SOLUTION BROCHURE

LAWFUL INTERCEPT SOLUTION

Building the Foundation for Lawful Intercept Compliance at Minimal Cost and Without Impacting Network Traffic Integrity or Performance

Lawful Intercept Solution Overview

New emphasis has been placed on regulations for authorized monitoring of data traffic as it crosses carrier networks. Enabling lawful intercept (LI) has consequently become a crucial issue for network service providers. As concern grows over everything from global terrorism to electronic fraud, the ability to catch network traffic and isolate it for in-depth analysis takes on much greater importance. Law enforcement authorities now require the ability to focus on individual subscribers and to monitor where data traffic is coming from, where it's headed, and what it might contain. This leaves carriers no choice but to implement technology that allows this close inspection – without impacting performance or the integrity of customer traffic.

Juniper Networks® routers incorporate technology that helps carriers enable LI of data traffic and demonstrate regulatory compliance. These routers feature highly granular packet filtering for selecting only those flows under surveillance, port mirroring for replicating that traffic, and forwarding capabilities for sending it to specialized mediation platforms for analysis. Further, Juniper Networks implementation of filtering and port mirroring has no impact on the forwarding performance of its routers. This is not the case with traditional routers, whose performance limitations have forced the current approach to LI, in which service providers deploy multiple, often costly external probes to handle the filtering and application-layer content processing. In contrast, Juniper Networks enables deployment architectures for LI that are highly scalable in terms of both capacity and operations, and that reduce the number of expensive content processing platforms.

These capabilities are an integral part of Juniper Networks' broad security capabilities, which provides a comprehensive approach to safeguarding voice, video, and data as they traverse carrier networks. With the Juniper Networks LI solution, carriers can comply with regulations without impacting the quality of their vital, revenue-generating services.

Figure 1 illustrates the general network architecture of Juniper Networks two approaches to filtering and replicating traffic, before passing it on to a law enforcement agency (LEA).

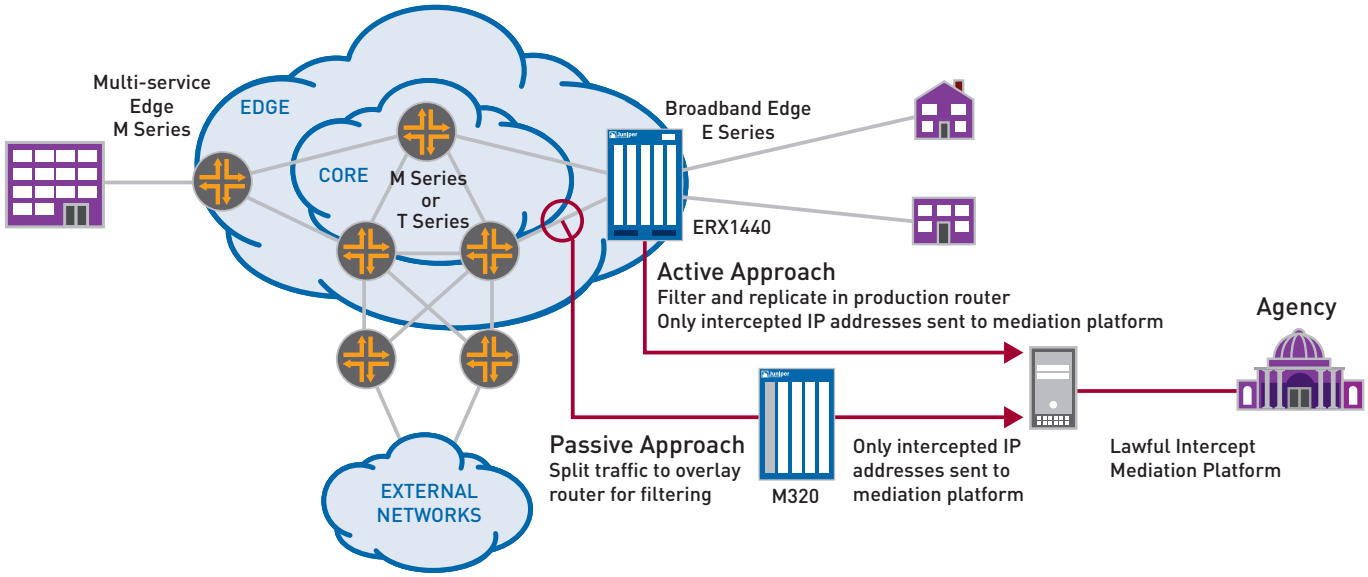

Figure 1: Juniper Networks LI Approaches

The LI Basics

Learning how LI affects carriers means learning exactly what it is and how it works. Simply put, LI is legally sanctioned access to private communications between organizations or individuals – whether phone calls or email – by law enforcement authorities.

