

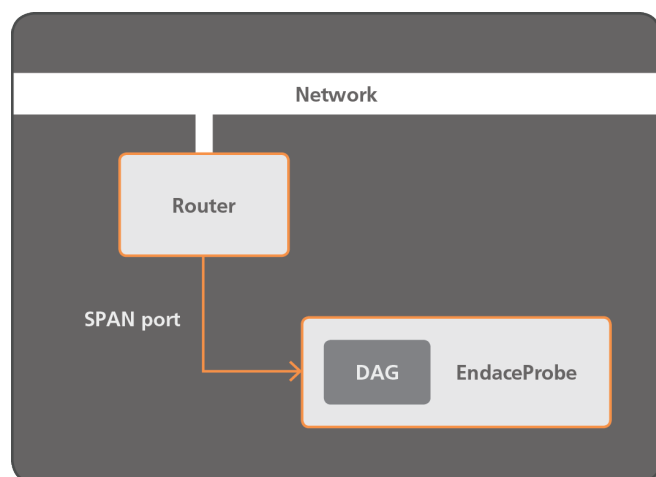
## Implementing Passive Tap Points for EndaceProbes

This document describes industry best practices for implementing network taps.<sup>1</sup>

There are two network tapping scenarios: passive and active. This document deals specifically with passive scenarios.

Passive tapping is transparent to network traffic, and is the preferred approach for cyber security monitoring and low latency monitoring. Historically, router and switch SPAN ports have been used to replicate traffic and direct it to particular applications.

SPAN ports have proven to be useful for monitoring at low speed. However, as network speeds and traffic loads have increased, SPAN ports have ceased to be an effective solution due to the increased load placed on the router, and so dedicated network taps are now highly recommended.



### Tap Basics

Taps typically have two types of ports: tap-ports and monitoring-ports. The tap's tap-ports connect to the network link and the monitoring-ports connect to the EndaceProbe. To work, the media type of the tap's tap-port must match the

media type of the link being monitored and the media type of the EndaceProbe's monitoring-port.

All EndaceProbes are equipped with modular SFP or XFP monitoring-ports. Some taps are fixed media, while others use modular SFP or XFP interfaces, so it's important to buy the right sort of tap. Endace recommends the use of modular media tap in all but the most homogeneous and static network monitoring deployments.

Using multi-mode fiber between the tap and the EndaceProbe is typically the lowest cost approach, but it's important to recognize that multi-mode connector loss and optical attenuation per meter is higher than single mode fiber. It's possible that optical power budgets will need to be checked, especially for long tap-to-EndaceProbe links.

For tapping fiber links there are other media-related issues to consider:

- Match the fiber diameter of the tap-port to the fiber diameter of the link
- Optical taps are directional, so be sure to connect the transmit side of the fiber link to the tap's receive tap-port, and the receive side of the fibre link to the tap's transmit tap-port.

### Monitoring bidirectional links

When tapping a bidirectional link, the potential bandwidth on the monitoring-port is twice the rated bandwidth of the link. To tap a bidirectional GE link you need 2Gb/s of monitoring-port bandwidth. You must therefore either use two GE ports on the EndaceProbe, or use an aggregation tap to combine the traffic onto a single 10GE monitoring-port.

Aggregation taps combine traffic from both directions of the monitored link and merge the traffic onto a single monitoring-port.

Aggregation taps have a number of important shortcomings that need to be understood.

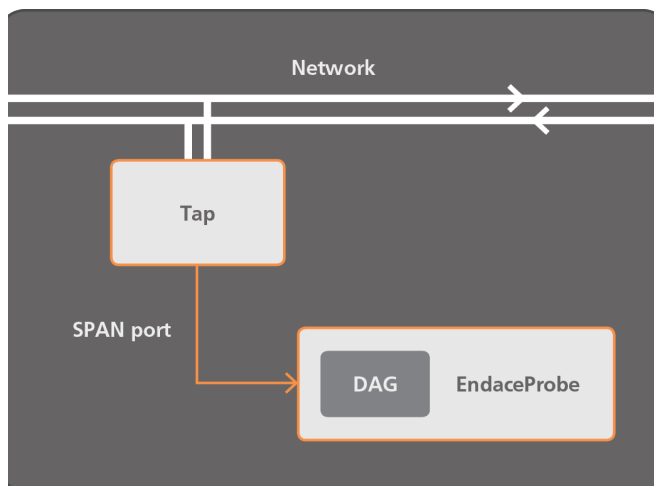
<sup>1</sup>The monitoring-ports on all EndaceProbes™ are based on the Endace DAG® card. Therefore, this application note is suitable as a guide for deploying network taps for any DAG card-based equipment.

