

## eTAP 20G with directly attached Monitoring Tools

The eTAP 20G transparently monitors critical network links in 10Gb/s networks and datacenters and selectively replicates application and network traffic to monitoring tools locally connected to two (2) 10G or two (2) 1G monitoring tools as illustrated below in Figure 1.

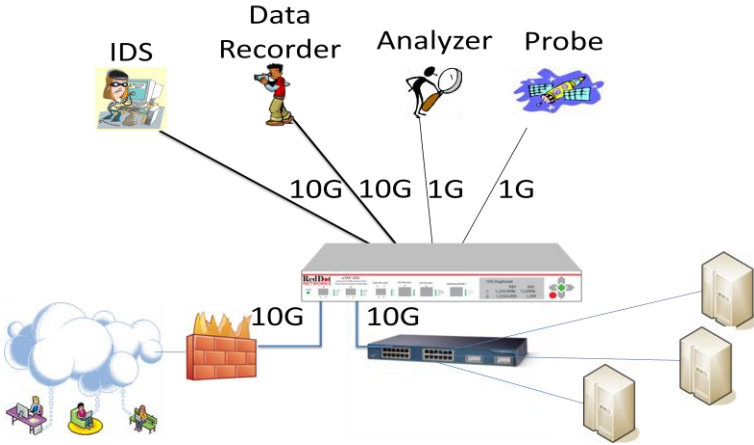


Figure 1 – eTAP 20G with locally attached tools

## eTAP 20G with remotely connected Monitoring Tools

For 10Gb/s networks and data centers which may not have all the monitoring tools locally attached to their critical links, the eTAP 20G provides a Remote TAP feature which tunnels selectively replicated traffic, using UDP encapsulation, out one or both 1G monitoring ports to monitoring tools over the Internet or private IP network as illustrated below in Figure 2.

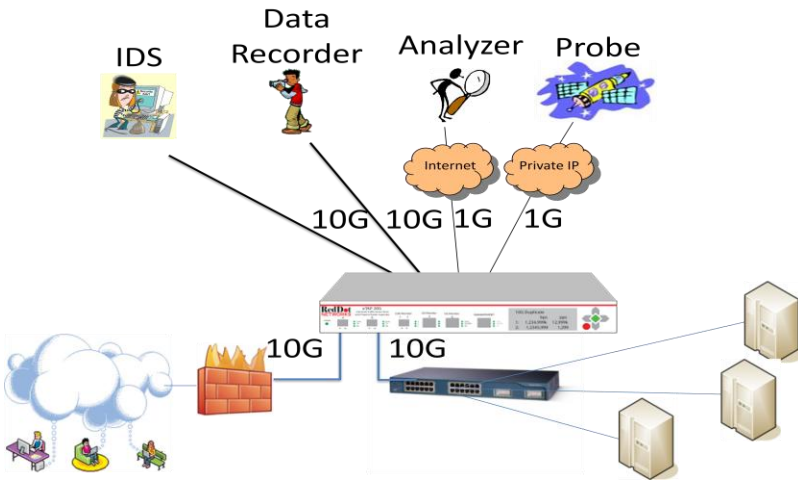


Figure 2 – eTAP 20G with UDP Tunneling to Remote Tools

## eTAP 20G Configuration

The eTAP 20G has the ability to transmit packets remotely via UDP (remotely forward) to configurable destination IP addresses and destination ports corresponding to remote monitoring tools or to RedDot Networks cdump utility which receives UDP packets from the eTAP 20G and stores them as PCAP files.

To facilitate remote forwarding, the eTAP 20G inserts an Ethernet->IP->UDP header (along with Packet ID, Packet Size, TAG and Timestamp fields) and a recalculated CRC to the original packet. A total of 56 bytes is added to the original packet. See Figure 3 below.

