AT&T’s Implementation of NSA Spying on American Citizens

31 December 2005

I wrote the following document in 2004 when it became clear to me that AT&T, at the behest of the National Security Agency, had illegally installed secret computer gear designed to spy on internet traffic. At the time I thought this was an outgrowth of the notorious “Total Information Awareness” program which was attacked by defenders of civil liberties. But now it’s been revealed by the *New York Times* that the spying program is vastly bigger and was directly authorized by president Bush, as he himself has now admitted, in flagrant violation of specific statutes and Constitutional protections for civil liberties. I am presenting this information to facilitate the dismantling of this dangerous Orwellian project.

AT&T Deploys Government Spy Gear on WorldNet Network

--16 January, 2004

In 2003 AT&T built "secret rooms" hidden deep in the bowels of its central offices in various cities, housing computer gear for a government spy operation which taps into the company's popular WorldNet service and the entire Internet. These installations enable the government to look at *every individual message* on the Internet and analyze exactly what people are doing. Documents showing the hardwire installation in San Francisco suggest that there are similar locations being installed in numerous other cities.

The physical arrangement, the timing of its construction, the government-imposed secrecy surrounding it, and other factors all strongly suggest that its origins are rooted in the Defense Department's "Total Information Awareness" (TIA) program which brought forth vigorous protests from defenders of Constitutionally-protected civil liberties last year:

> "As the director of the effort, Vice Adm. John M. Poindexter, has described the system in Pentagon documents and in speeches, it will provide intelligence analysts and law enforcement officials with instant access to information from Internet mail and calling records to credit card and banking transactions and travel documents, without a search warrant."
> --*The New York Times*, 9 November 2002

To mollify critics, the Defense Advanced Research Projects Agency (DARPA) spokesmen have repeatedly asserted that they are only conducting "research" using "artificial synthetic data" or information from "normal DoD intelligence channels" and hence there are "no U.S. citizen privacy implications" (Department of Defense, Office of the Inspector General report on TIA, December 12, 2003). They also changed the name of the program to "Terrorism Information Awareness" to make it more politically palatable. But feeling the heat, Congress made a big show of allegedly cutting off funding for TIA in late 2003, and the political fallout resulted in Admiral Poindexter's abrupt resignation last August. However, the fine print reveals that Congress eliminated funding only for "the majority of the TIA components," allowing several "components" to continue (DoD, *ibid*). The essential hardware elements of a TIA-type spy program are being surreptitiously slipped into "real world" telecommunications offices.

In San Francisco the "secret room" is Room 641A at 611 Folsom Street, the site of a large SBC phone building, three floors of which are occupied by AT&T. High speed fiber optic circuits come in on the 8h floor and run down to the 7th floor where they connect to routers for AT&T's WorldNet service, part of the latter's vital "Common Backbone." In order to snoop on these circuits, a special cabinet was installed and cabled to the "secret room" on the 6th floor to monitor the information going through the circuits. (The location code of the cabinet is 070177.04, which denotes the 7th floor, aisle 177 and bay 04.) The "secret room" itself is roughly 24-by-48 feet, containing perhaps a dozen cabinets including such equipment as Sun servers and two Juniper routers, plus an industrial-size air conditioner.

The normal workforce of unionized technicians in the office are forbidden to enter the “secret room,” which has a special combination lock on the main door. The telltale sign of an illicit government spy operation is the fact that *only people with security clearance from the National Security Agency can enter this room.* In practice this has meant that only one management-level technician works in there. Ironically, the one who set up the room was laid off in late 2003 in one of the company's endless “downsizings,” but he was quickly replaced by another.

Plans for the “secret room” were fully drawn up by December 2002, curiously only four months after DARPA started awarding contracts for TIA. One 60-page document, identified as coming from “AT&T Labs Connectivity & Net Services” and authored by the labs' consultant Mathew F. Casamassima, is titled “Study Group 3, LGX/Splitter Wiring, San Francisco and dated 12/10/02. (See sample pdf 1-4.) This document addresses the special problem of trying to spy on fiber optic circuits. Unlike copper wire circuits which emit electromagnetic fields that can be tapped into without disturbing the circuits, fiber optic circuits do not “leak” their light signals. In order to monitor such communications, one has to physically cut into the fiber somehow and divert a portion of the light signal to see the information.

This problem is solved with “splitters” which literally split off a percentage of the light signal so it can be examined. This is the purpose of the special cabinet referred to above: circuits are connected into it, the light signal is split into two signals, one of which is diverted to the “secret room.” The cabinet is totally unnecessary for the circuit to perform-- in fact it introduces problems since the signal level is reduced by the splitter—*its only purpose is to enable a third party to examine the data flowing between sender and recipient on the Internet.*

The above-referenced document includes a diagram (pdf 3) showing the splitting of the light signal, a portion of which is diverted to “SG3 Secure Room,” i.e., the so-called “Study Group” spy room. Another page headlined “Cabinet Naming” (pdf 2) lists not only the “splitter” cabinet but also the equipment installed in the “SG3” room, including various Sun devices, and Juniper M40e and M160 “backbone” routers. Pdf file 4 shows shows one of many tables detailing the connections between the “splitter” cabinet on the 7th floor (location 070177.04) and a cabinet in the “secret room” on the 6th floor (location 060903.01). Since the San Francisco “secret room” is numbered 3, the implication is that there are at least several more in other cities (Seattle, San Jose, Los Angeles and San Diego are some of the rumored locations), which likely are spread across the U.S.

One of the devices in the “Cabinet Naming” list is particularly revealing as to the purpose of the “secret room”: a Narus STA 6400. Narus is a 7-year-old company which, because of its particular niche, appeals not only to businessmen (it is backed by AT&T, JP Morgan and Intel, among others) but also to police, military and intelligence officials. Last November 13-14, for instance, Narus was the “Lead Sponsor” for a technical conference held in McLean, Virginia, titled “Intelligence Support Systems for Lawful Interception and Internet Surveillance.”* Police officials, FBI and DEA agents, and major telecommunications companies eager to cash in on the “war on terror” had gathered in the hometown of the CIA to discuss their special problems. Among the attendees were AT&T, BellSouth, MCI, Sprint and Verizon. Narus founder, Dr. Ori Cohen, gave a keynote speech. So what does the Narus STA 6400 do?

"The [Narus] STA Platform consists of standalone traffic analyzers that collect network and customer usage information in real time directly from the message...These analyzers sit on the message pipe into the ISP [Internet Service Provider] cloud rather than tap into each router or ISP device" (*Telecommunications* magazine, April, 2000),** A Narus press release (1 Dec.,1999) also boasts that its Semantic Traffic Analysis (STA) technology "captures comprehensive customer usage data...and transforms it into actionable information...[it] is the only technology that provides complete visibility for all Internet applications."***

To implement this scheme, WorldNet's highspeed data circuits already in service had to be re-routed to go through the special "splitter" cabinet. This was addressed in another document of 44 pages from AT&T Labs, titled "SIMS, Splitter Cut-In and Test Procedure," dated 01/13/03 (pdf 5-6). "SIMS" is an unexplained reference to the secret room. Part of this reads as follows:

> "**A WMS [work] Ticket will be issued by the AT&T Bridgeton Network Operation Center (NOC) to charge time for performing the work described in this procedure document**....
>
> "This procedure covers the steps required to insert optical splitters into select live Common Backbone (CBB) OC3, OC12 and OC48 optical circuits."