In many countries, rules governing LI were established early in the history of voice telephony. The rules for LI of data communications are newer and are currently being added into legislation around the globe (see sidebar: LI Rules and Regulations). Generally, the following points apply when it comes to implementing LI and demonstrating regulatory compliance:

- LI processes cannot be detectable by the party under surveillance.
- Unauthorized personnel cannot perform LI themselves or have knowledge about specific intercepts.

- Separate agencies targeting the same party must not be able to detect one another.
- Service providers must decrypt information for law enforcement officials, if they have access to the keys.

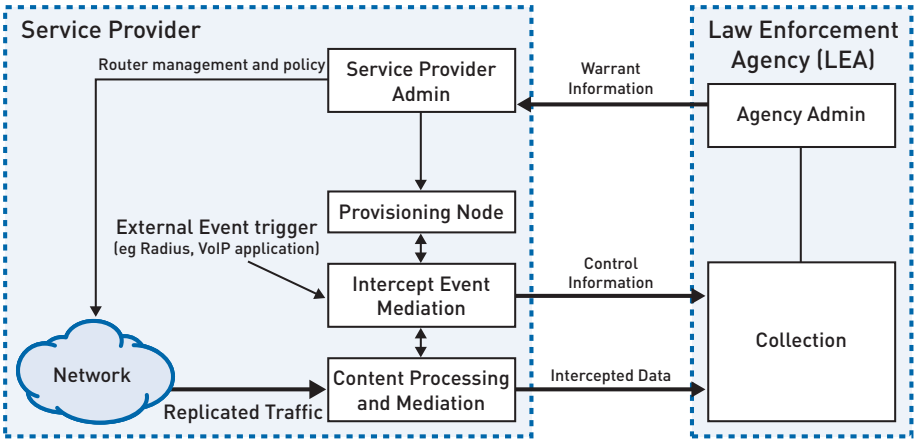

Figure 2.: Typical Architecture for Lawful Intercept

Comprehensive LI capabilities are already widely implemented in voice-centric, circuit-switched networks. But it's a different story with IP networks. LI has generally not kept up with the rapid growth of the Internet and the resulting rise in IP applications like email, Instant Messaging, voice over IP (VoIP), and peer-to-peer. This is the reason service providers need to be concerned. If they can't demonstrate the ability to enable LI for these applications, they can't comply with regulatory requirements. Figure 2 shows the typical architecture for LI.

Here's how the basic LI process works in a data network. If a law enforcement agency is interested in examining traffic from a specific source, it will identify that source according to various trigger criteria, from user name to IP address. This information is passed to the service provider as part of a warrant. The carrier uses filtering to isolate a flow from that source and replicate it to a mediation platform on the carrier premises, where it's safely sequestered from all other traffic. Processing involves application-layer analysis of the packet content before forwarding it to the law enforcement agency. This application-layer analysis is required, since most countries' regulations permit the agency to receive only the information that is relevant to their investigation – not all subscriber traffic. Application-layer processing enables service providers to zero in on specific content, whether Web traffic or email. The focus can be as specific as email directed to a certain recipient or email containing a specific keyword.

Finally, the mediation platform must present the intercepted traffic to the law enforcement agency in the format that it requires. The interfaces that handle this transaction are defined in regulatory standards. This traffic may include auxiliary frames with time stamps or reference codes, and may be encrypted in tunnels to the law enforcement agency's server. It is also worth noting that some of the hardware and operations involved can be outsourced to an authorized third-party provider.

The ability to zero in on the party under suspicion – also known as 'targeted efficiency' – is crucial. Targeted efficiency means that there's no need to examine all the traffic that passes through the router at the application layer, and flows from parties who are not suspected of anything remain completely private.

