Counter Link Safe Harbor Probe

The latest technology for a self-contained lawful-intercept compliance solution for Internet access providers, VoIP providers, fixed, airborne, and satellite-based communications systems, and multi-tenant Wi-Fi systems

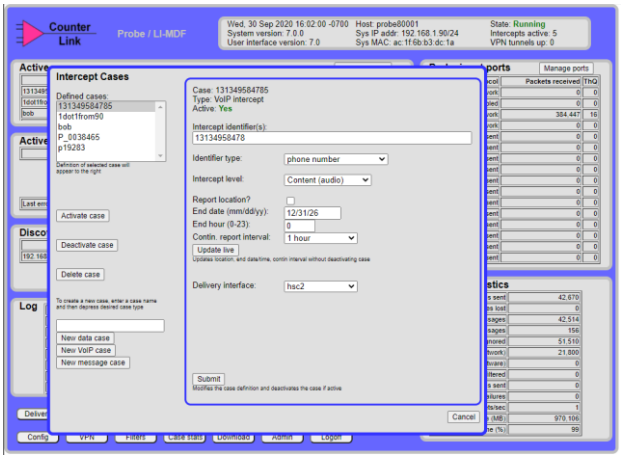
KEY FEATURES & BENEFITS

- In use at over 100 service providers
- Supports speeds up to 200G
- Supports ATIS, 3GPP, ETSI lawful-intercept standards
- Full IPv6 support
- Integrated provisioning requires no separate mediation or administrative system
- Supports tunneled inputs, such as GRE, VXLAN, ERSPAN, EoMPLS, HEP3, Geneve
- Content filtering can bypass streamed content (e.g., Netflix, YouTube, …)
- Integrated VPN reduces installation complexity
- Email alerts and notifications
- Buffering options selectable for each intercept
- Can operate alone or control separate VETaps™ or "subprobes"
- Can operate in cloud and virtual-machine environments

The Safe Harbor Probe is an easy-to-install, self-contained system that provides interception, administration, and VPN and TLS 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, RTP, RCS, SMS/MMS. 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 wireless infrastructure, the probe can be connected to the S5, S11, SGI, and S6a 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, MEI

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.

RCS Intercepts: The probe provides interception of RCS messaging. Options are MSRP headers only, entire MSRP payload, and file objects. The latter can be selectively intercepted based on size.

Standards: For data intercepts, the probe can be provisioned to generate the ATIS IAS V2 CALEA standard. Alternatively, ETSI 102 232-3 and 3GPP 33.108 can be used. For VoIP, the probe uses the ATIS 678 V4 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, VXLAN, HEP3, and Geneve destination, can terminate Ethernet over GRE and EoMPLS, and can reassemble fragmented SIP.

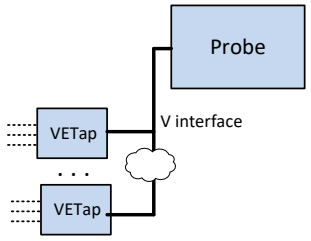
Performance. When used with an Nvidia ConnectX NIC, the probe can support wire-speed inputs of 10G, 25G, … up to 200G. It does this by using the chip's TCAM to block all traffic except for the current intercept identifiers (e.g., IP address, RTP endpoint) placed in the TCAM. The maximum output rate for 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.

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. The probe integrates a site-to-site VPN capability, eliminating the need for a separate VPN appliance. Alternatively, the probe can deliver using TLS.

Filtering: The probe provides an array of filtering capabilities to reduce the output traffic to law enforcement. 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™ Control: The probe can control an arbitrary number of remote points of interception, which are based on the VETap 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. The VETap is especially useful in cloud VM environments, such as AWS.



Security: The probe uses TLS over TCP to protect the provisioning, delivery, and VETap interfaces. 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 in that 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.

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.