The NOC referred to is in Bridgeton, Missouri, and controls WorldNet operations. (As a sign that government spying goes hand-in-hand with union-busting, the entire CWA Local 6377 which had jurisdiction over the Bridgeton NOC was wiped out in early 2002 when AT&T fired the union workforce and later re-hired them as non-union "management" employees.) The cut-in work was performed in 2003, and since then new circuits are connected through the "splitter" cabinet.

Another "Cut-In and Test Procedure" document dated January 24, 2003, provides diagrams of how AT&T Core Network circuits were to be run through the "splitter" cabinet (pdf 7). One page lists the circuit IDs of key Peering Links which were "cut-in" in February 2003 (pdf 8), including ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegiance, Abovenet, Global Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet, and Mae West. By the way, Mae West is one of two key Internet nodal points in the United States (the other, Mae East, is in Vienna, Virginia). It's not just WorldNet customers who are being spied on—it's the entire Internet.

The next logical question is, what central command is collecting the data sent by the various "secret rooms"? One can only make educated guesses, but perhaps the answer was inadvertently given in the DoD Inspector General's report (cited above):

> "For testing TIA capabilities, DARPA and the U.S. Army Intelligence and Security Command (INSCOM) created an operational research and development environment that uses real time feedback. The main node of TIA is located at INSCOM [in Fort Belvoir, Virginia]..."

Among the agencies participating or planning to participate in the INSCOM "testing" are the "National Security Agency, the Defense Intelligence Agency, the Central

Intelligence Agency, the DoD Counterintelligence Field Activity, the U.S. Strategic Command, the Special Operations Command, the Joint Forces Command and the Joint Warfare Analysis Center." There are also "discussions" going on to bring in "non-DoD Federal agencies" such as the FBI.

This is the infrastructure for an Orwellian police state. It must be shut down!

* TeleStrategies postings, see:
http://www.serviceprovidersclub.com/main/event-detail.cfm?eventId=36&v=agenda
http://telestrategies.com/issworld/sponsors.htm
http://telestrategies.com/iss_2004/index.htm

** see http://www.findarticles.com/cf_dls/m0TLC/4_34/62350496/p1/article.jhtml

*** see http://www.lucent.com/press/1299/991201.nsa.html

AT&T

Labs Connectivity & Net Services

Study Group 3
LGX/Splitter Wiring
San Francisco

Issue 1, 12/10/02

Author: Mathew F. Casamassima
Email: mcasamassima@att.com
Phone: (732) 420-2033

Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

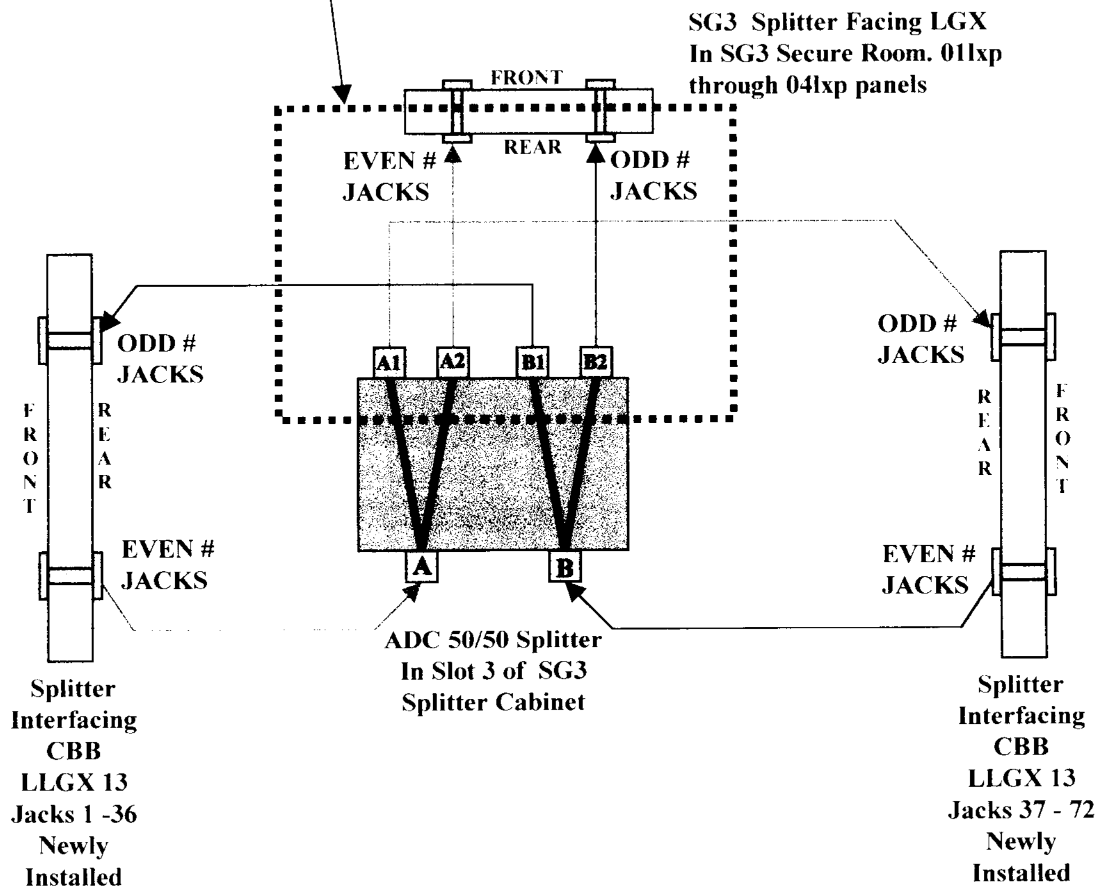
Cabinet Naming:

Equipment	Name
Splitter Cabinet	SPC
LGX Cabinet	LXC
Meta Data Cabinet	MDC
Network Management Cabinet	NMC
Data Filter Cabinet	DFC
Juniper M40E Router Cabinet	JC
Sun V880 Cabinet	S8C
Sun 3800 Cabinet	S3C
Sun Storedge Cabinet	SSC
ADC Chassis For LGX	lxp
ADC Chassis For Splitter	spp
ADC Splitter Module	spl
ADC Bulkhead Module (LGX)	bk
Juniper M160	jp
Juniper M40e	j4
Narus STA 6400	nr
Sun Fire V880/Narus Logic Server	s8
Sun Fire 3800	s3
Sun StorEdge T3	st
Sun StorEdge FC switch	sf
Cisco Catalyst 2924M-XL	cz
BayTech DS9	b9
BayTech RPC22	bv
Brocade SilkWorm 2800 Switch	bz
Lucent LGX	LLGX

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

Splitter to SG3 LGX Connectivity

The Tables in this section give the splitter to SG3 LGX connectivity as shown with in the bounds of this box.



Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

01lxp SG3 LGX Panel to Splitter Cabinet Connectivity

01lxp SG3 LGX Panel Port (In SG3 Room)	Splitter Cabinet Destination	SG3 LGX Designation Card Text	Splitter End Fiber Label Text
1	01spp/Slot 3/port 14	RR 070177.04 01spp/Slot 3/port 14	FROM: 060903.01 01lxp/JK 1 TO: 01spp/Slot 3/port 14
2	01spp/Slot 3/port 13	RR 070177.04 01spp/Slot 3/port 13	FROM: 060903.01 01lxp/JK 2 TO: 01spp/Slot 3/port 13
3	01spp/Slot 3/port 16	RR 070177.04 01spp/Slot 3/port 16	FROM: 060903.01 01lxp/JK 3 TO: 01spp/Slot 3/port 16
4	01spp/Slot 3/port 15	RR 070177.04 01spp/Slot 3/port 15	FROM: 060903.01 01lxp/JK 4 TO: 01spp/Slot 3/port 15
5	01spp/Slot 3/port 18	RR 070177.04 01spp/Slot 3/port 18	FROM: 060903.01 01lxp/JK 5 TO: 01spp/Slot 3/port 18
6	01spp/Slot 3/port 17	RR 070177.04 01spp/Slot 3/port 17	FROM: 060903.01 01lxp/JK 6 TO: 01spp/Slot 3/port 17
7	01spp/Slot 4/port 20	RR 070177.04 01spp/Slot 4/port 20	FROM: 060903.01 01lxp/JK 7 TO: 01spp/Slot 3/port 20
8	01spp/Slot 4/port 19	RR 070177.04 01spp/Slot 4/port 19	FROM: 060903.01 01lxp/JK 8 TO: 01spp/Slot 3/port 19
9	01spp/Slot 4/port 22	RR 070177.04 01spp/Slot 4/port 22	FROM: 060903.01 01lxp/JK 9 TO: 01spp/Slot 3/port 22
10	01spp/Slot 4/port 21	RR 070177.04 01spp/Slot 4/port 21	FROM: 060903.01 01lxp/JK 10 TO: 01spp/Slot 3/port 21
11	01spp/Slot 4/port 24	RR 070177.04 01spp/Slot 4/port 24	FROM: 060903.01 01lxp/JK 11 TO: 01spp/Slot 3/port 24
12	01spp/Slot 4/port 23	RR 070177.04 01spp/Slot 4/port 23	FROM: 060903.01 01lxp/JK 12 TO: 01spp/Slot 3/port 23
13	01spp/Slot 5/port B2	RR 070177.04 01spp/Slot 5/port B2	FROM: 060903.01 01lxp/JK 13 TO:01spp/Slot 5/port B2
14	01spp/Slot 5/port A2	RR 070177.04 01spp/Slot 5/port A2	FROM: 060903.01 01lxp/JK 14 TO:01spp/Slot 5/port A2
15	01spp/Slot 6/port B2	RR 070177.04 01spp/Slot 6/port B2	FROM: 060903.01 01lxp/JK 15 TO:01spp/Slot 6/port B2
16	01spp/Slot 6/port A2	RR 070177.04 01spp/Slot 6/port A2	FROM: 060903.01 01lxp/JK 16 TO:01spp/Slot 6/port A2

AT&T

Labs Connectivity & Net Services

SIMS
Splitter Cut-In and Test Procedure

Issue 2, 01/13/03

Author: Mathew F. Casamassima
Email: mcasamassima@att.com
Phone: (732) 420-2033

SIMS - Splitter Test and Cut-In Procedure

Issue 2, 01/13/03

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

1. *Procedure Overview*

A WMS Ticket will be issued by the AT&T Bridgeton Network Operation Center (NOC) to charge time for performing the work described in this procedure document. At some point prior to the splitter cut-in being performed your office will be contacted by the Bridgeton Network Operations Center (NOC) to confirm the WMS Ticket has been received. Bridgeton NOC personnel will again contact OSWF the night of the cut to begin coordination. The work described in the procedure will be supported, on-site, by an IP Field Support Specialist (FSS) from the Day Tech organization.

This procedure covers the steps required to insert optical splitters into select live Common Backbone (CBB) OC3, OC12 and OC48 optical circuits. The splitter insertion will be accomplished by removing existing optical cross-connects and installing new cross-connects all within the CBB LGX complex. The optical splitters will be contained in a standalone cabinet located in the proximity of the CBB LGX complex. The splitters will be pre-cabled by an EF&I vendor to the rear of a dedicated LGX bay (LLGX13) within the CBB LGX complex. A partial installation and test of cross-connects can be done prior to the actual splitter cut-in. This portion of the work can be done outside the CBB maintenance window. An IP FSS member of the Day Tech organization will contact OSWF to schedule the pre-cut portion of the work. Section 2 of this document will describe the pre-cut installation of cross-connects and the pre-cut testing of the new circuit path. The actual cut-in of the splitter will be done during the CBB maintenance window and will be closely coordinated with the Bridge NOC and will be supported, on-site, by an IP FSS member of the Day Tech organization. The actual splitter cut-in is described in Section 3 of this document.

The number of cross-connects required and the final path the circuit will take is dependant on the location of the affected LGX bays within the multiple line-ups of the CBB LGX complex. This procedure will describe all possible splitter cut-in circuit paths. The procedure will also describe the procedures for testing each possible circuit path.

