Notice

Every effort was made to ensure that the information in this manual was accurate at the time of printing. However, information is subject to change without notice, and VIAVI reserves the right to provide an addendum to this manual with information not available at the time that this manual was created.

Copyright

© Copyright 2020 VIAVI Solutions Inc. All rights reserved. VIAVI and the VIAVI logo are trademarks of VIAVI Solutions Inc. ("VIAVI"). All other trademarks and registered trademarks are the property of their respective owners. No part of this guide may be reproduced or transmitted, electronically or otherwise, without written permission of the publisher.

Copyright release

Reproduction and distribution of this guide is authorized for Government purposes only.

Terms and conditions

Specifications, terms, and conditions are subject to change without notice. The provision of hardware, services, and/or software are subject to VIAVI standard terms and conditions, available at www.viavisolutions.com/terms.

Specifications, terms, and conditions are subject to change without notice. All trademarks and registered trademarks are the property of their respective companies.

Federal Communications Commission (FCC) Notice

This product was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this product in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

The authority to operate this product is conditioned by the requirements that no modifications be made to the equipment unless the changes or modifications are expressly approved by VIAVI.

Laser compliance

This device is a class 1 laser product.

Industry Canada Requirements

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

WEEE and Battery Directive Compliance


This product, and the batteries used to power the product, should not be disposed of as unsorted municipal waste and should be collected separately and disposed of according to your national regulations. In the European Union, all equipment and batteries purchased from VIAVI after 2005-08-13 can be returned for disposal at the end of its useful life. VIAVI will ensure that all waste equipment and batteries returned are reused, recycled, or disposed of in an environmentally friendly manner, and in compliance with all applicable national and international waste legislation.

It is the responsibility of the equipment owner to return equipment and batteries to VIAVI for appropriate disposal. If the equipment or battery was imported by a reseller whose name or logo is marked on the equipment or battery, then the owner should return the equipment or battery directly to the reseller.

Instructions for returning waste equipment and batteries to VIAVI can be found in the Environmental section of VIAVI web site at . If you have questions concerning disposal of your equipment or batteries, contact VIAVI WEEE Program Management team at WEEE.EMEA@viavisolutions.com.

Technical Support

<table>
<thead>
<tr>
<th>Region</th>
<th>Phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>1.844.GO VIAVI / 1.844.468.4284</td>
</tr>
<tr>
<td>Latin America</td>
<td>+52 55 5543 6644</td>
</tr>
<tr>
<td>EMEA</td>
<td>+49 7121 862273</td>
</tr>
<tr>
<td>APAC</td>
<td>+1 512 201 6534</td>
</tr>
<tr>
<td>All Other Regions</td>
<td>viavisolutions.com/contacts</td>
</tr>
<tr>
<td>email</td>
<td><a href="mailto:customer.care@viavisolutions.com">customer.care@viavisolutions.com</a></td>
</tr>
</tbody>
</table>

Support hours are 7:00 A.M to 7:00 P.M. (local time for each office).
# Table of Contents

Chapter 1: Getting started........................................................................................................5
  Optical nTAP Overview........................................................................................................5
  Security, convenience, and dependability........................................................................5

Chapter 2: Why choose a TAP or SPAN port.........................................................................6
  Choosing between a SPAN, Aggregator, or full-duplex TAP................................................6
  Deciding whether to use a TAP or a SPAN/mirror port......................................................7
  When to use a SPAN/mirror port.......................................................................................9
  When to use the Aggregator TAP....................................................................................12
  When to use a full-duplex TAP........................................................................................13

Chapter 3: Features................................................................................................................14
  Features.................................................................................................................................14

Chapter 4: Standard and Optional Parts..............................................................................15
  Parts......................................................................................................................................15

Chapter 5: Optical nTAP Installation.....................................................................................16
  Installing.................................................................................................................................16

Chapter 6: Attenuation............................................................................................................18
  Attenuation and TAPs........................................................................................................18
  Managing attenuation.........................................................................................................19
  Attenuation and optical cables............................................................................................19
  Determining the best split ratio for you................................................................................19

Chapter 7: Technical Specifications......................................................................................24
  Technical specifications........................................................................................................24

Chapter 8: Troubleshooting...................................................................................................26
  What latency does a TAP create?........................................................................................26
  Not seeing traffic at the analyzer from the TAP...................................................................26
  Can I “team” or bond NICs in my analyzer?........................................................................27
  I am seeing CRC errors on my network............................................................................28
Chapter 1: Getting started

Optical nTAP Overview

Thank you for purchasing the Optical nTAP. Your new product is the most robust, secure, and convenient mechanism for network analyzers and similar devices to copy data streams from high-capacity network links.

A network Test Access Port (TAP) provides access to the data streams passing through a high-speed, full-duplex network link (typically between a network device and a switch). The TAP copies both sides of a full-duplex link (copper or optical, depending on type of TAP), and sends the copied data streams to an analyzer, probe, intrusion detection system (IDS) or any other analysis device. There are different TAP models available to monitor both copper and optical links.

Security, convenience, and dependability

The security and convenience of a TAP makes it preferable to inline connections for network analysis and intrusion detection and prevention (IDS/IPS) applications.

Because a TAP has no address on the network, the TAP and the analyzer connected to it cannot be the target of a hack or virus attack. TAPs are economical to install, allowing you to leave them permanently deployed. This allows you to connect and disconnect the analysis device as needed without breaking the full-duplex connection, much like plugging in an electrical device.

A TAP is also preferable to using a switch’s SPAN/mirror port to copy the data stream. Unlike the SPAN/mirror port, a TAP will not filter any SPAN/mirror port is a half-duplex link (that is, a send-only “simplex” data stream), it has the capacity to transmit only half of a fully-saturated link. Additionally, a TAP does not use any of the switch’s CPU resources.
Chapter 2: Why choose a TAP or SPAN port

Choosing between a SPAN, Aggregator, or full-duplex TAP

Whether you use a SPAN/mirror port, aggregator TAP, or full-duplex TAP depends on the saturation level of the link (up to 200% of link speed when both sides are combined) you want to monitor and the level of visibility you require.