- Even if average network load means the link is less than 50% utilized in both directions, bursts of activity can overload the aggregation tap's monitoring-port and lead to packet loss.
- Packet direction is lost once aggregation occurs. This isn't an issue under normal conditions because information such as MAC or IP address indicates which endpoint created the packet and thus which direction it was going. However, cyber security monitoring applications will certainly want to see any packets (particularly malformed packets) traveling in the wrong direction.
- During aggregation, packet misordering is possible. Packet misordering occurs when packets arrive almost simultaneously from both directions
- Aggregation can impact packet timestamping. As packets are sent onto the monitoring-port, large packets arriving on one tap-port will always delay packets arriving simultaneously from the other tap-port. Low latency monitoring tools require the most accurate time-stamping possible and thus should not be used in conjunction with aggregation taps.

### Scenario #1: Monitoring a single bidirectional link with a single EndaceProbe

The most basic form of passive tapping consists of a simple tap inserted into a single network link and connected to a single EndaceProbe.

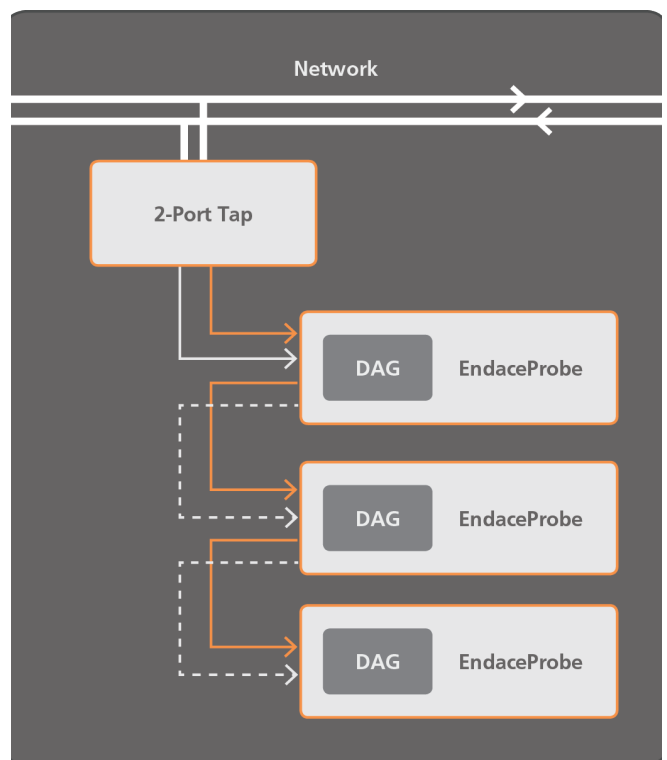
In this scenario Endace recommends the use of two monitoring-ports for each link rather than using an



aggregation tap. Installation planning consists mainly of matching media types, selecting appropriate splitter ratio to meet optical budgets, and ensuring the tap-ports are installed in the right direction.

### Scenario #2: Monitoring a single bidirectional link with multiple EndaceProbes

There are situations in which highly specialized or custom-developed monitoring tools need to co-exist with commercial tools, which means deploying multiple EndaceProbes at a single point. There are three techniques that enable multiple EndaceProbes to monitor a single link: replicator taps, physical layer daisy-chaining, and active forwarding.