Challenges: The Current Approach to Intercept – Many Distributed Probes

Of course, putting an LI process into practice is somewhat more complex. In the LI approach most commonly used today, all traffic on links into the network backbone is replicated using either an optical splitter (also known as a "tap") or replication in an Ethernet switch. The splitter or switch sends the copied traffic to the content processing component of the mediation platform (sometimes called a "probe") at the service provider's premises. This probe is passive and does not participate in the production network. It filters packets and performs content processing before forwarding data to the mediation platform and the LEA.

One advantage of using passive monitoring probes is that it offers operational isolation. Remember, a service provider's operational staff typically requires access to routers. But when sensitive LI processes are handled by a passive probe, carriers can restrict access to those devices to a small subset of administrators, helping them comply with rules on limiting access to intercepts.

On the other hand, this passive-probe approach can add expense, if only because there's a separate box to buy and manage. Multiple probes are generally required as these devices are performing filtering and application-layer content processing – a demanding packet-processing task that restricts their ability to handle large amounts of data. This can require a complex architecture of probes distributed across the edge of the network. Finally, many passive probes are restricted in the number of interface and encapsulation protocols they can support.

Juniper Networks routers possess capabilities that can help service providers implement an LI architecture easily and cost effectively, without sacrificing performance or risking noncompliance. These capabilities are part of the J-Protect security toolkit, which includes a comprehensive set of features for safeguarding the service provider infrastructure as well as customer traffic. These include the fundamental components built into the router, like fine-grained filtering, rate limiting, and port or interface mirroring. There are also specialized tools, like service cards for network address translation (NAT), firewalls, and encryption. These features form a critical part of Juniper's Next Generation Network (NGN) infrastructure which support multiple services, many of which are under regulatory control for LI. NGNs must therefore have the ability to identify and replicate packets for LI analysis.

Trends

Lawful intercept has been part of the PSTN for a while, and the interception of call events and content are well established. However, as subscribers move away from the PSTN towards broadband IP networks, the requirements for Lawful Intercept have changed to cover IP traffic as well.

Since LI is a regulatory compliance and not a revenue generator for communication carriers, the Juniper LI solution is designed to provide carriers with the key components require to achieve compliance with LI regulations while incurring only minimal CAPEX and OPEX costs, and without impacting network traffic integrity or performance.

LI RULES AND REGULATIONS

In the United States, rules governing lawful intercept were established in 1994, when Congress enacted the Communications Assistance for Law Enforcement Act (CALEA). In 2001, the Patriot Act expanded these powers to allow interception of IP-based communications. In 2004, the FBI, the Department of Justice, and the Drug Enforcement Agency filed a petition with the FCC to clarify implementation of lawful intercept for broadband and VoIP service providers. Despite an appeal by some service providers seeking to delay the FCC requirements, in 2006 the FCC second report and order mandated that communication carriers to be CALEA compliant by May 14, 2007.

CALEA stipulates that law enforcement officials be given the authority and ability to retrieve and examine electronic communications. In addition, CALEA sets out mechanisms to protect this ability, even as telecommunications and networking technology evolves. The regulation applies to all carriers and is technologyneutral. It does not expand the authority of law enforcement to conduct electronic surveillance, and it limits the traffic that can be sent to law enforcement to what's authorized in the original request or warrant.

There are also rules for just how LI should work. The American National Standards Institute (ANSI) has laid out definitions for filtering, replication and mediation in an effort to standardize the architectural underpinnings of LI. Among the most important standard is ANSI/ JSTD- 025, which defines the interfaces between the service provider and lawenforcement agency. By implementing these standardized approaches, carriers receive "safe harbor" – meaning they are considered in compliance with CALEA requirements.

The U.S. isn't alone in implementing LI rules and regulations. Countries around the world are drafting and enacting laws outlining LI procedures, while standardization groups like the European Telecommunications Standards Institute (ETSI) are creating LI technology specifications.

Juniper Networks Advantages: Filtering and Replication in Routers

Juniper Networks offers service providers two basic options for implementing LI:

- Building an overlay of "passive" router infrastructure separate from the production network
- Using production routers in an "active" approach

Hybrid LI solutions, which use both options, are also possible. No matter which deployment option service providers choose, these approaches can reduce the costs associated with LI compliance.

The Passive Router Approach

The first option involves deploying Juniper Networks M Series Multiservice Edge Routers or T Series Core Routers in an overlay. These routers do not participate in the production networks routing and are therefore passive. This approach uses an optical splitter to siphon 10 to 50 percent of the signal to an active router port link. Unlike other products in their class, M Series and T Series router ports are declared "up" with only the receive side connected, and will accept the packet for internal processing.