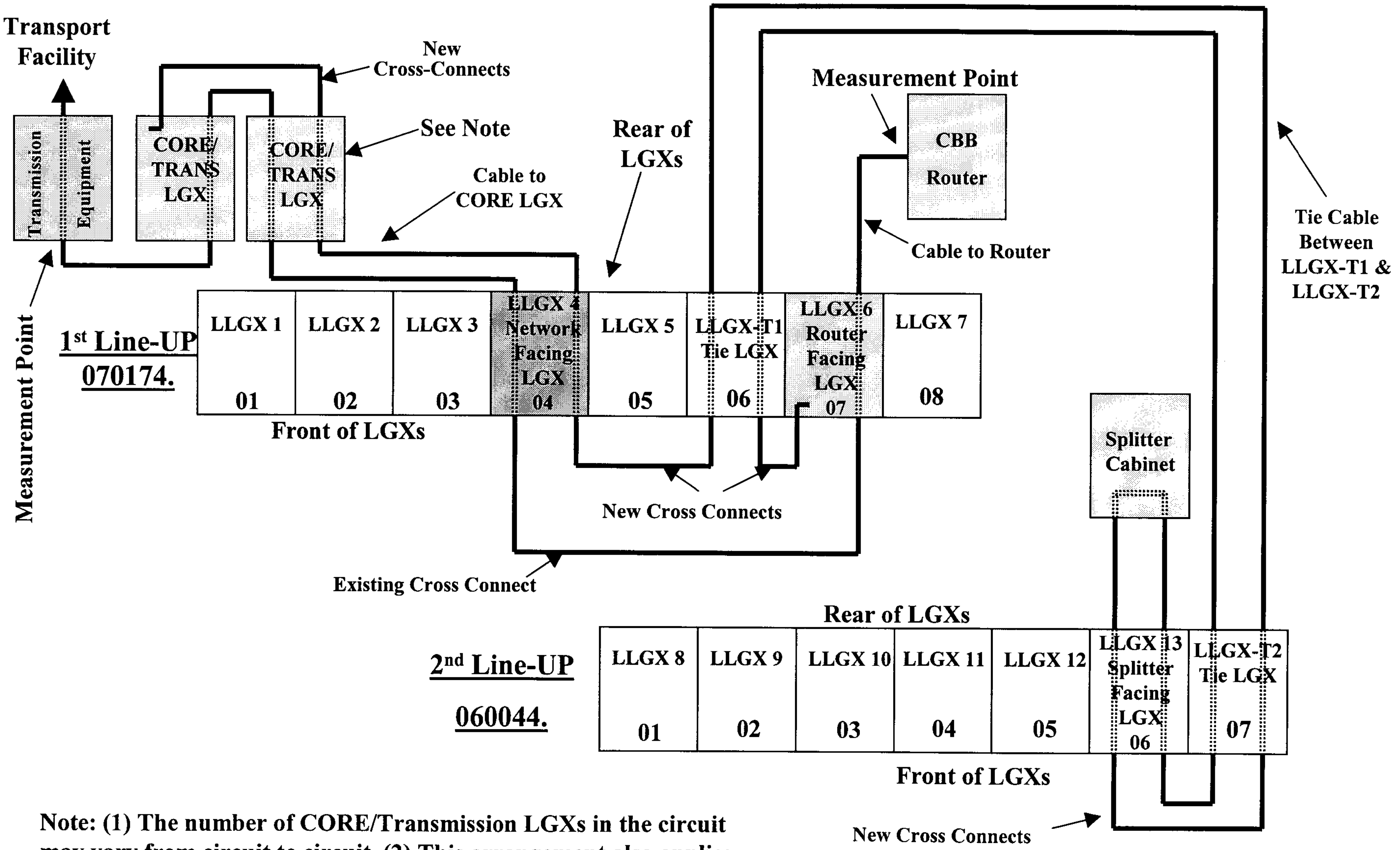
1.1. How to Use this Procedure

This procedure document is quite long. **It is not necessary to read this whole document to do the work.** There are 4 possible LGX arrange that may encounter. By reading section **1.2** below, determine which LGX arrangement applies to the circuit you are working. Then, after reading the introductory paragraphs in Sections 2 and 3, go directly to the subsections within Sections 2 and 3 associated with the LGX arrangement you are dealing with.

1.2. LGX Definition and LGX-Arrangement:

LGX Definition: There are multiple LGX bays affected by this procedure. Within the CBB LGX complex LGX bays follow a specific naming convention (LLGX 1, LLGX2, LLGX3, LLGX4, ...). This naming convention is uniform across sites. Since this document is designed to cover all sites, this uniform naming convention will be used here. Site-specific engineering will use the LGX FIC code rather than the naming. Prior to the start of the work described here the local IP FSS will label the LGX bays with the naming as presented in this document. The following are generic definitions for the LGX bays affected by this procedure:

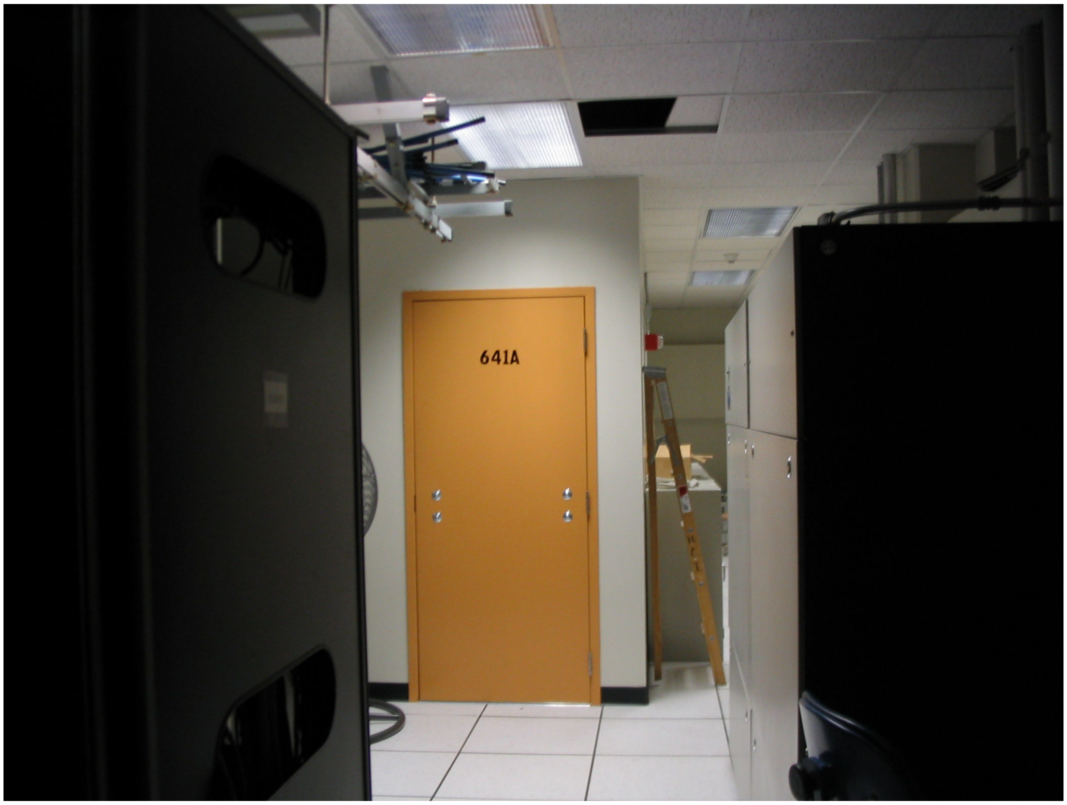
Figure 5 - Arrangement 3 - Circuit Connectivity – **Cut Night Measurements**
Network Facing & Router Facing LGX in 1st Line-Up / Splitter Facing LGX in 2nd Line-Up
Overhead View of Bays **(Applies to Circuits AGEC.671212, AGEC.622360, AGEC.622352, IVEC.517519, IVEC.578278, IVEC.502963, IVEC.547506, IVEC.509396, IVEC.597263, IVEC.502961, IVEC.502960 & IWEC.502947)**