There are numerous ways to access full-duplex traffic on a network for analysis: SPAN/mirror ports, Aggregator TAPs, or full-duplex TAPs are the three most common.

Each approach has advantages and disadvantages. SPANs and Aggregator TAPs are designed to work with a standard (and usually less expensive) network card on the analysis device, but their limitations make them less than ideal for situations where it is necessary to guarantee the visibility of every packet on the wire.

A full-duplex TAP is the ideal solution for monitoring full-duplex networks utilized at more than 50 percent (100% when both sides are combined), but its design requires that the analyzer be a specialized device with a dual-receive capture interface that is capable of capturing the TAP’s output, providing accurate timing, and recombining the data for analysis.

Table 1 (page 6) list the advantages and disadvantages of three common methods of accessing traffic from full-duplex networks for analysis, monitoring, or forensics:

<table>
<thead>
<tr>
<th></th>
<th>Aggregator</th>
<th>SPAN/Mirror</th>
<th>Full-Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires power</td>
<td>X</td>
<td>X</td>
<td>X(^1)</td>
</tr>
<tr>
<td>Better(^2) protection against dropped packets</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Uses single-receive capture card</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Uses internal buffer to mitigate traffic spikes</td>
<td>X(^3)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Choosing between a SPAN, Aggregator, or full-duplex TAP

Chapter 2: Why choose a TAP or SPAN port

<table>
<thead>
<tr>
<th>Suitable for networks with light to moderate traffic with occasional spikes</th>
<th>Aggregator</th>
<th>SPAN/Mirror</th>
<th>Full-Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Passes OSI Layer 1 &amp; 2 errors</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Not Addressable (cannot be hacked)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requires dual-receive capture card</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ideal for heavy traffic/critical networks</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Suitable for networks with light to moderate traffic</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Remotely configurable</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

1. The Optical TAP does not require power, but the Copper TAP does.
2. Better protection against dropping packets than SPAN/mirror.
3. Although the Aggregator TAP has an internal buffer that mitigates spikes in traffic, when the buffer itself is full, the new packets are dropped until the output of the buffer can catch up.

Whether you are monitoring a network for security threats or capturing and decoding packets while troubleshooting, you need a reliable way to see the network traffic. The appropriate TAP for capturing full-duplex data for analysis depends on the rates of traffic you must monitor, and what level of visibility you require.

- Attaching a monitoring or analysis device to a switch’s analyzer port (SPAN/mirror port) to monitor a full-duplex link.

Because a SPAN/mirror port is a send-only simplex stream of data there is a potential bottleneck when trying to mirror both sides of a full-duplex link to the analyzer’s single receive channel. When to use a SPAN/mirror port (page 9).

- Attaching a monitoring or analysis device to an Aggregator TAP inserted into a full-duplex link.

As with a SPAN, the Aggregator TAP copies both sides of a full-duplex link to the analyzer’s single receive channel. It uses buffering which makes it somewhat better able to keep up with higher traffic levels than a SPAN. For more details, see When to use the Aggregator TAP (page 12) and.

- Attaching a dual-receive monitoring or analysis device to a full-duplex TAP inserted into a full-duplex link.

*Dual-receive* means that the network card on the analysis device has two receive channels rather than the transmit and receive channels associated with a standard full-duplex link. For more details, see When to use a full-duplex TAP (page 13).

Deciding whether to use a TAP or a SPAN/mirror port

SPANs are great for proof of concepts and lightly used links. TAPs ensure you get all of the traffic, including on high speed links, and physical layer errors.

A TAP is a passive splitting mechanism installed between a device of interest and the network. A TAP copies the incoming network traffic and splits it. It passes the network traffic to the network and sends a copy of that traffic (both send and receive) to a monitoring device in real time.
A SPAN/mirror port on a switch that copies traffic on a port or group of ports and sends the copied data to an analyzer. By its very nature it is half-duplex, which means that it cannot send all of the send and receive traffic it sees if traffic exceeds 50% of the bandwidth. Moreover, switch manufacturers design their products so that the SPAN/mirror port has a lower priority in the switch operating system. Therefore, one of the first things to stop working when the switch gets busy is the SPAN/mirror port traffic flow. A SPAN/mirror port is fine for connections to stations at the edge of your network, but may be unable to keep up with the higher traffic volumes on your full duplex links at the core of your network. It is convenient for a proof of concept, but cannot pass physical layer errors (poorly formed packets, runts, CRCs) to the analyzer and give you all of the visibility you need for Gigabit, 10 Gigabit or 40 Gigabit networks, but a TAP will.

Most enterprise switches copy the activity of one or more ports through a Switch Port Analyzer (SPAN) port, also known as a mirror port. An analysis device can then be attached to the SPAN port to access network traffic.

There are four common ways to get full duplex data to a probe or analyzer:

- Connect the probe to a SPAN/mirror port. A SPAN/mirror port can provide a copy of all designated traffic on the switch in real time, assuming bandwidth utilization is below 50% of full capacity.
- Deploy an Aggregator TAP on critical full duplex links.
- Deploy a full duplex TAP on critical links to capture traffic. For some types of traffic, such as full duplex gigabit links, TAPs are the only way to guarantee complete analysis, especially when traffic levels are high.
- Traffic aggregators, like the Observer Matrix, allow you to copy and filter full duplex traffic. Because full-duplex Ethernet links lies at the core of most corporate networks, ensuring completely transparent analyzer access to those links is critical.

