1/10/40/100G Safe Harbor Probe

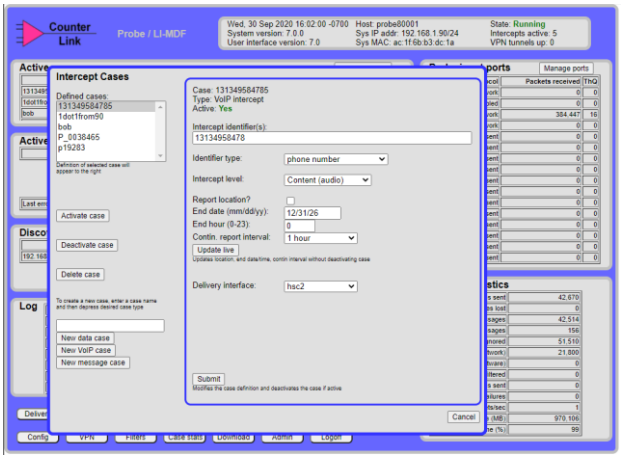
The latest technology for a self-contained lawful-intercept compliance solution for Internet access providers, fixed and airborne Wi-Fi systems, VoIP providers, LTE operators

KEY FEATURES & BENEFITS

- In use at ~100 service providers
- Supports ATIS, 3GPP, ETSI lawful-intercept standards
- Full IPv6 support
- Maximum of four 100G or 40G inputs, 16 10G inputs
- Modularity allows combinations of 1, 10, 40, and 100G inputs
- Integrated provisioning requires no separate mediation or administrative system
- Integrated VPN reduces installation complexity
- Email alerts and notifications
- Buffering options selectable for each intercept
- Can operate alone or control separate VETaps™ or "subprobes"
- Virtualized version can operate in cloud infrastructure environments

The Safe Harbor Probe is an easy-to-install, self-contained system that provides interception, administration, and VPN security — all in one device. As an out-of-line passive device, the probe can be connected to many different points in the network. These points can be network taps or span/mirror ports, or intelligent POIs (points of interception) called VETaps. Because the probe examines network traffic, it is independent of the specific equipment used in the network. Deep-packet inspection capabilities enable the probe to take special actions for certain protocols, such as DHCP, RADIUS, GTP, SIP and RTP. The probe can discover and track dynamic IP assignments.

Intercepts are configured or provisioned in the probe through a secure web-browser interface.



Data Intercepts: The Safe Harbor Probe provides for data intercepts on broadband, LTE, and UMTS networks. A wide range of identifiers can be provisioned for a target, including

- IPv4 static address or subnet
- IPv6 static address or prefixed
- DHCP identifiers (MAC address, client identifier, client name, option 82)
- RADIUS identifiers (user name, calling station ID, NAS port)
- MSISDN, IMSI, IMEI
- S-VLAN and C-VLAN tags

Case-by-case, the intercept can be specified as a pen-register intercept or full content intercept, with optional location reporting. For LTE, the probe can be connected to the S5 interface, or alternatively the S11 and SGi interfaces. Also, because courts often require "service separation," meaning that VoLTE/VoIP cannot be included in a data intercept, the Probe has optional filtering functions to remove VoIP signaling and content from a data intercept.

VoIP Intercepts: Without reliance on any other network equipment, the Safe Harbor Probe provides complete SIP/RTP VoIP intercepts. The identifiers that can be provisioned for a VoIP intercept include:

- Phone numbers, including partial or wild-carded phone numbers

- URIs
- MSISDN, IMSI, IMEI

As it listens to SIP traffic, the probe looks for the provisioned identifiers in a number of possible places, such as To/From/Contact/P-Asserted-Identity headers. Options, which are typically specified in the court order, include DTMF (dialed digits) reporting and location reporting. Options exist to ask the probe to detect and remove duplicate calls.

Standards: For data intercepts, including LTE, the probe can be provisioned to generate the ATIS IAS V2 CALEA standard. Alternatively, ETSI 102 232-3 can be used and, for LTE, the 3GPP 33.108 standard can be selected. For VoIP, the probe uses the ATIS 678 V3 and ETSI 102 232-5 standards. Optionally, prior versions of these standards can also be specified. The probe supports the optional features of the standards embraced by law enforcement, such as surveillance start, stop, and continuation messages. The probe also supports, in conjunction with the above, the ATIS-1000069 standard, which allows the probe to report conditions such as failed delivery interface, input interface down, lost output, dropped input, and others to the collection system(s).

Special Input Situations. In addition to listening for normal IP over Ethernet packets, possibly with VLAN and MPLS tags, the probe can deal with GTP-tunneled packets, can serve as an ERSPAN destination, can terminate Ethernet over GRE, can interpret proxied HTTP traffic, and can reassemble fragmented SIP.

Input Speeds. The probe as a physical appliance has two slots for input modules. Modules supplied are:

- 100G with two QSFP28 inputs
- 40G with two QSFP+ inputs
- 10G with eight inputs*
- 10G with four SFP+ inputs
- 1G with four inputs

The first four use specialized ASIC chips to filter traffic at wire speed. The 8x10G module uses two QSFP+ 40G ports that are internally configured to 4x10G behavior; a 4X cable to four SFP+'s or LC connectors is used.

Performance. The 100G, 40G, and 10G interfaces watch traffic at wire-speed rate. 1G inputs support 1 Gbps of typical Internet mix for data intercepts and 200 Mbps for RTP (VoIP media).