Figure 3 shows the passive approach to LI, with an overlay of routers for filtering and replication. Only targeted traffic is forwarded for content processing in the mediation platform. This approach supports all SONET / SDH, Ethernet, Asynchronous Transfer Mode (ATM), and multiple encapsulations.

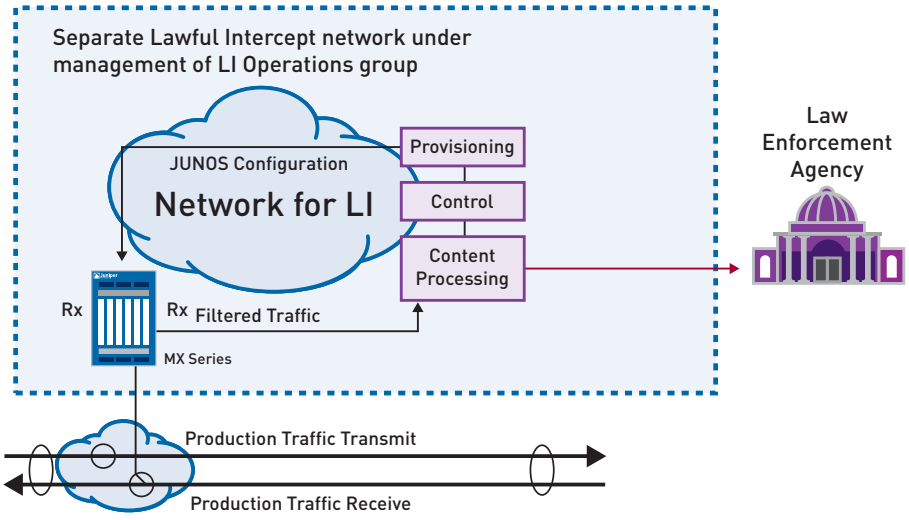

Figure 3: Passive Approach to Lawful Intercept

Using Juniper Networks routers in a passive approach, a wide range of interfaces is supported, up to and including backbone speeds of OC-48c/STM-16 and 10-Gbps OC-192c/STM-64. Passive approach routers support ATM interfaces as well as both Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC) on SONET/SDH links. Gigabit Ethernet interfaces can be placed in promiscuous mode to receive frames that other routers would silently ignore. The passive-router approach enables providers to monitor links between core routers from any alternate router vendor.

And these aren't the only advantages. Granular filtering can be applied at line rate to forward only the IP addresses under surveillance to the central application-layer content processing platform. This "first-stage filtering" in the router minimizes the number of expensive content processing platforms required.

Further, this approach offers complete operational separation from the production network, and isolation in the event of failure. In addition, because the overlay network receives a copy of all traffic, it can be leveraged to collect other network statistics such as summarized flow records for offline analysis in anomaly detection, traffic planning and accounting (see the section entitled Complementing LI with Flow Monitoring).

The Active Router Approach

Juniper's other approach to LI involves filtering and replicating traffic for analysis in core or edge routers, which are active routers in the production network. Figure 4 illustrates the active approach for filtering and replication in the production network router. This approach enables filtering and replication on any router interface, and for any encapsulation.

Typically, enabling functions like filtering and port mirroring on traditional routers negatively impact performance and affect the production traffic throughput and stability. But Juniper Networks filtering and replication through port mirroring allows data passing through Juniper Networks E Series Broadband Services Routers, M Series or T Series routers to be selectively copied for further analysis without performance penalties. It uses the same replication mechanism as multicast with no performance impact, and it provides a convenient means of copying data without additional hardware or software.

From each edge router, the replicated traffic may be forwarded over dedicated links to the mediation platform for content processing. Alternatively, traffic headed for the mediation platform can be forwarded via IPsec tunnels over the same link as production traffic.