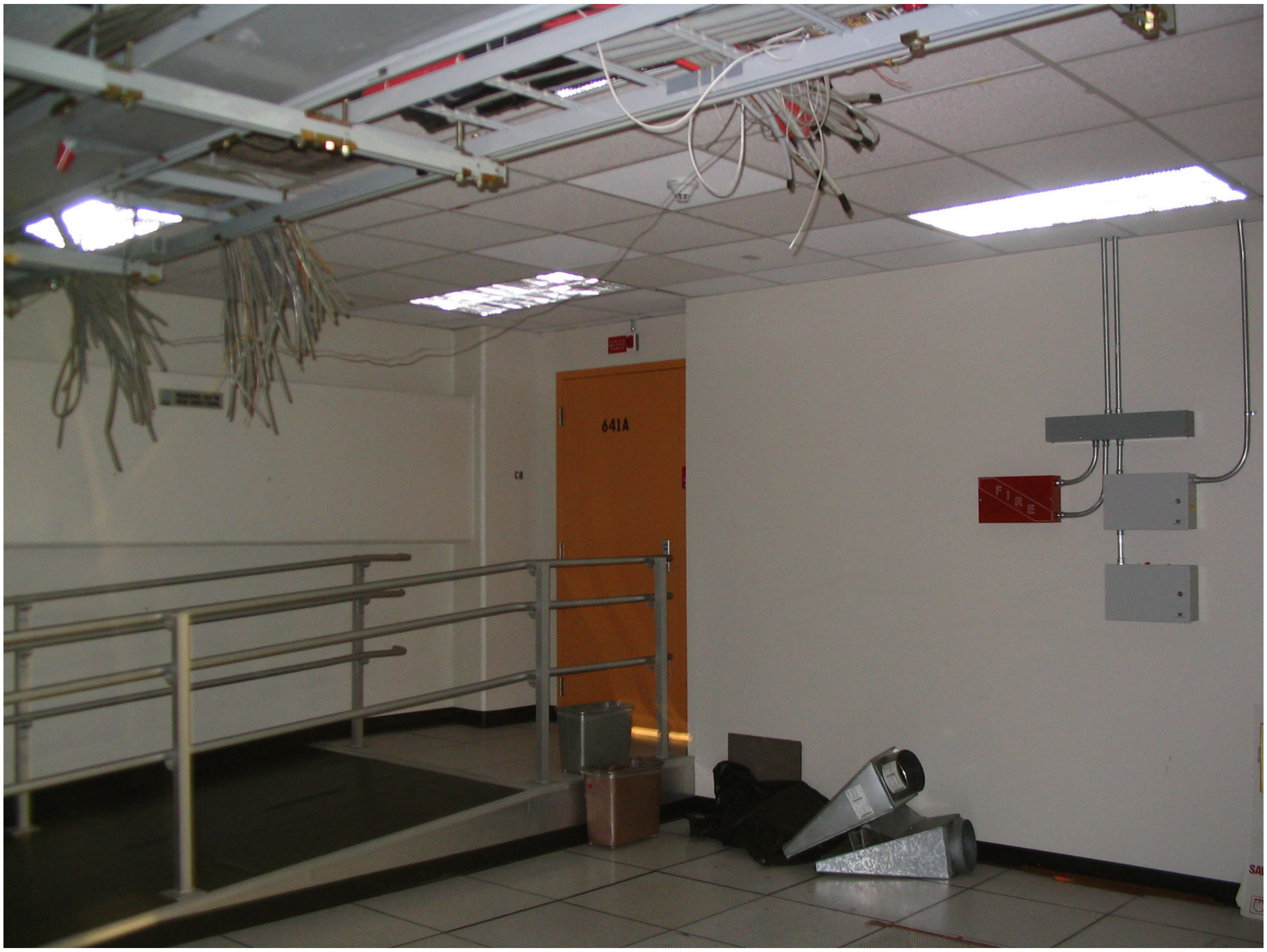


Note: (1) The number of CORE/Transmission LGXs in the circuit may vary from circuit to circuit. (2) This arrangement also applies to circuit AGEC.242541 except the Router facing LGX is LLGX 5.

Priority	Peering Link	Ckt Type	ID	AS Number	Circuit Comments	Router	Port	Circuit Engineering Change Order Issue Date	Circuit Engineering Complete Date Requested	Circuit Engineering Complete Date Actual	Splitter Pre-Test Date	Splitter in Circuit Date	Splitter Active Date	Comments
1	ConXion	OC-3	AGEC.622352	4544		sffca01ck	POS 1/3	1/22/2003	1/31/2003	1/22/2003	2/4/2003	2/6/2003		
2	Verio	OC-12	IVEC.517519	2914		sffca01ck	POS 3/1	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
3	XO	OC-12	IVEC.578278	2828		sffca01ck	POS 3/2	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
4	Genuity	OC-12	IVEC.502963	1		sffca01ck	POS 3/3	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
5	Qwest	OC-12	IVEC.547506	209		sffca01ck	POS 5/2	1/30/2003	2/7/2003	1/23/2003	2/11/2003	2/13/2003		
6	PAIX	OC-12	IVEC.509396	nap		sffca01ck	POS 8/1	1/30/2003	2/7/2003	1/23/2003	2/11/2003	2/13/2003		
7	Allegiance	OC-12	IVEC.597263	2548		sffca01ck	POS 8/3	1/30/2003	2/7/2003	1/24/2003	2/11/2003	2/13/2003		
8	Abovenet	OC-12	IVEC.502961	6461		sffca01ck	POS 9/2	1/30/2003	2/7/2003	1/24/2003	2/11/2003	2/13/2003		
9	Global Crossing	OC-12	IVEC.502960	3549		sffca01ck	POS 9/3		2/14/2003		2/18/2003	2/20/2003		
10	C&W	OC-48	IWEC.502947	3561		sffca01ck	POS 2/0		2/14/2003		2/18/2003	2/20/2003		
11	UUNET	OC-48	IWEC.509433	701		sffca02ck4	POS 2/0		2/14/2003		2/18/2003	2/20/2003		
12	Level 3	OC-48	IWEC.509434	3356		sffca02ck4	POS 3/0		2/14/2003		2/18/2003	2/20/2003		
13	Sprint	OC-48	IWEC.509438	1239		sffca02ck4	POS 11/0		2/21/2003		2/25/2003	2/27/2003		
14	Telia	OC-3	AGEC.671212	1299		sffca01ck	POS 0/1		2/21/2003		2/25/2003	2/27/2003		
15	PSINet	OC-3	AGEC.622360	174		sffca01ck	POS 0/2		2/21/2003		2/25/2003	2/27/2003		
16	Mae West	OC-3	AGEC.242541	nap		sffca82ck	POS 2/5		2/21/2003		2/25/2003	2/27/2003		

Entrances to the “secret room” at AT&T central office, 611 Folsom St., San Francisco





CLICK HERE TO GO TO TeleStrategies® www.telestrategies.com

SERVICE PROVIDERS CLUB

Home | Benefits | Become A Member | On-Line Tutorials | Club Meetings | Contact Us

MORE INFO

AGENDA

REGISTER

ISS World 2003:Intelligence Support Systems for Lawful Interception and Internet Surveillance Conference and Exhibits
Hosted by TeleStrategies

November 12 , 2003 : McLean, VA
TIME: 8:00 AM - 4:00 PM

Agenda:

November 13
8:30-10:00
Keynote Session
This keynote session addresses the new problems and challenges facing telecommunications service providers and law enforcement agencies regarding lawful interception and Internet surveillance. The distinguished panel will give their insight on such questions as “Is Intelligence Support Systems (ISS) a market of industry on its own?” “Are ISS just add-on features to billing systems, mediation devices, circuit switches or routers?” “How do service providers make a business case for ISS investment” “Can ISS investments be justified by revenue assurance, fraud detection or infrastructure protection?” And more!
Moderator
• *Dr. Jerry Lucas, President, TeleStrategies*
Panelists
• *Dr. Ori Cohen, Founder, Narus*
• *Tony Rutkowski, President, Global LI Industry Forum and VP, VeriSign*
• *Stewart Baker, Partner, Steptoe & Johnson*
• *Gene McLean, VP and Chief Security Officer, Telus Communications*
• *William Crowell, IT Consultant, Security and Intelligence Systems*
•*Albert Gidari, Partner, Perkins Coie LLP*