Figure 1: TAP versus SPAN

<table>
<thead>
<tr>
<th>Pros</th>
<th>TAP</th>
<th>SPAN/mirror port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Greatly reduces the risk of dropped packets</td>
<td>Low cost</td>
</tr>
<tr>
<td></td>
<td>Monitoring device receives all packets, including physical errors</td>
<td>Remotely configurable from any system connected to the switch</td>
</tr>
<tr>
<td></td>
<td>Provides full visibility into full-duplex networks</td>
<td>Able to copy intra-switch traffic</td>
</tr>
<tr>
<td>Cons</td>
<td>Analysis device may need dual-receive capture interface if you are</td>
<td>Cannot handle heavily utilized full-duplex links without dropping packets</td>
</tr>
<tr>
<td>TAP</td>
<td>SPAN/mirror port</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>using a full-duplex TAP (does not apply to the Aggregator TAP family)</td>
<td>Filters out physical layer errors, hampering some types of analysis</td>
<td></td>
</tr>
<tr>
<td>Additional cost with purchase of TAP hardware</td>
<td>Burden placed on a switch’s CPU to copy all data passing through ports</td>
<td></td>
</tr>
<tr>
<td>Cannot monitor intra-switch traffic</td>
<td>Switch puts lower priority on SPAN port data than regular port-to-port data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can change the timing of frame interaction altering response times</td>
<td></td>
</tr>
<tr>
<td>Bottom line</td>
<td>A TAP is ideal when analysis requires seeing all the traffic, including physical-layer errors. A TAP is required if network utilization is moderate to heavy. The Aggregator TAP can be used as an effective compromise between a TAP and SPAN port, delivering some of the advantages of a TAP and none of the disadvantages of a SPAN port.</td>
<td>A SPAN port performs well on low-utilized networks or when analysis is not affected by dropped packets.</td>
</tr>
</tbody>
</table>

**When to use a SPAN/mirror port**

The advantage of using a SPAN/mirror port is its cost, as a SPAN/mirror port is included for free with nearly every managed switch. A SPAN/mirror port is also remotely configurable, allowing you to change which ports are mirrored from the switch management console.

There are some limitations in using a SPAN/mirror port. Limitations of a SPAN/mirror port stem from the aggregation necessary to merge full-duplex network traffic into a single receive channel. For examples, when traffic levels on the network exceed the output capability of the SPAN/mirror port, the switch is forced to drop packets. Another reason that a SPAN/mirror port may not be the right choice is because Layer 1 and 2 errors are not mirrored and therefore never reach the analyzer. When performing network troubleshooting, seeing these errors can be important.

When monitoring with a SPAN/mirror port on a switch, the switch does three things:

- Copies both the send and receive data channels
- Reconstructs an integrated data stream from the two channels
- Routes the integrated signal to the send channel of the SPAN/mirror port

Each of these activities burdens the switch’s internal processor. These demands on the switch’s CPU have implications for both your monitoring equipment and general network performance. Using a SPAN/mirror port to capture network traffic for analysis presents the following risks:

- As total bandwidth usage for both channels exceeds the capacity of the outbound link to the analyzer, the excess traffic is dropped from the analyzer stream. There simply is not enough bandwidth to transmit both sides of the full-duplex traffic across a single standard interface.
- The switch’s CPU must act as both a network switch and a packet-copier. The switch’s CPU must also integrate the two data streams (send and receive) together correctly. Both packet copy/re-direction and channel integration is affected by switch load. This means the SPAN/mirror port may not deliver accurate captures when the switch is under heavy...
Choosing between a SPAN, Aggregator, or full-duplex TAP

Load. Monitoring a 10/100 network through a Gigabit SPAN/mirror port and analyzer does not alleviate these concerns. Also, there is no notification when the SPAN/mirror port is dropping packets or delivering inaccurate time stamps.

A SPAN/mirror port can deliver satisfactory results when used to monitor lightly used, non-critical networks. If network utilization exceeds the capacity of the outbound (analyzer) link, packet loss results—which invalidates many types of analysis, and makes monitoring for certain kinds of network activity impractical. For example, you might miss a virus signature because packets are being dropped. When analyzing a transaction or connection problem, the analyzer may detect problems where none exist because expected packets are being dropped by the SPAN/mirror port. Hardware and media errors will also be impossible to troubleshoot through a SPAN/mirror port, as these errors are not mirrored to the analyzer.

Cloning your SPAN/mirror port

You can still access your SPAN/mirror port even if all of your SPAN/mirror ports on your switch are used. This is fairly common, and you can use a TAP to produce two copies of the SPAN/mirror port.

By cloning a SPAN/mirror port you get the benefits of a duplicate copy of the traffic and no security risk.
Joining SPAN/mirror ports

If you have a primary switch and a failover switch, you can connect both of them to the Aggregator TAP. Connect one of them to Link A and the other to Link B.

It does not matter whether the primary switch is connected to Link A or Link B, and you do not need to know which one is “live.” The Aggregator TAP joins the active and inactive SPAN/mirror port session together and sends the result to the analyzer. Regardless which switch is primary, the Aggregator TAP sends the SPAN/mirror port data from that switch to the analyzers.
When to use the Aggregator TAP

The Aggregator TAP offers a compromise between the SPAN/mirror port and full-duplex TAP options. It costs more than a full-duplex TAP due to the added complexity and memory requirements of its built-in buffer.

The Aggregator TAP does not require a specialized (and potentially more expensive) analyzer with a dual-receive capture interface. Like a full-duplex TAP, it is independent of the network, making it immune to security threats.

The Aggregator TAP includes an internal buffer to mitigate the bandwidth problem associated with converging both sides of the full-duplex traffic from the network into one side of the full-duplex link to the analyzer. The buffer is able to cache some spikes in network utilization, but the Aggregator TAP drops packets when the bursts of activity exceed its buffer capacity.

The Aggregator TAP is ideally suited to work with an analysis device with a standard, single-receive capture interface or NIC. This means that a laptop or a standard system can be deployed as an analyzer rather than the more expensive specialized analyzers or appliances that are designed to accept full-duplex traffic through a dual-receive capture interface.

Just like a SPAN/mirror port, the Aggregator TAP is ideal for a lightly used network that occasionally has utilization peaks above the capture capacity of the analyzer. Unlike a SPAN/mirror port, the Aggregator TAP will forward Layer 1 and 2 errors to the analysis device.

Another advantage the Aggregator TAP has over a SPAN/mirror port session is its internal memory buffer. The memory buffer provides limited protection against packet loss, and if the network utilization does not regularly exceed the capacity of the analyzer’s capture card, an Aggregator TAP may be the right choice.