#### Replicator Taps

Also called regeneration taps, these take each packet received on the tap-ports and replicate the packet N times, once for each of the N monitoring-ports. Simple replicator taps replicate all received traffic to all monitoring-ports. It is equivalent to, but much simpler than, taping the link N times



using N standard taps. More sophisticated replicator taps are capable of replication, aggregation and traffic filtering.

### Daisy-chaining

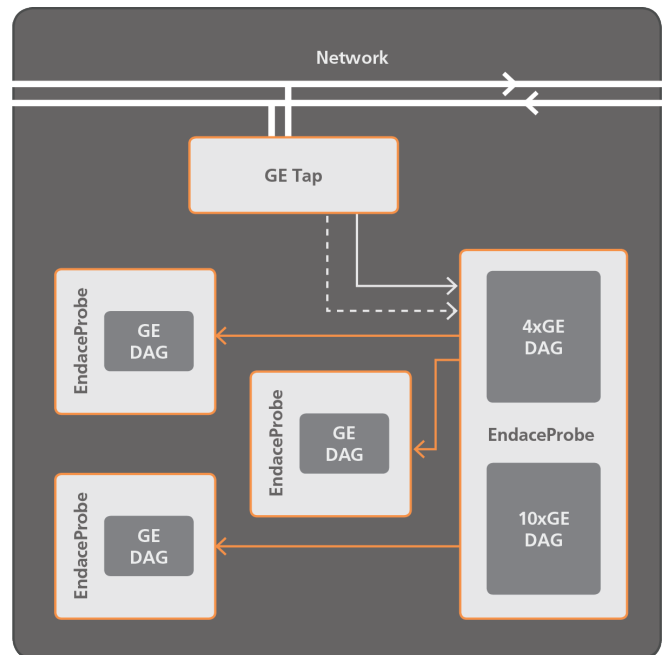
This is an option available on the monitoring-ports of most EndaceProbes. The EndaceProbe is configured such that all traffic received on the Rx side of a monitoring-port is duplicated in hardware and transmitted on the Tx side of that same monitoring-port. Because the duplication is in the monitoring-port hardware this functionality places no load on the EndaceProbe's CPU and introduces very little delay. To allow multiple EndaceProbes to capture the same traffic, all but the last EndaceProbe in the chain forward all traffic to the next EndaceProbe, as shown in the figure.

### Forwarding

This is an option available on EndaceProbes that run OSm (Endace's Operating System for Monitoring). It is similar to daisy-chaining except the traffic replication is done at the software layer of the EndaceProbe rather than at the hardware level.

### Scenario #3: Monitoring multiple links with a single EndaceProbe

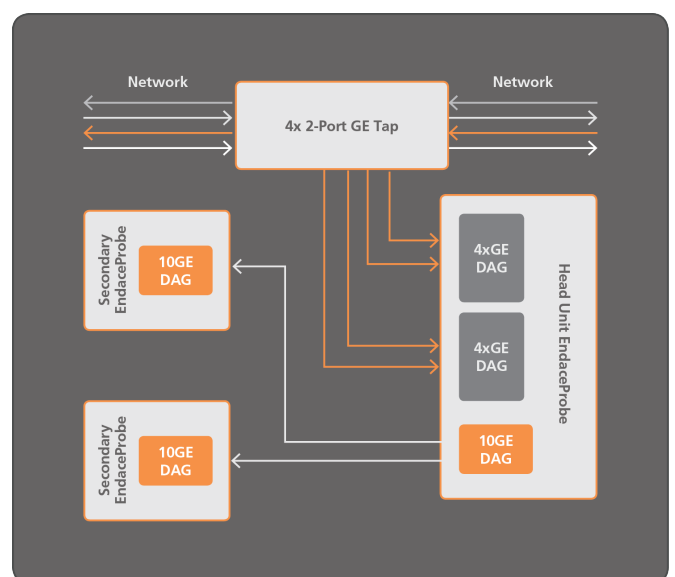
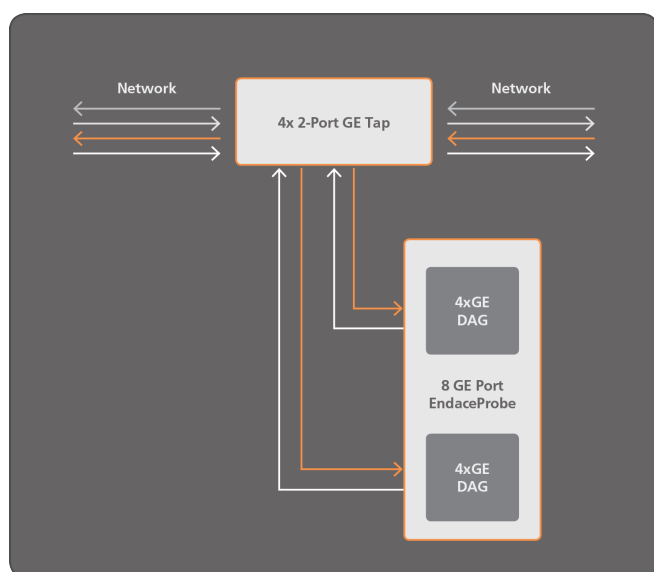
Endace does not recommend using an aggregation tap to combine traffic from multiple links onto single or dual monitoring-ports. Instead, Endace recommends selecting an EndaceProbe with sufficient monitoring ports (two per link) to directly monitor all the traffic from all links simultaneously. For example, EndaceProbes with up to 20 GE monitoring ports are available and can monitor 10 bidirectional links simultaneously.