10:00-6:00
Exhibits Open

10:30-12:00
*Session A: **FCC and FBI Update***
There are numerous vexing questions raised with the convergence of voice and data, voice over the Internet, does CALEA apply to Internet services and funding of IP CALEA. This panel addresses these and other issues from a federal government regulatory and law enforcement perspective.
• *Scott Marcus, Senior Advisor for Internet Technology, Office of Strategic Planning and Policy Analysis, FCC*
• *Eric Mason, Supervisory Special Agent , CALEA Implementation Unit, of the Electronic Surveillance Technology Section.*

• *Agent Martin J. King, Supervisory Special Agent, Technology Law Unit, Office of the General Counsel, FBI*
• *James Craig, Special Agent in Charge of New Orleans DEA Field Division*

OTHER UPCOMING EVENTS

Understanding the New Telecommunications Technologies and Industry Dynamics
- **February 17 - 18 , McLean**
- Sponsored By: TeleStrategies

More Info Register

Accelerating Profit Potential-Obtaining the Right Information for Porting, Billing and Provisioning
- **February 23 , McLean**
- Sponsored By: TeleStrategies

More Info Register

Mastering Resale in a Microsoft.NET World
- **March 11 , McLean**
- Sponsored By: TeleStrategies

More Info Register

Session B: ***Internet Surveillance Options***

There are two approaches telecommunications service providers have to support lawful interception and Internet surveillance. They can either create their own ISS infrastructure or they can outsource. Two leading vendors will present their visions and solutions.

- *Dr. Ori Cohen, Founder, Narus*
- *Raj Puri, Vice President, VeriSign*

12:00-1:30

Hosted Lunch

1:30-3:00

Session A: ***International Development in Lawful Interception***

Lawful interception is a global requirement. However, surveillance laws and requirements differ from country to country and region to region. A further complication is surveillance activities cross international boundaries. The panelists will address the differences between North America and Western Europe, and the United States and Canada regarding lawful interception as well as global cooperative efforts underway.

- *Tony Rutkowski, President, GLIIF and VP NetDiscovery, Verisign*
- *Frank Fransen, TNO Telecom, The Netherlands*
- *Ian Cooper, HomeOffice, National Technical Assistance Centre, (UK)*
- *Jay Thomson, President, Canadian Association of Internet Providers*
- *Gene McLean, VP and Chief Security Officer, Telus Communications*

Session B: ***Electronic Surveillance Challenges and Solutions for Wireless Service Providers***

Mobile wireless communications is the service choice of drug dealers, terrorist and other criminals. The surveillance challenges are many including roaming, pre-paid and the new IP data services. The panel will address today's regulatory issues and technology solutions assisting law enforcement including precise location service and packet data interception.

- *Julius Knapp, Deputy Chief of Office of Engineering and Technology, FCC*
- *Todd McDermott, Vice President, Verint Technology*
- *Joe Hogan, CTO, Openet Telecom*

3:30-5:00

Session A: ***Electronic Surveillance Challenges in Supporting Local and State Law Enforcement***

The interface between telecommunications service providers and law enforcement agencies is crucial in the war against criminals and terrorists. This session looks at the issues from a former local prosecutor and law enforcement prospective. The panel will address the challenges of wireless state to state roaming, as well as the issues of dealing with subpoena backlogs, service provider technical support and electronic delivery of intercept data.

- *Owen Carragher, Partner, Lankler and Carragher*
- *Kenneth Hicks, Special Agent, Criminal Intelligence Division, Technical Support Unit, Virginia State Police*
- *Sgt. David Heslep, Technical Assistance Section Supervisor, Technical Investigation Division, Maryland State Police*
- *Sgt. Donald Yates, Major Narcotics Branch, Electronic Surveillance Unit, Metropolitan Police Department, Washington, D.C.*

Session B: ***Electronic Surveillance Challenges and Solutions for Cable VoIP Providers***

The cable TV industry is preparing the first massive roll out of VoIP in the local exchange environment. Meeting CALEA and Internet surveillance mandates is a challenge. In this regard, CableLabs has been at the forefront of standards development for local VoIP service. This panel looks at cable standards, equipment and cable operator readiness to support lawful interception.
• Eric Rosenfeld, Project Director, PacketCable Security, CableLabs
• Cherie Kiser, Partner, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo
• Cemal T. Dikmen, General Manager, Lawful Intercept Products, SS8 Networks
• Rafael Fonseca, Senior Director, Product and Network Evolution, Cedar Point Communications

5:00-6:00
Evening Reception
Sponsored by: Narus

November 14
8:00-10:00
Session A: **Electronic Surveillance Cost Recovery Solutions**
Service providers receive subpoenas, court orders and search warrants requiring the production of records and technical assistance. The panel will discuss which law enforcement related costs are reimbursable and provide guidance in developing the reimbursement request.
• H. Michael Warren, President, Fiducianet
• Mark Tauber, Chair, Telecom Practice Group, Piper Rudnick
• Other speakers to be announced

Session B: **Next Generation Internet Surveillance Tools**
Government mandates for Internet surveillance has stimulated new product development and approaches. This panel addresses how to transform packet intercept into intelligence, new developments in non-intrusive probes and Internet Access Point (IAP) function options.
• Arkady Linshitz, Director of Marketing, ECTel
• Adam Weinberg, Director of Technologies, Nice Systems Ltd
• Tal Givoly, Chief Scientist, XACCT Technologies
• Fred Dohen, General Deputy Manager, Aqsacom

Session C: **Electronic Surveillance Solutions for VoIP Service Providers**
VoIP presents major challenges to lawful interception. This panel addresses what VoIP signals need to be intercepted, how should the signals be handed over to the LEA and when should a service provider have lawful interception capabilities in place.
• Frank Fransen, TNO Telecom, The Netherlands
• Dave Ashby, Regional Manager, MetaSwitch
• Mandy Schuyler, VP, Product Solutions, Sotas
• Charllie Baker, Product Manager, Brooktrout Technology

10:00-1:00
Exhibits Open

10:30-11:30
Session A: **Law Enforcement Support Services**
Outsourcing law enforcement support services is an option for telecommunications service providers just like billing and other OSS/BSSs. This session presents alternatives to meeting legal demands

for customer records and technical assistance and explores various options for managing these outsourced functions.

• *H. Michael Warren, President, Fiducianet*

• *Bill Oswald, Senior Consultant, Crucial Security, Inc., and former Executive Director of Security, Qwest*

Session B: **Electronic Surveillance Standards Update** (10:30-12:30)
Standards in support of lawful interception is a three-legged stool. First you need standards for the interface between the Law Enforcement Agency to service providers infrastructure, second you need standards for ISSs internal to service providers infrastructure, finally, you need global standards to support international law enforcement activities and ISS industry development. This panel addresses the status of standards in ATIS T1S1, ETSI, OASIS, CableLabs and other standard bodies around the world.

Moderator

• *Tony Rutkowski, President, GLIIF and VP, NetDiscovery, Verisign*

Panelists

• *Ian Cooper, National Technical Assistance Center, HomeOffice, (UK)*

• *Greg Ratta, Vice Chairman, T1S1 Lawfully Authorized Electronic Surveillance and Lucent Technologies*

• *Eric Rosenfeld, Project Director, PacketCable Security, CableLabs*

• *Stewart Baker, Partner, Steptoe & Johnson*

Session C: **Electronic Surveillance Challenges and Solutions for ISPs**
ISPs were not covered under CALEA but lawful interception mandates were under the USA Patriot Act. This panel explores implications of new FCC proceedings as well as what COTS tools are available that both LEAs and ISPs can use today for Internet surveillance.