The appropriate solution for capturing full-duplex data for analysis depends on the rates of traffic you must monitor, and what level of visibility you require. When monitoring a lightly-used network, using a SPAN/mirror port or Aggregator TAP to supply an analysis device with a standard NIC (i.e., single-receive) interface can be an economical choice. The Aggregator TAP can provide protection against packet loss, but if usage spikes exceed its buffer capacity before the link to the analyzer can catch up, the Aggregator TAP drops packets.

To monitor a critical, heavily utilized full-duplex link, a full-duplex TAP is the only alternative. Monitoring a full-duplex connection using a full-duplex TAP and an analyzer with a dual-receive
capture interface guarantees complete, full-duplex capture for monitoring, analysis, and intrusion detection regardless of bandwidth saturation.

**When to use a full-duplex TAP**

A full-duplex TAP is the only option guaranteeing all of the network traffic makes it to the analysis device (including Layer 1 and 2 error information). Although this can be the most expensive option, it is also the only option that guarantees complete accuracy when the network is highly saturated.

A full-duplex TAP is more complex and potentially expensive to implement, but where there is high network utilization and an importance to guarantee the capture of “everything on the wire” along with errors from all network layers, a full-duplex TAP is the *only* choice. If the analysis requires a high level of data stream fidelity (for instance, looking for jitter in video or VoIP), only a full duplex TAP forwards the original data timing to the analyzer.

**Note:** A full-duplex TAP must be coupled with a probe or monitoring device capable of receiving both channels of a full-duplex signal and recombining the two channels into a single data stream for analysis.

A full-duplex TAP is a passive mechanism that is installed between two network devices. An Optical TAP is non-electronic (no power) and optically splits the signal into two full-duplex signals. One signal maintains the network link, while the other is passed to an analyzer equipped with a dual-receive capture card. A Copper TAP performs the same function, but uses electronic circuitry to duplicate the signals.

Because a full-duplex TAP copies both the send and receive channels from a full-duplex link to the analyzer (where the data is integrated), the analyzer can monitor a full-duplex network at line rate—assuming the capture card in the analyzer is capable.

All TAPs from VIAVI, except the Aggregator TAP family, are full-duplex TAPs.
Chapter 3: Features

Features

Key features of the Optical nTAP include:

- No AC power required
- Passive access without packet tampering or introducing a single point of failure
- All traffic (including errors) is passed from all OSI layers for analyzing
- Enhanced security because the nTAP does not require or use an IP address, making it undetectable compared to a SPAN
- Allows you to connect and disconnect the analysis device as needed without taking the network down
- Fully IEEE 802.3 compliant
- Fully RoHS compliant
- Front-mounted connectors make installation simple
- Optional 19-inch 1U rack mount panel holds up to three nTAP
Chapter 4: Standard and Optional Parts

Parts

The Optical nTAP comes with several parts. If any part is missing or damaged, contact VIAVI immediately.

The Optical nTAP ships with the following items:

♦ Optical nTAP
♦ Quick Reference Card

Your kit may also contain optionally available parts (for instance, patch cables).
Chapter 5: Optical nTAP Installation

Installing

Prerequisite(s):

- Decide where to place the nTAP and physically mount it, if desired. Depending on the form factor purchased, this may be in a drive bay, rack mount bracket, or wherever it is most convenient.
- Connect your device of interest (for instance, switch, router, etc.) to the Optical nTAP using standard optical cables with an LC connector to complete the pass-through connection.
- Connect the nTAP to your analyzer or other monitoring device using optical cables. Be certain to connect to the receive ports of the capture card in your analyzer.
- The network adapter you connect to the Analyzer side of the Optical nTAP must have auto-negotiation disabled, otherwise no traffic will be passed to that network adapter. This also means the network adapter must support the ability to disable auto-negotiation; not all third-party network adapters support this. However, all Gen3 capture card models can enable and disable auto-negotiation.

An Optical TAP splits the full-duplex signals, allowing the monitoring device access to a copy of the data stream while maintaining uninterruptable data flow through the monitored link. Optical TAPs require no external power. They are available in various split ratios to match the optical signal strength requirements of the network connections and of the monitoring equipment.

When traffic comes in to Link A, two copies are made in the TAP. One copy is sent out Link B to the switch and the other copy is sent out the Analyzer port A to the analysis device. A similar thing happens with traffic that comes in Link B. Two copies are made. One copy is sent out Link A and the other copy is sent out the Analyzer port B. Due to how the TAP is designed, it is not possible for traffic from the Analyzer side to pass to the Link side.
Caution: Before you temporarily break the link between the device of interest and the network, you may want to shut down access to that device and notify users of the down time.

1. Disconnect the cable from your device (typically a switch) and connect it to Link B.
2. Use another full-duplex cable to connect the network device (or primary device in a failover arrangement) to Link A port, thus completing the pass-through link.
3. Use a Y-cable (i.e., a splitter cable) to connect the nTAP’s Analyzer port to the receive sockets on your analyzer’s capture interface. Be certain to connect the cable to the capture card in your analyzer. As an alternative, you can split your own duplex cable (or use two simplex cables) to connect each side of the Analyzer ports on the TAP to the receive ports on each of the NICs in the analyzer.
4. Ensure that auto-negotiation is disabled on the receiving capture card in your analyzer. See the documentation for your capture card or analyzer for details. If auto-negotiation is enabled, the analyzer will not be able to receive the stream from the TAP until it is.

All Optical TAP devices contribute to optical attenuation. See a fuller discussion of it in Attenuation.
Chapter 6: Attenuation

Network administrators who manage optical links have the added challenge of dealing with signal attenuation—the rate at which light dissipates over a network.

Attenuation is caused by a number of factors and can affect both network performance and the ability to analyze the network.

Excessive signal attenuation can cause link failure. Understanding signal levels, selecting the right split ratio on TAPs, and carefully managing the location of repeaters can prevent problems. This section defines attenuation, explains how it is affected by fiber and other optical elements on a network, and how it can be efficiently managed.

**Attenuation** is the reduction of signal strength during transmission caused by the absorption of light from the materials through which it travels. Greater signal loss equals higher attenuation. A signal can lose intensity or experience increased attenuation with each surface or medium it traverses. Many factors contribute to the attenuation rate of signals including devices such as TAPs and transmission through optical cables.