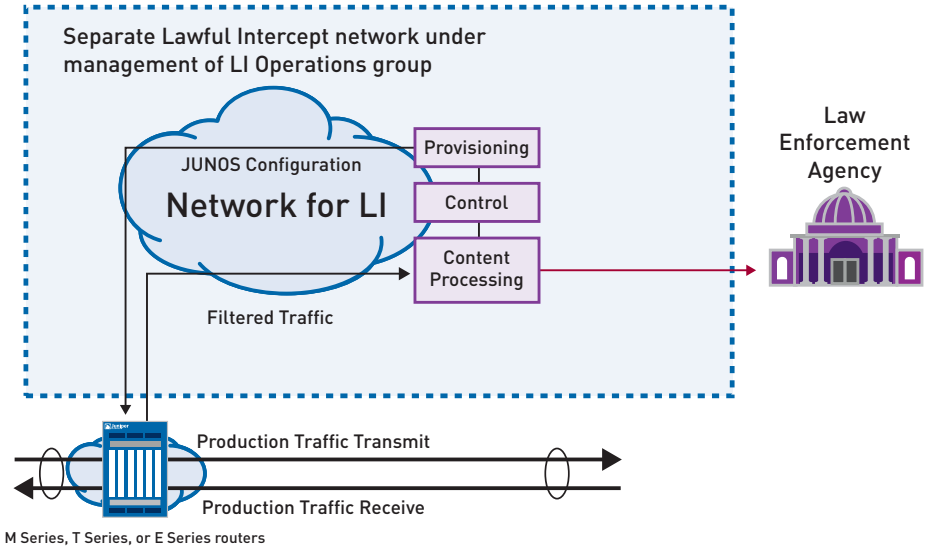

Figure 4: Active Approach for Filtering and Replication in the Production Network Router

This active monitoring approach offers several advantages. First, it eliminates the need for passive probes distributed across the network, and reduces the associated operations and administrative costs. Second, the filtering reduces the volume of traffic sent for content processing, which reduces capital expenditure on content processing platforms.

There is also a choice when it comes to identifying subscribers in the edge router of the broadband network. Three approaches are possible in the active edge router: Command line interface (CLI)-based IP interface mirroring, policy-based mirroring, and Dynamic Tasking Control Protocol (DTCP)-based filter criteria.

CLI-based IP Interface Mirroring

Traffic entering or exiting the M Series and T Series routers through a specified IP interface is filtered on IP header variables and then replicated by mirroring. This action can be configured dynamically by the provisioning component of third-party mediation systems. The mediation systems are given the target IP address through some external triggers – a warrant, an IP Telephony call server or a user authentication system, for example. This approach is useful in environments where a user typically logs on to the same edge router, or where mirroring needs to take place in core or peering routers. This type of filtering and mirroring has limited applications in Broadband Remote Access Server (B-RAS) environments, in which the users log in and log out frequently.

B-RAS routers are located at the edge of the service provider network, where they provide subscriber management and deliver advanced IP services per subscriber. Typically, the B-RAS receives the subscriber login credentials, authenticates the user against a RADIUS server, and assigns an IP address, enabling dynamic subscriber identification. This can mean that users have a different IP address each time they log into the network. Static IP filters aren't effective in identifying broadband users under surveillance, since they might be associated with different addresses at each login. That makes dynamic identification a necessity, so that when a subscriber logs in and is assigned an IP address, filtering and port mirroring are automatically activated to monitor that flow and forward it to the mediation platform. To address this need, Juniper Networks JUNOSe™ Software for the E Series B-RAS platform uses policy-based mirroring as a new approach to initiate filtering and replication for LI.

