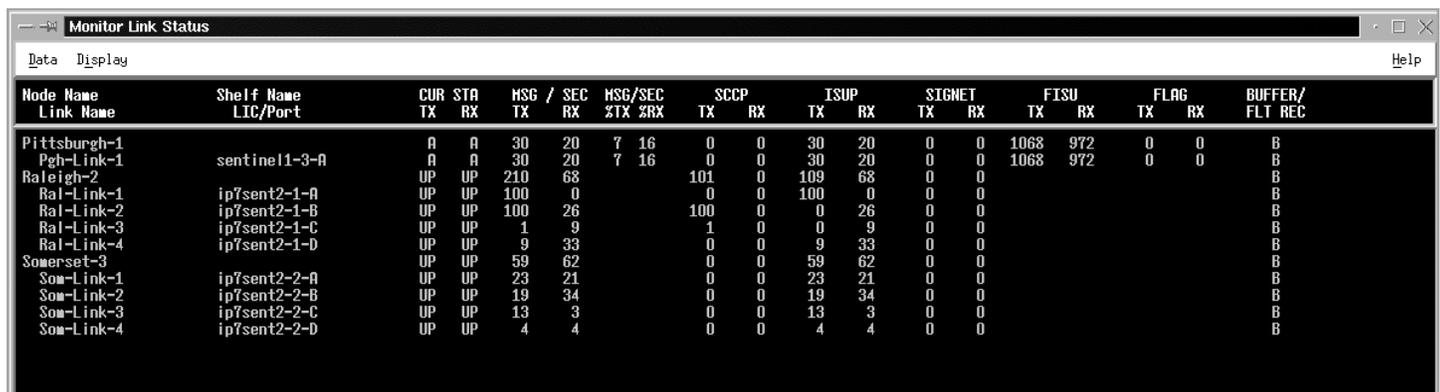
Sentinel also provides options for analyzing data and traffic patterns in the network. Sentinel includes a network-wide traffic monitoring and reporting system that provides link utilization information for definable periods. Information is derived from the 4,000 peg counters in the system

and is accessible from a web browser. The system collects statistical data from multiple nodes simultaneously and combines it to produce various types of reports, such as link-level reports, node-level reports, or network-wide reports. The system is able to generate reports for periods of 15 minutes, 30 minutes, one hour, six hours, and 24 hours. The Sentinel traffic home page allows users to generate traffic reports and configure monitored nodes.

Carriers are challenged with new requests from law enforcement for activity reports on specific subscribers. Sifting through billing records, traffic reports, and other data is a manual and tedious task. Sentinel,

### The Tekelec Sentinel

The Sentinel platform provides carriers with revenue assurance tools to keep them profitable while giving them visibility of and access to their signaling system 7 (SS7), Internet protocol (IP), and converged networks. Business applications such as fraud detection, billing, billing verification and analysis, quality of service, looping detection, and mass call detection interface with the Sentinel platform to process network data. Most importantly, in this time of heightened national security, Sentinel includes network monitoring, surveillance, and intrusive capabilities to ensure the safety of carrier networks.



Node Name Link Name	Shelf Name LIC/Port	CUR TX	STA RX	HSG / SEC TX RX	HSG/SEC %TX %RX	SCCP TX RX	ISUP TX RX	SIGNET TX RX	FISU TX RX	FLAG TX RX	BUFFER/ FLT REC							
Pittsburgh-1		A	A	30	20	7	16	0	0	30	20	0	0	1068	972	0	0	B
Pgh-Link-1	sentinel1-3-A	A	A	30	20	7	16	0	0	30	20	0	0	1068	972	0	0	B
Raleigh-2		UP	UP	210	68			101	0	109	68	0	0					B
Ral-Link-1	ip7sent2-1-A	UP	UP	100	0			0	0	100	0	0	0					B
Ral-Link-2	ip7sent2-1-B	UP	UP	100	26			100	0	0	26	0	0					B
Ral-Link-3	ip7sent2-1-C	UP	UP	1	9			1	0	0	9	0	0					B
Ral-Link-4	ip7sent2-1-D	UP	UP	9	33			0	0	9	33	0	0					B
Somerset-3		UP	UP	59	62			0	0	59	62	0	0					B
Som-Link-1	ip7sent2-2-A	UP	UP	23	21			0	0	23	21	0	0					B
Som-Link-2	ip7sent2-2-B	UP	UP	19	34			0	0	19	34	0	0					B
Som-Link-3	ip7sent2-2-C	UP	UP	13	3			0	0	13	3	0	0					B
Som-Link-4	ip7sent2-2-D	UP	UP	4	4			0	0	4	4	0	0					B