Optical signal strength is measured in decibels (dB) and is based on a logarithmic scale. If a signal attenuates too much, the destination device cannot identify it or the signal may not even reach the destination. This is why some optical links depend on repeaters, which amplify the signal.

**Attenuation and TAPs**

As with all devices inserted into an optical link, one side effect of TAP usage is signal attenuation.

TAPs are used to provide access to the data streams passing through a high-speed, full-duplex network link. TAPs deliver a complete copy of data to a monitoring device for accurate analysis. An Optical TAP optically splits the light power of the full-duplex signal into two copies. One part of the split signal is sent to the other device on the network, while the other is simultaneously passed to the analysis or monitoring appliance.
A TAP attenuates the signal for two reasons:

♦ A portion of the signal strength is “siphoned off” and sent to the analyzer. How much of the signal strength is redirected for analysis depends on the split ratio of the TAP.
♦ The connections and internal TAP cables and connectors absorb and refract a small portion of the signal.

An Optical TAP contributes to signal attenuation, but typically not enough to make a significant difference on the network.

An optical split ratio must be designated on each TAP. In most cases, a 50/50 split ratio is ideal, providing sufficient light to both the network and monitoring device. However, there may be special cases that require an alternative ratio in order to meet signal power needs. For example, if a TAP is cabled close to the analyzer NIC and the link under test requires a long cable run, you may want to provide more light power back to the network than to the monitoring device. If you do choose a ratio other than 50/50, keep in mind that the signal has to be strong enough for it to be interpreted at the analyzer. More details about this are covered in Determining the best split ratio for you (page 19).

Managing attenuation

Managing signal attenuation is critical for running a network at optimal performance.

If signal attenuation is too high, destination devices may not be able to establish a link or receive network traffic. Repeaters can help, but they can be costly and inconvenient to implement. In general, unless a signal must travel a long distance or is compromised by patch panels, there should not be a problem using the 50/50 split ratio. The most efficient and cost-conscious way to manage attenuation is to measure signal levels throughout the network and place repeaters only when and where they are needed.

To determine if a light signal is at an acceptable level at any point on a network, it is helpful to use an optical power meter. Optical power meters measure signal power at a port, helping you determine whether a device is receiving a strong enough signal and thereby identifying if repeaters need to be placed. The meters are typically inexpensive and are offered from a number of vendors.

Attenuation and optical cables

Optical cables contribute to signal attenuation. As light travels through an optical cable, some of its energy gets dispersed and absorbed by the cable. The attenuation rate varies depending on the cable type used.

Depending on your transmission technology, you may be required to use a specific cable type. Examples include single-mode (for LX or LR) and multimode (for SX or SR). Multimode cable has a larger core diameter than single-mode cable, resulting in greater light dispersion. Unless the cable run is extremely long, the signal attenuation for both cable types is a minor contributor to the power loss budget. However, multimode cable does cause higher signal attenuation than single-mode cable. Check with the cable manufacturer to determine specific attenuation rates.

Determining the best split ratio for you

To ensure that all of the devices receive enough light power to establish and maintain a connection, you must understand where light can be “lost” as it travels between the network devices connected to the TAP and from the TAP to the analyzer.
Fiber optic data travels on light power. A fiber optic TAP makes a copy of the data for the analyzer by splitting the light power.

After the send strength and receive sensitivities of the ports and cable distances are known, a “power loss budget” can be calculated. The power loss budget can be helpful in determining if there is enough signal strength left at the analyzer receive port for a desired split ratio.

The primary factors that need to be collected to determine loss budget are the:

- Transmit power from the network devices
- Cable distance from the network device to the TAP
- Maximum insertion loss from the TAP
- Cable distance from the TAP to the analyzer
- Analyzer port receive sensitivity
- Other less crucial items that may also affect you include:
  - Number or quality of any connectors or patch panels in the path to and from the TAP
  - Age of the fiber cables
  - Amount of heat in the environment where the fiber runs

Table 3. Maximum Insertion Losses

<table>
<thead>
<tr>
<th>Split Ratio</th>
<th>Multimode 62.5 micrometer</th>
<th>Multimode 50 micrometer</th>
<th>Single-Mode 9 micrometer</th>
</tr>
</thead>
<tbody>
<tr>
<td>50/50</td>
<td>3.9/3.9</td>
<td>4.7/4.7</td>
<td>4.5/4.5</td>
</tr>
<tr>
<td>60/40</td>
<td>3.0/5.0</td>
<td>3.8/5.7</td>
<td>3.7/5.6</td>
</tr>
<tr>
<td>70/30</td>
<td>2.3/6.3</td>
<td>3.0/7.0</td>
<td>2.9/7.0</td>
</tr>
<tr>
<td>Fiber Loss/km</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Connector Loss</td>
<td>.5</td>
<td>.5</td>
<td>.5</td>
</tr>
</tbody>
</table>

1. The ratio is network/analyzer. So, a 70/30 connection has 70% of the light power for the network and 30% for the analyzer.
2. Fiber loss is per kilometer of fiber.

In each split ratio, what you are dividing is the light power from the incoming network link. The larger percentage of the light power is used for the connection to the other network device and the smaller portion is the light power for the analyzer. As long as there is sufficient light power, all data is still sent to the analyzer regardless of the split ratio chosen.

Determining your power loss budget is a several step process that requires you to know the send power and receive sensitivities of the devices connected to the TAP, and requires that you do some basic math. Use these equations to determine the light available in decibels at the analyzer.

1. Determine your power loss budget by subtracting the receive sensitivity of the device connected to Link B from the send power of the device connected to Link A. Get these values from the device manufacturers. The amount of loss that you can have through attenuation and connector loss must be less than this power loss budget.

   Example: \((\text{Send Device Power}) - (\text{Receive Device Sensitivity}) = \text{Power Loss Budget}\)

   These values will be negative numbers, so you will be subtracting a negative number from a negative number and its product will be a positive number.
2. Determine the loss caused by attenuation. Use Table 3 for values to assist you. If your cables are less than one kilometer, convert your cable length for the equation.