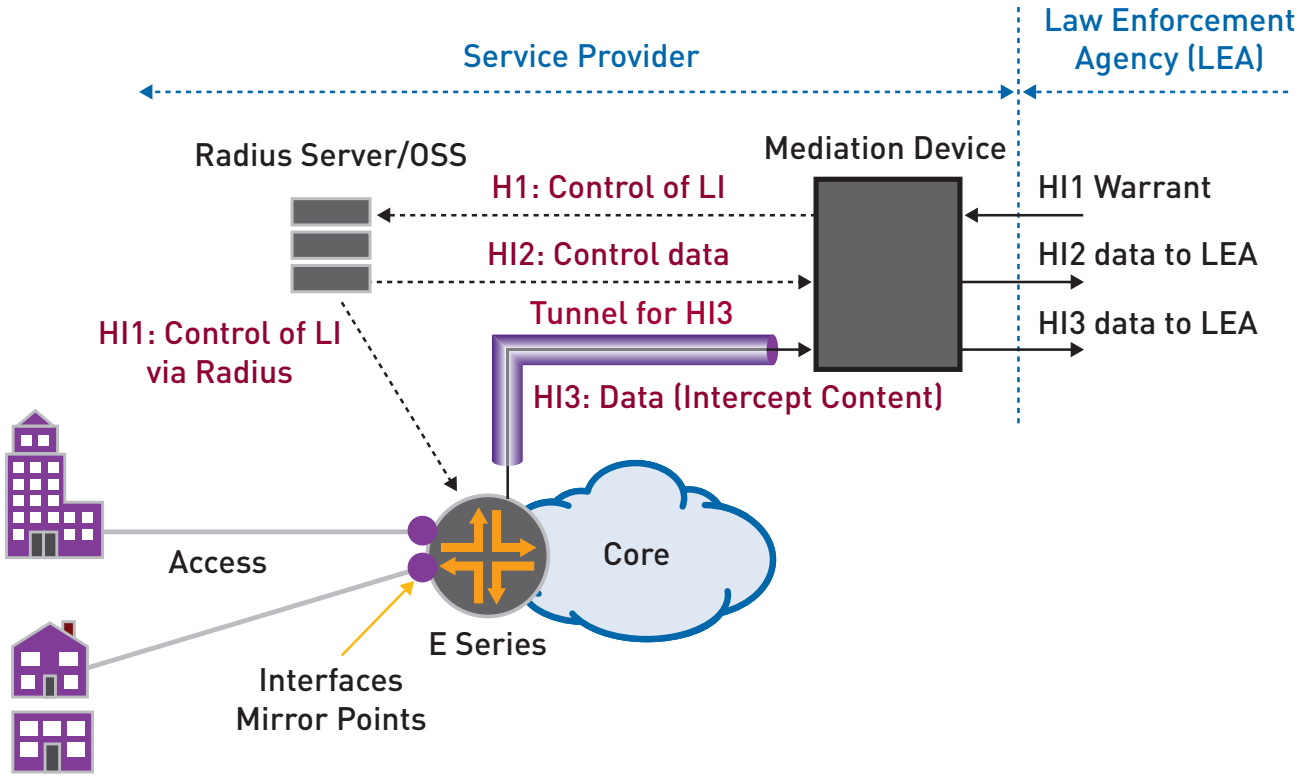

Figure 5: Reference Model for RADIUS-Initiated Lawful Intercept

Policy-based Mirroring

JUNOSe implements new "secure" policies. These secure policies trigger mirroring when needed, and can be applied via RADIUS, CLI, or Simple Network Management Protocol (SNMP). These triggers are persistent, and the LI configuration can be entered prior to user login. When the targeted user logs in, a user-initiated secure policy is applied in the E Series router to mirror the traffic. If the user is already logged in, a RADIUS-initiated secure policy is applied.

Within RADIUS, vendor-specific attributes (VSAs) are sent to the E Series B-RAS and used to create dynamic, secure policies for the mirroring of traffic from targeted subscribers (see Figure 5). Secure policy-based mirroring is an excellent solution for B-RAS networks that support a large number of dynamic interfaces.

Operational isolation of secure policies is built in, and secure policies allow only personnel with appropriate privilege to configure or display LI policy. Providers may assign higher level privileges to these commands and related information, limiting access to authorized personnel only. RADIUS-initiated mirroring is supported on IP and Layer 2 Tunneling Protocol (L2TP) interfaces.

Dynamic Tasking Control Protocol-based Filter Criteria

The Flow-Tap application in an active monitoring router provides the ability to intercept IP packets that match filter criteria and send a copy to one or more content destinations. Flow-Tap can be used for LI and also include flexible trend analysis for detection of new security threats. Filter criteria are specified using over SSH. DTCP supports operations to add, delete and list filters, among others. Each filter specifies unidirectional criteria, filters are applied for all IPv4 traffic through the router, and this operation does not add any perceptible delay in forwarding path. Filters are not persistent, and filters installed by one user are not visible to others. Flow-Tap provides a strong administrative model which includes access control via user classes.

Complementing LI with Flow Monitoring

Juniper Networks routers can create summarized records of unidirectional streams of packets transmitted from a source host to destination host. This process is known as "flow monitoring" and Juniper Networks implementation is termed J-Flow. Packets are classified as members of these traffic flows by source IP address, destination IP address, protocol type, source port number, destination port number, DSCP/type of service, and input router interface.

