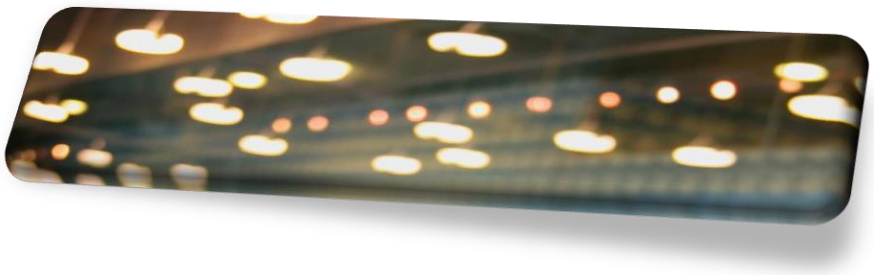
10/40/100G Subprobe

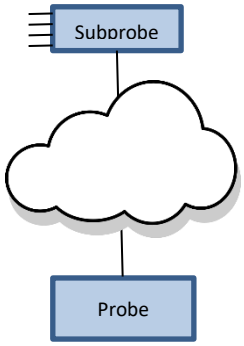


The latest technology in distributed interception for CALEA compliance

KEY FEATURES & BENEFITS

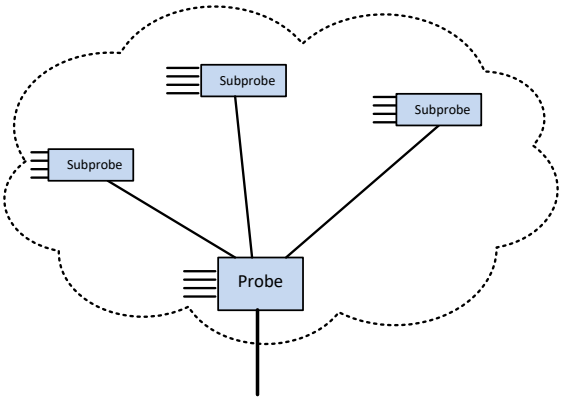
- Provides the means to intercept remotely networks that have expanded to 10G, 40G, or 100G
- Can be a more-economical solution than a full probe
- In a larger network that may be spread geographically, provides intercept access points that tie into a central probe
- Full support of VoIP and data intercepts
- Full IPv6 support
- Optional end-end encryption between subprobe(s) and probe eliminates the need for VPNs

The St. Helens Subprobe is a device that operates on behalf of a St. Helens Probe, which may be in the same network or completely outside. One usage is the model below. Here, instead of deploying a probe in a service-provider's network, the subprobe is deployed instead, and the subprobe runs under the control of a remote probe. The remote probe might be a physical probe, or a virtual-machine version of the probe running in a cloud environment such as Amazon Web Services.

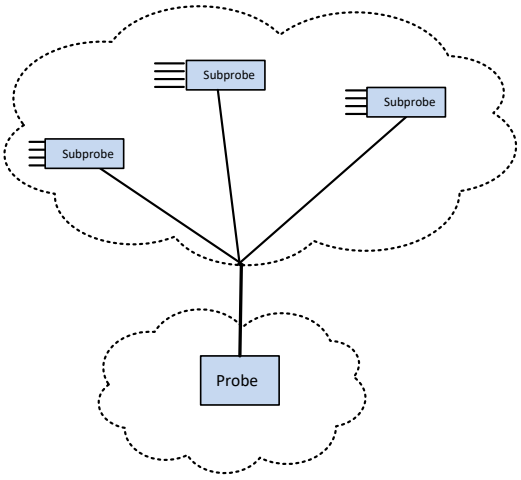


The benefit of this approach is that the subprobe is a simpler and less-expensive device. Everything that a probe can do, the probe can do remotely with the subprobe.

A different use of the subprobe is shown in the next figure. Here there is a need to deploy a probe in the service-provider's network, but the number of points in the network that need to be seen by the probe is either larger than one probe can handle, or geographically dispersed, or both. Thus the solution is to deploy both a probe and some number of subprobes.



To a user of the probe, the subprobes are generally invisible; the probe determines what it needs to access for the intercepts that are provisioned, and then, if the probe sees that subprobes are connected, it uses these subprobes to participate in the intercepts. If it is not necessary for the probe to have direct inputs itself, the Probe could be located remotely, as shown below.



Virtual Ethernet Tap

The subprobe consists of two critical pieces of software: software that directly controls the 10G hardware and thus bypasses the underlying Linux operating system to read packets, and the Virtual Ethernet Tap™ or VETap™, which operates under the direction of the probe. The VETap contains filters provided to it by the probe. For instance, if the service is a VoIP service, when an intercept is activated on the probe, the probe might instruct the VETaps to deliver all SIP traffic seen, or all SIP traffic matching a particular identifier, and nothing else. If a call occurs involving an intercept

target, the probe will determine the information needed to locate the RTP packets and broadcast these to the VETaps.

Subprobe inputs. Typically the subprobe is fed from network taps. It can also be fed from a mirror/span port if the load on the router or switch containing the port is low. The basic configuration is four 10G inputs and one 1G input. Optionally, the subprobe can have a combination of 10, 40, and 100G inputs (maximum of 16 10G inputs, four 40G or 100G inputs).

Subprobe/Probe Traffic. Traffic between the probe and the VETaps in the subprobes consists of commands sent from the probe, statistics and other state information sent to the probe, and captured packets sent to the probe.

Security. Communication between probe and subprobe occurs over one transport port, and firewall rules in the subprobe limit communications to this single port. End-to-end encryption is provided, which secures the traffic without requiring VPN appliances. For troubleshooting and maintenance, remote Linux access can be provided, but this traffic is encrypted and requires a private key to be initiated.

Statistics and logs. The subprobe maintains a set of statistics on its behavior, and also a log of significant events (e.g., being enabled, being given a filter, encountering an error). These statistics and logs can be requested by the probe and are viewable in the user interface of the probe.

Performance: The subprobe usually talks with the probe over a 1G interface, and can send captured packets to the probe at a 1 Gb/s rate. Optionally, a 10G interface between subprobe and probe can be used.

Subprobe 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