   **Example:** \((\text{Number of Connectors} \times \text{Connector Loss}) + (\text{Fiber Length of Link A} \times \text{Fiber Loss}) + (\text{Fiber Length of Link B} \times \text{Fiber Loss})=\text{Attenuation}\)

3. Subtract the output from step 2 from step 1.

   **Example:** \(\text{Power Loss Budget} - \text{Attenuation}=\text{Actual Loss}\)

   If the actual loss is less than the power loss budget, then your budget is feasible with your chosen split ratio; however, you must also calculate the power loss budget for the analyzer from Link A and from Link B. Only if both power loss budgets are feasible is the chosen split ratio usable.

4. Determine your maximum insertion loss by subtracting the receive sensitivity of the analyzer from the send power from the device connected to Link A. Get these values from the device manufacturers. This is the amount of loss that you can have through attenuation and connector loss.

   **Example:** \((\text{Send Device Power}) - (\text{Analyzer Sensitivity})=\text{Power Loss Budget}\)

5. Determine the loss caused by attenuation. See **Maximum Insertion Losses** for values to assist you.

   **Example:** \((\text{Number of Connectors} \times \text{Connector Loss}) + (\text{Fiber Length of Link A} \times \text{Fiber Loss}) + (\text{Fiber Length of Analyzer} \times \text{Fiber Loss})=\text{Attenuation}\)

6. Subtract the output from step 5 from step 4.

   **Example:** \(\text{Power Loss Budget} - \text{Attenuation}=\text{Actual Loss}\)

7. Repeat step 4 through step 6 for Link B to the analyzer.

   For example, **Figure 5 (page 21)** shows cable lengths to the TAP from the network devices and from the TAP to the analyzer. Using these cable lengths and some information from the device manufacturers, you can determine the power loss.

   **Figure 5: Cable lengths to/from the TAP**

   The equations here are examples of how to calculate a power loss budget with actual values.
This shows the power loss budget for Link A to Link B.

<table>
<thead>
<tr>
<th></th>
<th>Link A # Link B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Device Power</td>
<td>-9.000</td>
</tr>
<tr>
<td>Receive Device Sensitivity</td>
<td>-19.5</td>
</tr>
<tr>
<td><strong>Power Loss Budget</strong></td>
<td><strong>10.500</strong></td>
</tr>
<tr>
<td>Number of Connectors</td>
<td>4.0</td>
</tr>
<tr>
<td>Connector Loss (^1)</td>
<td>x 0.5</td>
</tr>
<tr>
<td><strong>Connector Loss</strong></td>
<td>2.0</td>
</tr>
<tr>
<td>Fiber Length Link A (8 meters)</td>
<td>0.008</td>
</tr>
<tr>
<td>Fiber Loss Link A (^2)</td>
<td>x 3.0</td>
</tr>
<tr>
<td><strong>Fiber Loss Link A total</strong></td>
<td>+0.024</td>
</tr>
<tr>
<td>Fiber Length Link B (40 meters)</td>
<td>0.04</td>
</tr>
<tr>
<td>Fiber Loss Link B</td>
<td>x 3.0</td>
</tr>
<tr>
<td><strong>Fiber Loss Link B total</strong></td>
<td>+0.120</td>
</tr>
<tr>
<td><strong>Attenuation</strong></td>
<td>-2.144</td>
</tr>
<tr>
<td><strong>Power Loss Budget - Attenuation</strong></td>
<td>8.356</td>
</tr>
</tbody>
</table>

1. Multimode.
2. 850nm multimode.
3. Light power available for network. Any network split ratio smaller than this number is feasible so long as the analyzer side is also feasible.

The budget for the network side is 8.356 dB. Any split ratio is valid because 8.356 dB is greater than any of the insertion losses from Maximum Insertion Losses (page 20).

Before we can say that any split ratio will work though, we must also check the light power to the analyzer.

This shows the power loss budget for Link A to the analyzer.

<table>
<thead>
<tr>
<th></th>
<th>Link A &gt; Analyzer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Device Power</td>
<td>-9.000</td>
</tr>
<tr>
<td>Receive Device Sensitivity</td>
<td>-17.5</td>
</tr>
<tr>
<td><strong>Power Loss Budget</strong></td>
<td><strong>9.000</strong></td>
</tr>
<tr>
<td>Number of Connectors</td>
<td>4.0</td>
</tr>
<tr>
<td>Connector Loss (^1)</td>
<td>x 0.5</td>
</tr>
<tr>
<td><strong>Connector Loss</strong></td>
<td>2.0</td>
</tr>
<tr>
<td>Fiber Length Link A (8 meters)</td>
<td>0.008</td>
</tr>
<tr>
<td>Fiber Loss Link A (^2)</td>
<td>x 3.0</td>
</tr>
<tr>
<td><strong>Fiber Loss Link A total</strong></td>
<td>+0.024</td>
</tr>
<tr>
<td>Fiber Length to Analyzer (75 meters)</td>
<td>0.075</td>
</tr>
<tr>
<td>Fiber Loss Analyzer</td>
<td>x 3.0</td>
</tr>
<tr>
<td><strong>Fiber Loss Link B total</strong></td>
<td>+0.225</td>
</tr>
<tr>
<td><strong>Attenuation</strong></td>
<td>-2.249</td>
</tr>
</tbody>
</table>
Power Loss Budget - Attenuation

1. Multimode.
2. 850nm multimode.
3. Light power available for the analyzer. Any split ratio smaller than this number is feasible so long as the network side is also feasible.

The budget for the analyzer side is 6.751 dB. The network side allowed us to choose any split ratio, but the analyzer side presents some limitations. Our budget was 9.0 dB, which is greater than our 6.751 dB availability. Since we only have 6.751 dB available, the split ratios we can use are 50/50 and 60/40 after looking at Maximum Insertion Losses (page 20). All others do not provide enough light power to the analyzer.

After completing this task:

Use this page to create your own power loss budget from Link A to Link B if you are considering an Optical TAP with a split ratio other than 50/50. Then use it for your Link A or the analyzer, whichever link has the longer fiber length. Use Maximum Insertion Losses (page 20) to assist you.