### Scenario #4: Monitoring multiple links with multiple EndaceProbes

In most respects this configuration is simply a more complex version of case #2. It is, however, the most likely scenario where the forwarding configuration discussed previously will be an optimal solution.

In this case the head-unit receives all traffic from all links, and stores the traffic once in a large rotating file stored on disk. Secondary units (with greatly reduced storage requirements) receive either all or subsets of the received traffic over high-speed links connecting the head-unit to the secondary EndaceProbes.





## Comparison Table

Option	Pros	Cons
Replicator Tap	<ul style="list-style-type: none"> <li>One EndaceProbe can die or be taken offline without impacting the operation of other EndaceProbes</li> </ul>	<ul style="list-style-type: none"> <li>Replicator taps are slightly more expensive than standard taps</li> <li>If the tap is a significant distance from the monitoring EndaceProbes there will be numerous long monitoring links required</li> <li>Number of monitoring-ports must be predetermined when the tap is installed</li> </ul>
Daisychaining	<ul style="list-style-type: none"> <li>A simple two monitoring-port tap is all that is required</li> <li>Reduces amount of cabling from tap point to where EndaceProbes are located</li> <li>Scales easily; EndaceProbes can be added as needed</li> </ul>	<ul style="list-style-type: none"> <li>If an EndaceProbe in the chain dies then the chain is broken and downstream Probes stop receiving traffic</li> <li>More complex wiring among EndaceProbes</li> <li>Each EndaceProbe must store all the traffic it wants to record. This is expensive, and can lead to the various Probes having an inconsistent record of what happened</li> </ul>
Forwarding	<ul style="list-style-type: none"> <li>A simple two monitoring-port tap is all that is required</li> <li>Reduces amount of cabling from tap point to where EndaceProbes are located</li> <li>Allows a subset of traffic to be sent to each secondary EndaceProbe, either as a continuous 'push' service in real-time, or as a 'pull' service (i.e. data mining). This can extend the useful life of legacy (i.e. already installed) low-speed monitoring EndaceProbes by ensuring they only sent the amount of traffic they can actually handle</li> <li>Helps put in place procedures for controlling and securing access to information</li> <li>Allows a single EndaceProbe to create a single copy of all data, and this data becomes the authoritative dataset for that link</li> </ul>	<ul style="list-style-type: none"> <li>Complex wiring among EndaceProbes</li> <li>If the head-unit EndaceProbe fails then all Endace-Probes stop receiving traffic</li> <li>The number of ports of the head-unit EndaceProbe must be sufficient to support future installation of additional EndaceProbes</li> </ul>

For more information on Endace products visit: [endace.com](http://endace.com)  
 For enquiries email: [enquiries@endace.com](mailto:enquiries@endace.com)