The Monitor Link Status Screen Displays Link Status Thresholding

Event#	Time	Link	SI	OPC	DPC	SLS	DIR	Flavor	MT	CIC	Int'l	Int'wrk	QoR	TRN	Called Number	Calling
00005519	17:20:41.961	PN-Link-1	ISUP	2-2-2	1-1-1	230	->	ANSI-SS7	ACH	1272						
00005535	17:20:42.263	PN-Link-1	ISUP	2-2-2	1-1-1	230	->	ANSI-SS7	ANM	1272						
00005786	17:20:47.271	PN-Link-1	ISUP	1-1-1	2-2-2	236	<-	ANSI-SS7	REL	1272						
00005802	17:20:47.579	PN-Link-1	ISUP	2-2-2	1-1-1	230	->	ANSI-SS7	RLC	1272						
00006003	17:20:51.649	PN-Link-1	ISUP	1-1-1	2-2-2	78	<-	ANSI-SS7	IAM	1372	NO	NO	NO	NO	5193651272	67134233
00006019	17:20:51.961	PN-Link-1	ISUP	2-2-2	1-1-1	71	->	ANSI-SS7	ACH	1372						
00006035	17:20:52.263	PN-Link-1	ISUP	2-2-2	1-1-1	71	->	ANSI-SS7	ANM	1372						
00006286	17:20:57.280	PN-Link-1	ISUP	1-1-1	2-2-2	78	<-	ANSI-SS7	REL	1372						
00006302	17:20:57.589	PN-Link-1	ISUP	2-2-2	1-1-1	71	->	ANSI-SS7	RLC	1372						
00006503	17:21:01.649	PN-Link-1	ISUP	1-1-1	2-2-2	192	<-	ANSI-SS7	IAM	1472	NO	NO	NO	NO	5193651272	67134233
00006519	17:21:01.961	PN-Link-1	ISUP	2-2-2	1-1-1	192	->	ANSI-SS7	ACH	1472						
00006535	17:21:02.263	PN-Link-1	ISUP	2-2-2	1-1-1	192	->	ANSI-SS7	ANM	1472						
00006786	17:21:07.280	PN-Link-1	ISUP	1-1-1	2-2-2	192	<-	ANSI-SS7	REL	1472						
00006802	17:21:07.589	PN-Link-1	ISUP	2-2-2	1-1-1	192	->	ANSI-SS7	RLC	1472						
00007003	17:21:11.649	PN-Link-1	ISUP	1-1-1	2-2-2	34	<-	ANSI-SS7	IAM	1572	NO	NO	NO	NO	5193651272	67134233
00007019	17:21:11.960	PN-Link-1	ISUP	2-2-2	1-1-1	33	->	ANSI-SS7	ACH	1572						
00007035	17:21:12.263	PN-Link-1	ISUP	2-2-2	1-1-1	33	->	ANSI-SS7	ANM	1572						
00007286	17:21:17.270	PN-Link-1	ISUP	1-1-1	2-2-2	34	<-	ANSI-SS7	REL	1572						
00007301	17:21:17.578	PN-Link-1	ISUP	2-2-2	1-1-1	33	->	ANSI-SS7	RLC	1572						
00007503	17:21:21.649	PN-Link-1	ISUP	1-1-1	2-2-2	132	<-	ANSI-SS7	IAM	1672	NO	NO	NO	NO	5193651272	67134233
00007519	17:21:21.961	PN-Link-1	ISUP	2-2-2	1-1-1	130	->	ANSI-SS7	ACH	1672						
00007535	17:21:22.263	PN-Link-1	ISUP	2-2-2	1-1-1	130	->	ANSI-SS7	ANM	1672						
00007786	17:21:27.280	PN-Link-1	ISUP	1-1-1	2-2-2	132	<-	ANSI-SS7	REL	1672						
00007802	17:21:27.588	PN-Link-1	ISUP	2-2-2	1-1-1	130	->	ANSI-SS7	RLC	1672						
00008003	17:21:31.649	PN-Link-1	ISUP	1-1-1	2-2-2	230	<-	ANSI-SS7	IAM	1772	NO	NO	NO	NO	5193651272	67134233
00008019	17:21:31.961	PN-Link-1	ISUP	2-2-2	1-1-1	227	->	ANSI-SS7	ACH	1772						
00008035	17:21:32.263	PN-Link-1	ISUP	2-2-2	1-1-1	227	->	ANSI-SS7	ANM	1772						
00008286	17:21:37.280	PN-Link-1	ISUP	1-1-1	2-2-2	230	<-	ANSI-SS7	REL	1772						
00008302	17:21:37.588	PN-Link-1	ISUP	2-2-2	1-1-1	227	->	ANSI-SS7	RLC	1772						
00008503	17:21:41.649	PN-Link-1	ISUP	1-1-1	2-2-2	72	<-	ANSI-SS7	IAM	1872	NO	NO	NO	NO	5193651272	67134233
00008519	17:21:41.960	PN-Link-1	ISUP	2-2-2	1-1-1	68	->	ANSI-SS7	ACH	1872						
00008535	17:21:42.262	PN-Link-1	ISUP	2-2-2	1-1-1	68	->	ANSI-SS7	ANM	1872						
00008786	17:21:47.271	PN-Link-1	ISUP	1-1-1	2-2-2	72	<-	ANSI-SS7	REL	1872						
00008802	17:21:47.579	PN-Link-1	ISUP	2-2-2	1-1-1	68	->	ANSI-SS7	RLC	1872						

*Continuous Call Trace is a Security Feature of the Tekelec Sentinel*

combined with the calling pattern analysis tool, automates the process. By analyzing CDRs generated by the Sentinel CDR generator, call pattern analysis software provides a comprehensive graphical report on a number of calls with similar characteristics. These tools are used by security departments to track and monitor activities of suspect subscribers, providing law enforcement with the tools they need to track and identify threatening operations.