• *David Baker, VP, Law and Public Policy, EarthLink*

• *Paul Thornton, Customer Services Manager, Accuris*

• *Ken Georgiades, Senior Director, Top Layer Networks*

11:45-12:30

Session A: **Router-Based Solutions for Lawful Intercept**
Conventional packet switches can perform the Intercept Access Point (IAP) function as an alternative to dedicated probes. This session addresses the advantages of the router approach, the IAP “toolkit” functions available in modern COTS routers/CSR platforms to support lawful intercept, and using XML for mediation content of the IAP.

• *Tim LeMaster, Systems Engineer, Juniper Networks*

Session B:**Electronic Surveillance Standards Update** (continued from 10:30 session)

Section C: **SS7-Based Solutions for Lawful Interception**
The nervous system of today’s PSTN is the Signaling System 7 (SS7) network. This session looks at the value that SS7 brings when used for lawful intercept and the types of tools that can be used to automate the process of intelligence gathering.

• *Travis Russell, Product Marketing, Tekelec*

TeleStrategies®
www.telestrategies.com

ISS World 2003

Intelligence Support Systems for Lawful Interception and Internet Surveillance

November 13-14, 2003 - McLean, VA

Click on the brochure cover to download a conference brochure

Conference Agenda | Pre-Conference Tutorial | Sponsoring Companies | Hotel Information | Register Now!

For sponsorship or exhibiting information, contact Tatiana Lucas at 703-734-2639, or talucas@telestrategies.com

LEAD SPONSOR

NARUS®

Narus' software products provide real-time information from the world's largest telecommunications networks and are able to respond with action. These products empower carriers & operators to offer value-based services, lower delivery costs, and protect network infrastructure. Narus also enables government & law enforcement agencies to monitor and intercept intelligence for national security purposes. Narus is the recognized performance leader, with production environments exceeding 10 billion records per day, for global applications in wireless, WiFi, prepaid, broadband, voice and data. Customers include Cable & Wireless, Comcast, KDDI, KPN, T-Mobile, Ono, Qwest and WilTel. Narus is headquartered in Palo Alto, California with offices throughout the world. Backed by AT&T, Bowman Capital, JP Morgan, Intel, Mayfield, and NTT, Narus is fully-funded, and privately held.

ASSOCIATE SPONSOR

VeriSign®
The Value of Trust℠

VeriSign, Inc. (Nasdaq: VRSN), delivers critical infrastructure services that make the internet and telecommunications networks more intelligent, reliable and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence. Additional news and information about he company is available at http://www.verisign.com

OTHER SPONSORS & EXHIBITING COMPANIES

AQSACOM

SS8 Networks

ecTel

NICE

TEKELEC

VERINT.
POWERING ACTIONABLE INTELLIGENCE

ClearTrail

Lucent Technologies
Bell Labs Innovations

TeleStrategies, Inc.
7918 Jones Branch Dr., 3rd Floor
McLean, VA 22102
voice: 703-734-7050 fax:703-893-3197

TeleStrategies®
www.telestrategies.com

ISS World 2004

Intelligence Support Systems for Lawful Interception, Fraud Control and Network Security

May 5-7, 2004 - Washington, D.C.

Call For Speakers

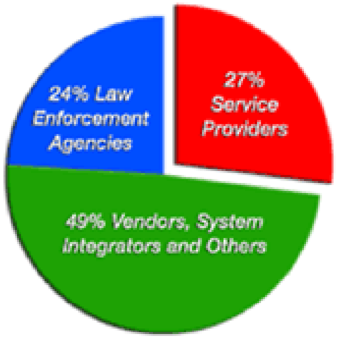
Call for Speakers | Conference Location | Exhibitors & Sponsors Info | Last Years Brochure (pdf) | Register Now!

ISS World is now an international event where service providers, law enforcement agencies, other government officials and vendors can meet to create cost effective lawful interception, fraud control and network security solutions that balance privacy, national security and public safety. Last November's' ISS World attracted 221 attendees, over half of whom were service providers and law enforcement agents. We believe this is the largest gathering of its kind open to service providers vendors and law enforcement agencies.

This May's ISS World exhibits will be collocated with Billing and OSS World 2004 exhibits. Many lawful interception, fraud control and network security vendors are also in this market space. More importantly for ISS World exhibitors, lawful interception managers also report to the same senior managers that have Billing and OSS oversight responsibilities.

For information on presenting, sponsoring or exhibiting at ISS World 2004, contact Tatiana Lucas, Director of Business Development at talucas@telestrategies.com or call 703.734.2639.

ISS World 2003 Attendees



Service Providers

AT&T
AT&T Wireless
BellSouth
Bluegrass Cellular
British Telecom
Comcast
Earthlink
ICG Communications
Intelus
LDMI Telecom
Level 3
Lightship Telecom
MCI
Nemont Telephone
Nextel
Pac-West
South Central Rural Telephone
Sprint
Sprint PCS
T-Mobile
Telus
Telenor
TelePacific Communications
Telestra
U.S. Cellular
United Online
Verizon
Z-Tel

Law Enforcement Agencies

Australian Federal Police
D.C. Police Department
Drug Enforcement Administration
Federal Bureau of Investigation
Florida Dept. of Law Enforcement
Maryland State Police
National Drug Intelligence Center
Quebec Police Force
Royal Canadian Mounted Police
U.S. Capital Police
U.S. Secret Service
Vancouver Police Department
Virginia State Police

Attending Countries

Argentina
Australia
Canada
Denmark
France
Germany
Ireland
Israel
Italy
Netherlands
Philippines
Singapore
Sweden
United Kingdom
United States

TeleStrategies, Inc.
7918 Jones Branch Dr., 3rd Floor
McLean, VA 22102
voice: 703-734-7050 fax:703-893-3197

You are Here: Articles > Telecommunications > April, 2000 > Article

Narus Defines Internet Business Infrastructure Market.(Software Development Kit, Virtual Analyzer)(Product Announcement)
Telecommunications, April, 2000

www.narus.com

Most ISPs have focused on building out their networks and plugging customer usage data into generic, flat-rate billing applications, with profit margins an afterthought. But to stay afloat, ISPs need real-time customer usage data, analysis and applications. A new market has emerged that some expect will turn customer usage data into gold mine for ISPs. Internet business infrastructure (IBI) will permit ISPs to collect and analyze information about customers and network patterns in real time and then act on that intelligence to deliver enhanced products and services. The Yankee Group predicts ISPs will look to IBI applications for data collection and aggregation, IP billing and fraud analysis, operations support and business planning. The research group estimates the IBI market this year will reach $525 million, growing to $7.6 billion in 2004.

Narus Inc. has helped ignite this market with its Software Development Kit (SDK) Platform, which is now available. The STA Platform consists of standalone traffic analyzers that collect network and customer usage information in real time directly from the message don't affect rate, content or network performance. "This is novel in the industry," according to Karl Whitelock, program director of Stratecast Partners, OSS Competitive Strategies Analysis Service. These analyzers sit on the message pipe into the ISP cloud rather than tap into each router or ISP device. Consequently, Narus has interoperability on its side because it's not connected to a device like other vendor offerings, according to Whitelock.