Network > Analyzer

Send Device Power
Receive Device Sensitivity -

**Power Loss Budget**

Number of Connectors
Connector Loss x

Fiber Length Link A (or Link B)
Fiber Loss Link A (or Link B) x
*Fiber Loss Link A (or Link B) total* +
Fiber Length to Analyzer
Fiber Loss Analyzer x
*Fiber Loss Analyzer total* +

**Attenuation**

1. Light power available for analyzer. Any split ratio smaller than this number is feasible.
Chapter 7: Technical Specifications

Product dimensions, weight, power consumption, installed operating system, RAM and details along with photos of the appliance.

Technical specifications

This section lists the dimensions, power requirements, supported media, and environmental requirements.

<table>
<thead>
<tr>
<th>Power requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Input</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Environmental requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature range</td>
<td>-40° to +185°F / -40° to +85°C (operating)</td>
</tr>
<tr>
<td></td>
<td>-52° to +185°F / -47° to +85°C (storage)</td>
</tr>
<tr>
<td>Humidity</td>
<td>35-85% (non-condensing)</td>
</tr>
<tr>
<td>Supported media</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fiber</td>
<td>Multimode or Single-Mode</td>
</tr>
<tr>
<td></td>
<td>Multimode support for 1 Gb and 10 Gb only</td>
</tr>
<tr>
<td>Connector</td>
<td>LC</td>
</tr>
<tr>
<td>Fiber diameter</td>
<td>Multimode: 50/125 µm or 62.5/125 µm</td>
</tr>
<tr>
<td></td>
<td>Single-mode: 9/125 µm</td>
</tr>
<tr>
<td>Wavelength ranges</td>
<td>Multimode: 850 or 1300 nanometers</td>
</tr>
<tr>
<td></td>
<td>Single-mode: 1310 or 1550 nanometers</td>
</tr>
<tr>
<td>Wavelength tolerance ranges</td>
<td>Multimode 850/1300 (Dual-window) +/- 20 nanometers</td>
</tr>
<tr>
<td></td>
<td>Single-mode 1310 or 1550 (Dual-window) +/- 40 nanometers</td>
</tr>
<tr>
<td>Insertion losses</td>
<td>See Determining the best split ratio for you (page 19)</td>
</tr>
<tr>
<td>Dimensions</td>
<td></td>
</tr>
<tr>
<td>Width</td>
<td>5.62 in/14.28 cm</td>
</tr>
<tr>
<td>Height</td>
<td>1.15 in/2.93 cm</td>
</tr>
<tr>
<td>Length</td>
<td>7.79 in/19.78 cm; LC connector adds .476 in/1.213 cm</td>
</tr>
</tbody>
</table>
Chapter 8: Troubleshooting

What latency does a TAP create?

Fully optical TAPs (TAPs with only optical connections and that require no power) do not create any latency or delay.

Not seeing traffic at the analyzer from the TAP

If your TAP is not transmitting to the analyzer as you expect, check the following:

♦ The Link is definitely up and running.
♦ The cable connected to the analyzer functions properly. Use a different cable to confirm this.
♦ The Ethernet/SPAN or Fiber channel is not diverted elsewhere.
♦ Try swapping the cables between the ports.
♦ Use a light meter to verify there is enough light power for any optical links.
♦ If you are using an optical connection from the nTAP to your analyzer, including a GigaStor, ensure that the receive NIC on the analyzer has auto-negotiation disabled. If auto-negotiation on the NIC is enabled, you will not be able to see traffic from the nTAP. If this network adapter does not have the option to disable auto-negotiation, you must obtain a different network adapter that can—there are no exceptions.
♦ If the system you are monitoring is Linux or UNIX based, you may have an issue with the Maximum Transmission Unit size. The TCP stack in the UNIX system uses algorithms to produce an MTU based on response time from SYN ACK. A small MTU forces a server and client to redo their handshake. Increase the MTU on your server to alleviate this issue.
Can I “team” or bond NICs in my analyzer?

Yes, it is possible with some limitations. Sometimes it is desirable to use two standard full-duplex capture cards to capture full-duplex TAP output for analysis. Because a standard capture card port has only one receive channel you must aggregate the receive channels from two ports to see both sides of the two-way connection being monitored. Intel’s Advanced Network Services allows you to team multiple connections at the driver level, presenting your analyzer with an aggregated view of send and receive channels.

Because of the processing overhead and its effect on capture card performance, this method is not recommended for monitoring moderate to highly saturated links, such as those between switches. However, it can be an economical alternative when monitoring more lightly used connections, such as between a server and switch.

In addition to the bandwidth limitations, connection teaming is also less accurate when timestamping packets, which can cause unexpected results when your analyzer attempts to display certain charts and statistics such as Connection Dynamics or VoIP jitter. You also will not be able to tell which side is DCE vs. DTE. In short, if you do not have a dual-receive analysis capture card, it is always better to analyze the SPAN or port mirror session through a standard capture card rather than using the connection teaming method described here.

**Note:** You need at least one capture card that supports Advanced Network Services. If the card has two ports, they can be teamed, otherwise another capture card with an unused port must be present.

Figure 6: Capture card teaming

This figure is for illustrative purposes and may not match your product.

1. Configure the IntelPro/1000 Driver Software to Define Teamed Connections. For Ubuntu Linux instructions for port bonding, see the [Ubuntu documentation](#).
2. Connect the TAP to the analyzer using the appropriate cables.
   
   The TAP is cabled between the devices being monitored normally (i.e., it provides a pass-through circuit for the link under test). Instead of connecting to a single dual-receive port (as is the preferred deployment), connect the send lines to the transmit (TX) sides of the two ports you intend to aggregate. You can team ports on separate cards as long as one of them is an IntelPro card.
4. Right-click a Monitor Port from an IntelPro/1000 card (which one does not matter) and choose Properties. Click the Teaming tab.

5. Choose the “Team with other adapters” option and then click New Team... to start the New Team Wizard. The first dialog lets you name the Team (you may want to call it something like “Virtual Dual-receive”).

6. Click Next and add another adapter/port that supports teaming (for example the second port on a dual-port IntelPro card).