### Data Mining

The Sentinel CDR generator open feed provides a flexible interface for applications, enabling service providers to leverage, in real time, the data traversing their networks. Through an easy-to-use interface, carriers are able to configure the system to connect to any external application. Tekelec provides the open CDR feed along with professional services to support applications provided by external vendors.

### LAW ENFORCEMENT SUPPORT

Law enforcement and telecommunications carriers are working closely together, identifying threats and sharing information in the current environment of heightened security. With numerous caller-locator capabilities, the telecommunications network is one of the greatest weapons on terrorism for law enforcement. The signaling network is the richest source of data for this defense. There are numerous ways to obtain information about suspect subscribers. Subscriber profiles; call pattern matching; identifying phone scams designed to hide criminals; and call trace are just a few. The Tekelec Sentinel provides the tools essential to carriers in gathering information.

### Subscriber Profiling

One way Sentinel provides assistance to law enforcement is through subscriber profiling. When a suspect is identified, it is helpful to keep track of the calling

patterns. Being able to identify places and people called; the frequency of calls to these numbers; when these calls were placed; the amount of time spent on individual calls; and so forth, is critical information for law enforcement officials. Most carriers have to tediously pour over billing records to manually organize the information into a usable report. With Sentinel, the process is automatic. The Sentinel CDR generator feeds the information into the customizable profiling software.

### Probeless Sentinel

The EAGLE® 5 Integrated Sentinel combines Tekelec's industry-leading, next-generation network signaling platform, EAGLE 5 Signaling Application System (SAS), with Sentinel, to form a powerful, probeless monitoring system. The EAGLE 5 Integrated Sentinel supports auto configuration, eliminating time-consuming administration required to keep equipment in synch, and network wide data collection, which proves a carrier-grade platform that is NEBS compliant.

## Call Pattern Matching

Often times, a suspect may be operating with an alias or may have calling patterns similar to those of a suspect under investigation. Call pattern matching software analyzes call detail records for similar characteristics and visually indicates when there are matches originating from different subscribers.

## Call Forwarding Detection

Recent features such as call waiting, call forwarding, remote call back, and so forth have greatly enhanced the value of telephones. However, the features have complicated matters for law enforcement, particularly in the case of call forwarding. In many situations, suspects are aware that their calls are being traced. Therefore, they set up a scenario in which they call a specific number, which is then forwarded to another number, which might even be forwarded to yet other numbers. There could be many numbers in the chain. Regular call trace features only trace the first leg of the call without showing where the call was terminated. Call forwarding detection is able to show the call and any subsequent legs of the call established through forwarding, identifying the final destination of the call.

## Call Trace

Call trace capability is a key security feature of Sentinel. Call trace isolates numbers in the network. The Sentinel user enters the specific phone number called, and the Sentinel displays all signaling messages associated with the call. By displaying the signaling messages, the calling party can be immediately identified.

The system identifies all numbers traveling to the specified number, regardless of the network from which the call may have originated. Call trace is implemented based on a trace rule that defines how a call or

protocol procedure should be traced.

The trace rule is not hard coded into the Sentinel application itself, but is defined using a configuration file. The process allows for quick modification to adapt to changes in the protocol specification; it is also able to create new rules for different protocols.

With the call trace feature, information is available in either real time, as historical data, or via a continuous trace. Real-time call trace provides information as it is happening and is especially useful in combination with the Sentinel alarm management system. Historical call trace provides a past record of calls made to or from a specific number, retrieving them from stored data. Continuous call trace provides information only about the calls made to or from one specific number for a period of time. Call trace information may be retrieved from both wireline and wireless networks and is available “in reverse,” meaning not only can calls be traced coming from a specific number, they can also be traced going to a specific number.

Worldwide communications often are the target of today’s sophisticated criminals. Law enforcement and carriers are working closely together to deter criminals before disastrous crimes occur, and Sentinel’s security features are playing an instrumental role in this new partnership.

The Tekelec logo is a registered trademark and Sentinel is a trademark of Tekelec. All other products are registered trademarks or trademarks of their respective holders.

This material is for informational purposes only and subject to change without notice.

5200 Paramount Parkway  
Morrisville, North Carolina 27560  
TEL 888.628.5521  
TEL 919.460.5500  
FAX 919.460.0877

26580 West Agoura Road  
Calabasas, California 91302  
TEL 818.880.5656  
FAX 818.880.6993

2425 N. Central Expressway  
Richardson, Texas 75080  
TEL 972.301.1300  
FAX 972.643.4510

Katherine House  
85 The High Street  
Egham TW 20 9HF, UK  
TEL +44.1784.437000  
FAX +44.1784.477121

[www.tekelec.com](http://www.tekelec.com)



**TEKELEC**