To further support interoperability, Narus has introduced Virtual Analyzer Plug-ins that permit different types of data collection for ISPs that might, for example, use Cisco routers with NetFlow, SNMP over a gateway device, or server logs from an application server. The NetFlow Plug-ins for SNMP and log files will be available in Q2. Narus is also testing its STA technology with Cisco's 12000 Gigabit Switch Router.

Narus LogicServers then aggregate the data and apply business rules, or RuleSets, to transform the data into information for specific applications for billing, customer care, business analysis, fraud detection, usage profiling and customer retention. Currently, Narus offers Intelligence and a Billing Mediation System (BMS). Narus Intelligence, which is shipping, supports analysis and other decision-support activities in IP networks. The BMS began shipping in December 1999, and the company is working to integrate it into Cisco's OSS reference architecture.

Recognizing the importance of a standard billing protocol, Narus co-founded with AT&T the Internet Protocol Detail Record (IPDR) Working Group, the purpose of which is to develop Internet billing standards. But Whitelock contends that Narus and other IBI players should focus on making a flexible product, regardless of protocol.

ISPs can also use the SDK v.1.0 application programming interface to customize the STA platform with custom logic RuleSets. Narus, however, does not position itself as an applications provider. Instead, through its Solution Partner Program. Narus has joined forces with application heavy-weights and network platform developers, including Amdocs, Convergys, Portal, Solect and sun Microsystems. Convergys, for example, has added QoS pricing as well as scalability to aggregate billing data for millions of users in real time. Whitelock considers the application-development aspect of IBI as a significant market opportunity: "Narus is providing the means through which service providers can how generate revenues not associated with actual network usage. Thus, service providers have a market opportunity for information that has nothing to do with the network services you provide." SDK v. 1.0 runs on Microsoft Windows and NT and is deployed or is being looked at by more than two dozen service providers, including MediaO ne.

1

Related Terms

- Computer software industry Product introduction
- Internet service providers Planning
- Performance analysis software Product introduction
- Program development software Product introduction

DIRECTORY WEB ARTICLES

SEARCH all magazines FOR Search · Advanced Search · Help

Home | Solutions and Products | Customer Support | Bell Labs | About Lucent   Glossary   Contact us   Log in

Search
Go
Advanced search

About Lucent:
News & Events
- Press Room
- Events/Speakers
- Photo Gallery
- Press Contacts

Investor Relations
Company Information
Work@Lucent
Partner Programs

Select Month Go
Search press releases
Go

Lucent Technologies
Bell Labs Innovations

NARUS teams with Lucent Technologies to deliver industry's first IP Business Infrastructure solution for OC-48 carrier networks

FOR RELEASE WEDNESDAY DECEMBER 01, 1999

Lucent's breakthrough technology allows NARUS to scale semantic traffic analysis technology to meet the needs of the highest-speed IP networks

REDWOOD CITY, Calif. - (Editor's note: This release was issued by NARUS Inc.) NARUS Inc., the leading provider of IP Business Infrastructure (IBI) solutions, announced today that it will use breakthrough Optical Area Networking technology from Lucent Technologies (NYSE: LU) in its NARUS Semantics™ solutions. This will enable service providers to develop, price and deploy new services for their target customers at the speed of light.

Specifically, NARUS is integrating Lucent's OptiStar™ OC48 network adapter cards into its NARUS Semantics Analyzers, which form the first tier of its Semantic Traffic Analysis (STA) technology platform. With the new OptiStar-enabled devices from NARUS, service providers using optical networks will, for the first time, have real-time access to critical customer usage information, allowing them to better understand their customers' preferences, track network use, and provide services more closely tailored to their customers' needs.

"NARUS is dedicated to providing service providers of all sizes with the information they need to remain competitive, profitable, and customer-focused," stated Mark Stone, NARUS' President and COO. "This 'win-win' agreement using Lucent's advanced optical area networking technology will allow us to scale to meet the needs of any service provider on the planet - whether that provider has a customer base in the hundreds or millions."

Lucent's OptiStar OC48 is an IP network adapter card that can be plugged into servers and other network appliances, connecting them directly to the backbone network using high-speed fiber optics. Supporting speeds up to 2.5 gigabits per second (Gb/s), the OptiStar OC48 enables servers and other appliances to operate at much higher speeds than they do today, while minimizing network complexity.

"Our breakthrough Optical Area Networking technology is ideally suited for NARUS' platform," stated Tim Sullivan, Lucent's Vice President and General Manager, Optical Area Networking. "We are pleased to be playing an integral role in helping NARUS deliver these leading IBI solutions to the marketplace."

Integration of OptiStar

technology into the NARUS Semantics Platform allows NARUS to assist even the largest providers of IP services to expand their focus from building reliable, scalable networks to delivering differentiated services - such as IP telephony, video conferencing, and applications hosting. NARUS Semantics Analyzers, which form the first tier of the Platform, are unique hardware appliances that install easily in any network and capture application-level usage information in real time directly from the network without any impact on performance.

The Analyzers pass data to NARUS Semantics LogicServers, which form the second tier of the Platform. The LogicServers further process the data according to flexible business rules, and provide the resulting usage information to applications such as the NARUS Intelligence decision support application, the NARUS Billing Mediation System and other applications from third parties including fraud detection, churn management and service planning.

NARUS Semantics Analyzers enabled with Lucent's OptiStar OC48 technology will be available in Q1 of next year.

About NARUS:
NARUS, the leading provider of IP business infrastructure (IBI) solutions, gives IP service providers the flexibility to implement and manage new services and business models profitably, and at will. NARUS' solutions are based on the company's Semantic Traffic

Analysis (STA) technology, which captures comprehensive customer usage data directly from carrier-grade networks and transforms it into actionable information. The patent-pending STA technology, which is the only technology that provides complete visibility for all Internet applications, is the foundation for applications that range from decision support to IP billing mediation. NARUS is a founding member of the Internet Protocol Data Record (IPDR) initiative, along with AT&T, TeleStrategies, and many others. Privately held and based in Redwood City, CA, NARUS investors include Frontier Internet Ventures, Inc., a subsidiary of Frontier Communications (NYSE: FRO), MediaOne Ventures, a division of MediaOne Group (NYSE: UMG), Mayfield Fund, Walden Ventures, Chase Capital, and others. The company's Web address is http://www.narus.com.

ABOUT LUCENT
Lucent Technologies is a global leader in optical networking technology. Bell Labs, Lucent's research and development, has garnered more than 2,000 patents in optical technology alone. And with more than 4,000 dense wave division multiplexing (DWDM) systems installed, Lucent has the largest global deployment of next-generation optical networking systems. Lucent Technologies designs, builds and delivers a wide range of public and private networks, communications systems and software, data networking systems, business telephone systems and microelectronics

components. For more information about Lucent Technologies, visit its Web site at http://www.lucent.com.

For more information, reporters may contact:

Frank Briamonte
Lucent Technologies
908) 559-5692 - office
(800) 607-9849 - pager
Email:fbriamonte@lucent.com

Deborah Hamilton
Sterling Communications
(408) 441-4100
Email:dhamilton@sterlingpr.com

Richard Kagan
NARUS, Inc.
(650) 306-9100
Email:rickk@narus.com

View the information and policies regarding Lucent's press release archive.