7. Click Next and choose Static Link Aggregation. This option works best for aggregating both sides of a full duplex link for analysis. Click Next, and then Finish.

The My Network Places display should now list the new virtual adapter.

I am seeing CRC errors on my network

If you are seeing an uncommonly high number of CRC errors, this could indicate that there is an issue with the TAP, but it may also indicate that the TAP is fine and there are other problems on your network. Contact VIAVI Technical Support for assistance.

VLAN tags not visible at the analyzer

All TAPs pass VLAN tags with the packets. If you are not seeing the VLAN tags at the analyzer, check the following:

♦ On the switch:
  • Confirm that the SPAN was created to pass VLAN tags. Sometimes SPANs are created and passing VLAN tags is not enabled.
  • Confirm the communication between the switch and the router is passing the VLAN tags (normally the communication between them is not a trunk).

♦ On a GigaStor, if you are using one:
  • Confirm the capture card has been enabled to receive or pass VLAN tags.

Memory

Fully optical TAPs do not have internal memory or any electronic components and are strictly a pass-through wherein a copy of the data is made. TAPs with any copper connections have two distinct and separate memory stores.

The two memory stores are non-volatile memory and volatile memory. They are not connected in any way and no data can move between them. The non-volatile memory provides certain functions that make the device work and cannot be modified or changed during normal operation of the device. Volatile memory holds network data as it is copied and passed through the device. Turning off the device clears any data in the volatile memory buffer.

Maximum frame size

The maximum frame size allowed through an nTAP is up to 16K; 64K super jumbo frames are not supported.

Understanding why Link B is active when Link A is offline

Link B is an active port. It is used to negotiate speeds for both Link A and Link B.
Applies to: Any copper-based nTAP.

When the main use of the nTAP is to monitor a server connection, Link A is for the server and Link B is for the router or switch. This allows the server to use a redundant link if Link B goes down, and it keeps the router or switch active if the server goes offline. Should Link A come back up, negotiations to get the link back online are enhanced because Link B already has an active link.

As already stated, Link B is an active port. It is used to negotiate speeds for both Link A and Link B. When you plug in Link A by itself, no negotiation occurs. If you plug in Link B, it negotiates a link speed with whatever device is connected to Link B. Then it negotiates with Link A at that speed. If Link A cannot use that speed, it then negotiates with the end device on Link B at a different rate until a compatible rate between the Link A device and Link B can be established.

One of the great advantages to having this capability is to use the nTAP to replicate traffic to multiple devices and not use it strictly for pass through. For example, when you use an aggregation nTAP and if you connect Link B to a SPAN, you can then pass the SPAN traffic out the two analyzer ports and have two copies of the SPAN traffic going to two different devices. You can have another device receiving the SPAN data on Link A, and if you disconnect Link A, the SPAN traffic for Link B still goes to the analyzer ports for monitoring.

An nTAP is not just for only passing bidirectional communication between Link A and Link B and copying traffic to the two analyzer ports. Take advantage of the active Link B port to daisy chain multiple TAPs together to receive multiple sets of SPAN data streams and combine the multiple SPAN sessions into a single stream. Without the ability for Link B to stay up if Link A were to go offline, you lose this capability.
Chapter 9: FCC compliance statement

<table>
<thead>
<tr>
<th>Specification</th>
<th>Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emissions</td>
<td>FCC Part 15 Class B</td>
</tr>
<tr>
<td>CE Mark</td>
<td>EN61000-3-2, EN55024, EN55022A</td>
</tr>
</tbody>
</table>

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.
Index

Numerics
10/100 network 9
40 Gbps optical cables 19

A
advantages
SPAN 6
aggregator 28
analyzer 26
  auto-negotiation 26
dual-receive capture card 6
no traffic from TAP 26
single-receive capture card 6
attenuation 18
  managing 19
optical cables 19
power loss budget 19
TAPs 18
auto-negotiation 26, 26
analyzer 26

B
bottleneck, SPAN 6
buffer 12

C
cable distance 19
cable lengths 19
cables 19
  see also crossover and straight-through cables 19
capture card 6, 28
choosing NIC, SPAN 27
cloning, SPAN 10
CRC errors 7, 28

D
daisy chain 28
DCE 27
decibels 19
DTE 27
dual receive analyzer 6
dual-receive capture card 6

F
failover, SPAN 11
FCC Compliance Statement 30
full-duplex NIC 27
full-duplex TAP 6, 13

G
GigaStor 26, 28

H
half-duplex 5
half-duplex, SPAN 5

I
IntelPro 27
joining 11
joining, SPAN 11
jumbo frame 28

L
latency 26
light meter 26
light power 18, 19
Link A 28
Link B 28
link loss budget, see power loss budget 19
link negotiation 28
Linux 26, 27
LR 19
LX 19

M
maximum frame size 28
Maximum Transmission Unit 26
mirror port, see SPAN 9
MPO 19
MTU 26
multimode 19, 19, 19

N
NIC teaming 27
NIC, see single-receive capture card and dual-receive capture card 6
no traffic from TAP 26
no traffic from TAP , analyzer 26

O
optical cables 19
optical cables, attenuation 19
optical power meter 19
Optical TAP 26
OSI Layer 1 & 2 errors 5, 6, 12
SPAN 9

P
packets 7
patch panels 19
port bonding 27
power loss budget 19
attenuation 19

R
redundant 28
Regulatory Compliance 30
repeaters 18, 19
risks, SPAN 9
runts 7

S
security 5
SFP modules 26
single-mode 19, 19, 19
single-receive capture card 6
    analyzer 6
    SPAN 12
SPAN 6, 28
    advantages 6
    as bottleneck 6
    choosing NIC 27
    cloning 10
    failover 11
    half-duplex 5
    joining 11
    pros and cons 7
    risks 9
    single-receive capture card 12
    VLAN tags 28
SPANOSI Layer 1 & 2 errors
    OSI Layer 1 & 2 errors 9
split ratios 19
SR 19
SX 19
SYN ACK 26

T
TAP 28
TAPs 18
TCP stack 26

U
UNIX 26

V
VLAN tags 28

W
when to use, SPAN 7