BYTE	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	ENCAPSULATION HEADER: ETHERNET, IP, UDP															
16																
32											PKT ID	PKT SIZE	TAG			
64	TIMESTAMP															
...	ORIGINAL PACKET															
END													ENCAPSULATION CRC			

Figure 3 – Encapsulation of Original Packet

The Packet ID, Packet Size, TAG and Timestamp fields are defined in Table 1 on the back side of this page. To configure monitor ports 3 and/or 4 for tunneling, the following steps are required:

- 1) Set port for UDP encapsulation mode.
- 2) Set MTU size.
- 3) Set the source MAC address, IP address and UDP port number.
- 4) Set the destination MAC address, IP address and UDP port number.
- 5) Optionally set rate limiting for the tunneled traffic to 100 Kb/s, 1Mb/s, 10Mb/s or 100 Mb/s to prevent overwhelming the Private IP or Internet connection.

## cDump Configuration

Available for Windows 32 bit, Linux and FreeBSD, cDump runs on a client machine that is set-up as the destination for the UDP encapsulated tunneled packets (udp mode) or is directly connected to one of RedDot Networks output ports configured to output time stamped and truncated packets (raw-t-p mode). cDump is a utility that creates a listening port(s) on the client machine for receiving packets from RedDot Networks devices. It also normalizes the data stream into a standard PCAP file format and creates file or files based on option settings. Alternatively, the normalized output can be sent to “stdout” where it can be piped directly to a local or remote monitoring tool (e.g. Wireshark).

There are several advantages to cDump utility:

- 1) **Accurate and synchronized time stamping of replicated traffic.** The eTAP 20G is synchronized based on NTP or GPS clocking and use this precise timing to timestamp the packets when they are first seen on the ingress to the eTAP not the remote tool. Whether the replicated traffic is locally captured or being sent to remote capture device, the timestamp is based on a standard universal clock and not on the capture devices clock. Micro-second latency measurements can be made easily with a monitoring tool located anywhere.
- 2) **Centralized or remote repository for replicated traffic.** cDump option flags allow for the creation and storage of replicated traffic for archiving. The flag settings can be set to capture traffic or create a PCAP file of a user defined size and then automatically close that file when it reaches the defined size and create a new one with an incremental number in the file name. This allows for the creation and management of traffic captures of correct sizing for later playback, unique naming and archival.
- 3) **Remote capture.** When the eTAP 20G is configured to replicate traffic into a UDP encapsulated tunnel for forwarding to a remote capture device over a routed network (e.g. Private Network or Internet), the replicated traffic can be stored as a PCAP file or it can be “piped” to a sniffer utility like Wireshark as an example. This has many uses as it permits an engineer to configure the eTAP 20G to forward very specific traffic types to where she is whether it is at her desk or home, The alternative would require the engineer and tool to at the network operations or data center.

Field	Size (bytes)	Description
ETHERNET	14	Ethernet dst, src, and type.
IP	20	IP src and dst addresses.
UDP	8	UDP src and dst ports.
PACKET ID	2	16 bit sequential number of the original packet. If the original packet is segmented, the same packet ID is used for all segments of that packet.
ORIGINAL PACKET SIZE	2	Size of the original packet, including the 4-byte CRC (sometimes called FCS).
TAG	2	TAG[15:11] contains the SEGMENT ID. If the original packet is segmented, each segment will have incrementing SEGMENT ID, where the first SEGMENT ID is 0. Access SEGMENT ID with ((TAG >> 11) & 0x1F).  TAG[1] is used to encode the port the packet was received on. 0 = received on port A, 1 = received on port B. Access the port with ((TAG >> 1) & 0x1).  TAG[0], and TAG[10:2] are reserved.
TIMESTAMP	4	4-byte timestamp, with the least significant byte first as used by networks. In other words, if this field is 01 02 03 04, the actual timestamp is 0x04030201 microseconds.
ORIGINAL PACKET	X	Original packet, including original CRC.
NEW CRC (FCS)	4	The packet has a new CRC attached to the end as required by the Ethernet protocol.

**Table 1 – Encapsulated Packet Field Size and Description**

## Conclusion

The eTAP 20G allows organization to Pre-Instrument 10G network and data centers. Monitoring tools can be directly connected to the eTAP 20G or remotely connected via a Private Network or Internet connection. The end result is 100% Application and Network Visibility even when an engineer or monitoring tool is not physically present at the network operations or data center.