Juniper Networks J-Flow gives service providers the ability to collect packet-flow data and export it to an external device. The J-Flow records are based on industry standards, so records can be exported to third-party offline applications. These applications enable usage-based accounting, traffic profiling, traffic engineering, attack/intrusion detection and service-level agreement (SLA) monitoring. J-Flow can also be used to provide summary information to law enforcement agencies.

PERFORMANCE-ENABLING SERVICE AND SUPPORT

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains, faster rollouts of new business models and ventures, and greater market reach, while generating higher levels of customer satisfaction. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/products-services.**

All Juniper Networks router platforms operating in active mode can create J-Flow records as they forward production traffic. However, because flow analysis is packet processing-intensive, specialized flow monitoring service Physical Interface Cards (PICs) are used on the M Series and T Series routers to add the capacity needed for monitoring and analyzing greater numbers of flows. For maximum flow analysis capacity, multiple monitoring service PICs are combined in a passive router and added as an overlay on the production network (as described in the passive approach for LI). In both active and passive configurations, flow monitoring can take place alongside LI and port mirroring – without impacting performance.

The Role of Partners

Juniper routers enable architectures for LI that leverage router filtering and replication capabilities. However, this is only part of the total LI solution. Receiving warrants, authenticating and interpreting required actions, pushing configurations into the routers, and application-layer processing remain the responsibility of mediation platform vendors.

Juniper routers can replicate and forward standards-based IP traffic into mediation platforms from any vendor. Juniper Networks has also partnered with the leading mediation platform vendors to ensure interworking. This includes integration to offer solutions with automated configuration of the routers. Juniper also offers multiple methods for configuring platforms, including CLI, Extensible Markup Language (XML) and RADIUS-based messages.

Juniper Networks Solution Portfolio for Lawful Intercept

Juniper Networks has been working steadily with service providers to ensure they are prepared to meet LI requirements. Through both the E Series routers with JUNOSe Software and the M Series and T Series router product families running JUNOS, a full suite of features enables service providers to meet current LI requirements without any interruption of service.

For E Series routers, JUNOSe has a variety of internal capabilities designed to meet LI requirements. For example, JUNOSe only permits administrators with specialized clearance who are approved for CALEA configuration and monitoring to have access to provisioning and logging of LI transactions and events. This includes hiding the identity of the mirrored subscribers from general network operations staff, thus limiting the identity of mirrored subscribers to an extremely small group of people. To further ensure security, CLI commands dealing with LI do not appear on the network configuration screen without the use of a special command which can be very closely controlled and implemented remotely.

At the core of the network, using M Series and T Series routers, LI functionality can be achieved through the use of port mirroring, passive monitoring, or by active monitoring using Flow-Tap to intercept packets based on dynamic filtering criteria, which can be updated by service providers on a real-time basis without introducing any perceptible delay in forwarding traffic.

Summary – Juniper Networks Enables Low-Cost, Low-Impact Lawful Intercept Compliance

As countries around the world enact new laws concerning LI, carriers must be able to demonstrate that their networking equipment incorporates the functions necessary for regulatory compliance.

The current approach to LI requires that probes be distributed across the network. These probes perform filtering and content processing before forwarding targeted traffic to the mediation platform and law enforcement agency. This overlay has associated capital expenditure and operations overhead, which can be reduced by leveraging router infrastructure.

Traditional routers suffer from poor performance when they are required to filter and replicate traffic. However, Juniper Networks router platforms maintain performance with fine grained IP filtering of targeted subscribers and enabled replication.

Juniper Networks routers present new approaches to LI:

- The active approach uses production routers to filter and replicate only the intercepted subscriber's IP traffic to the content processing function of the mediation platform. This is ideal when customers are directly connected to an edge router or B-RAS.
- The passive approach uses an overlay of routers. Generally, traffic is optically split into the passive router, where it is filtered, and only the intercepted subscriber IP traffic is forwarded to the content processing function of the mediation platform. This approach particularly suits LI of high-speed backbone links or of production networks built from non-Juniper Networks routers.
- Juniper Networks LI solution forwards standards-based traffic into mediation platforms from any vendor. Additional interworking is possible with Juniper Networks mediation partners.

The Juniper Networks LI solution offers service providers a choice of deployment options that not only comply with regulatory standards but can also greatly reduce the cost of LI implementation.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net.**

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

1600011-001-EN Apr 2009