The maximum rate for intercepted traffic depends on a number of factors, such as whether the intercept is pen register or full content and whether content filtering (discussed below) is used. Ultimately the rate is determined by the maximum speed at which the probe can send to a law-enforcement collection system. The maximum delivery rate is about 1 Gbps on a 1G interface and 5.5 Gbps on a 10G interface.

Capacity. The current ASIC modules being used limit the number of active data-intercept cases to 32 (although multiple cases based on the same intercept identifier count as one). The maximum number of VoIP intercepts (cases) is 256. In the situation of VoIP content intercepts, there is a limit of 15 concurrent calls that are being intercepted.

Email Alerts and Notifications: The probe can be provisioned to send periodic reports to designated email addresses, including overall status reports (e.g., to operational personnel), and intercept-case-specific reports to law enforcement. Additionally, certain events (e.g., delivery error, disk capability, VoIP call start) can be selected to trigger email messages.

Delivery: The Safe Harbor Probe contains a variety of mechanisms to maximize the robustness of the intercept delivery. One of these, buffering, prevents the loss of intercept information if anything fails on the upstream path. The buffering implemented in the probe is called "transparent buffering" in that the file structure used is not visible outside the probe and thus this can be used with any law-enforcement collection system. Nominally, 1 TB of RAID-1 disk space is provided for buffering.

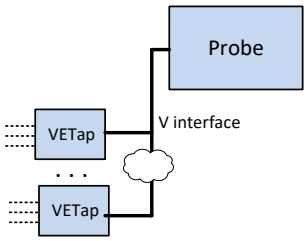
The probe integrates a site-to-site VPN capability, eliminating the need for a separate VPN appliance. The VPN is provisioned through the probe's web-browser-based interface.

Security: The probe has two interfaces, both of which are highly protected – the provisioning interface and the delivery interface. The firewall function permits access to only a few services, and permits access from only a certain set of IP addresses. A specific client certificate is required to access the TLS-based provisioning interface. The delivery interface is typically protected using the built-in VPN capability. Certain information within the probe is encrypted, such as buffer files and the probe's database.

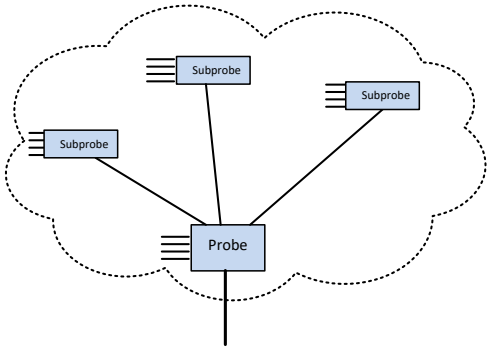
The probe is significantly more secure than an "active" lawful-intercept approach because it doesn't rely on controlling, and getting data back from, the LI features in the other equipment in the network, and thus is better protected from insider attacks.

Filtering: The probe provides an array of filtering capabilities to reduce the output traffic to law enforcement, should the court order allow for this. The probe can filter on specific VLAN tags and can filter out specified IP address and port combinations. It also uses an extendible rules-based file to filter out specific services, such as Netflix, YouTube, Amazon Prime, Hulu, and others.

VETap™ and Subprobe Control: The probe can also control an arbitrary number of remote points of interception, which are based on the VETap (virtual Ethernet tap) technology. The VETap is a software product that can be placed in a separate physical or virtual machine to act as an intelligent surrogate for the probe.



A VETap can also be placed in a separate dedicated hardware system, in which case this hardware system is known as a "subprobe." This allows the probe to distribute its reach, even to remote locations. The interface between VETaps/subprobes and the probe uses reliable TCP transport and end-end encryption, allowing this remote connectivity.



POI Maps. A further optional capability related to the above is the ability to define POI (points of interception) maps. Nominally, when an intercept is activated, it is communicated to all POIs. The POI map is a way to override this behavior by designating that only specific POIs or subsets of POIs are to receive target information for specific intercept cases.

Virtual Probe. When a service that needs to comply with lawful-interception laws moves into a cloud-provider virtual environment such Amazon Web Services (AWS), a different approach of listening to traffic is needed. This Is provided by the combination of running the probe as a virtual machine, and using VETaps to listen to network traffic on other virtual machines. In AWS, for instance, the probe may be run In the same virtual private cloud (VPC) as the virtual machines containing the VETaps, or In a separate VPC connected via an Amazon peering connection.

High Availability: A pair of physical or virtual probes can be configured as an active/standby pair. The standby probe monitors the state of the active probe and can, automatically or manually, instantly become the active probe.

Miscellaneous Functions: The probe also has a set of functions to assist with installation and troubleshooting, such as

- Statistics and log viewing pages
- Reports on "satellite" controllers – subprobes/VETaps and ERSPAN routers
- Ability to receive input from a pcap file rather than the actual network interfaces
- Ability to generate a pcap file showing the Ethernet frames it is ignoring

Safe Harbor Probe Physical and Electrical Characteristics

- 1U, 16.9" deep
- Approximately 16 lbs
- Operating temperature: 10-35ºC
- One 1G system port
- Two to 16 input ports, depending on speeds selected
- Max input rate: 400Gbps
- AC power. Base unit is ~150W max. Each 10G and 40G module adds ~30W max. Each 100G module adds ~60W max. Each QSFP+/QSFP28 transceiver adds ~4W.
- Remote management via BMC/IPMI