Net Optics Learning Center Presents

The Fundamentals of Passive Monitoring Access

Agenda

Goal: Present an overview of Tap technology and how it makes network monitoring and security devices more effective and efficient.

Schedule:

Section 1	Tap Technology Overview
Section 2	Taps, Port Aggregators, and Regeneration Taps
Section 3	Active Response and Bypass Switches
Section 4	Link Aggregators and Matrix Switches
Section 5	Taps with Intelligence

Tap Technology Overview

Passive Monitoring Access

Access means having visibility to packets.
100% visibility includes packet fragments and Layer 1 and 2 errors.

Passive means without affecting traffic.

- No latency
- No IP Address
- No packets added, dropped, or manipulated
- No link failure

Traffic can be collected from wired networks in the following ways:

- Hubs
- SPAN ports
- In-line Devices
- Taps

What is Zero Delay?

Zero Delay eliminates delays caused by the 10 msec delay found in most taps when the Tap loses power. This short delay can cascade into longer delays while devices renegotiate the link.

Zero Delay means if the Tap loses power,

- No packets are dropped or resent
- No latency is introduced
- Power loss to the Tap in undetectable in the network

Net Optics Products with Zero Delay

- 10/100BaseT Taps
- 10/100BaseT Regeneration Taps

Hubs

Hubs are networking devices that repeat a packet on every interface except the interface that transmitted the packet. All hosts connected to the hub see each other's traffic.

Advantages:

- Very inexpensive
- Easily available

Disadvantages:

- Point of failure
- Half-duplex only
- No retransmission of collisions
- Impractical in a switched network

Placing Devices In-line

A very simple method of deploying security and monitoring devices is to place them in-line on the link.

Advantages:

- See all traffic including Layer 1 and 2 errors
- Preserve full-duplex links
- No access device or additional cables required

Disadvantages:

- Introduces a point of failure
- Relocating the device means link downtime
- Device gets “locked in” one location, limiting device usefulness

SPAN Ports

Switched Port Analyzer (SPAN) Ports, also referred to as “port mirroring” and “port monitoring,” present combined traffic from multiple switch ports.

Advantages:

- Easy access to network traffic because a single NIC on the sensor can connect to a single SPAN port on the switch
- SPAN ports can combine traffic from a variety of switch ports

Disadvantages:

- Switch configuration requires time and resources and can introduce errors resulting in missed traffic
- Under heavy loads, SPAN ports may not see all traffic
- SPAN ports only supply traffic passing through a single switch. Seeing traffic on other devices requires a different approach
- Filters out Layer 1 and 2 errors

Test Access Ports (TAP)

Taps are designed to duplicate traffic for monitoring devices. They create permanent access points for passive monitoring of traffic between any two network devices.

Advantages:

- See all traffic including Layer 1 and Layer 2 errors
- Preserve full-duplex links
- Device neutral - can be installed between any 2 devices
- Remain passive
- Do not introduce a point of failure
- Increases connectivity options for monitoring devices

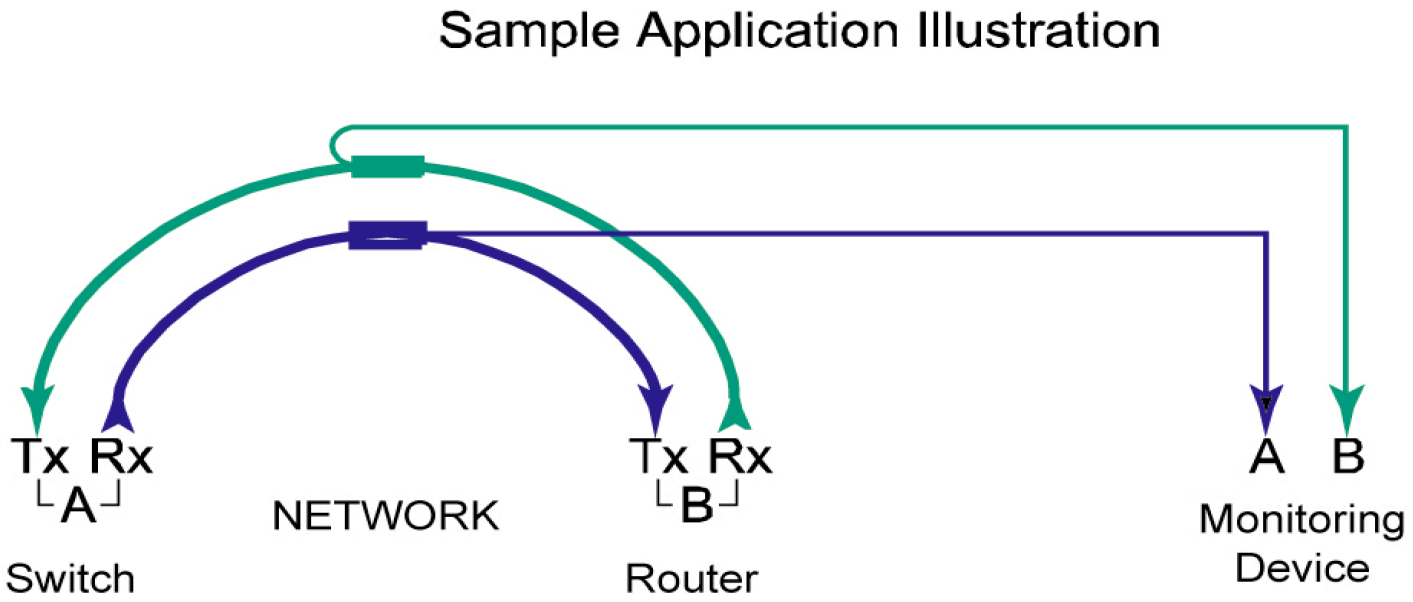
Disadvantage:

- Requires initial monetary investment

What is a Tap?

A Network Tap creates a permanent access port for passively monitoring all traffic on a link without data stream interference or introducing a potential point of failure.

Network Taps use passive splitting or regeneration technology to transmit in-line traffic to an attached management or security device.



Basic Tap Types

There are a variety of Taps available for nearly every network type, from 10Mbps to 10Gbps, fiber and copper. Aside from network type and connectivity there are the following basic types of Taps and similar devices:

Single Tap - Duplicates link traffic for a monitoring device

Regeneration Tap - Duplicates link traffic for multiple monitoring devices

Link Aggregator Tap - Combines traffic from multiple links

Matrix Switches - Offers software-control access to multiple links

Other Tap options include:

Built-in Media Conversion - Use mismatched interfaces without separate media converter

Active Response - Inject responses back into the link

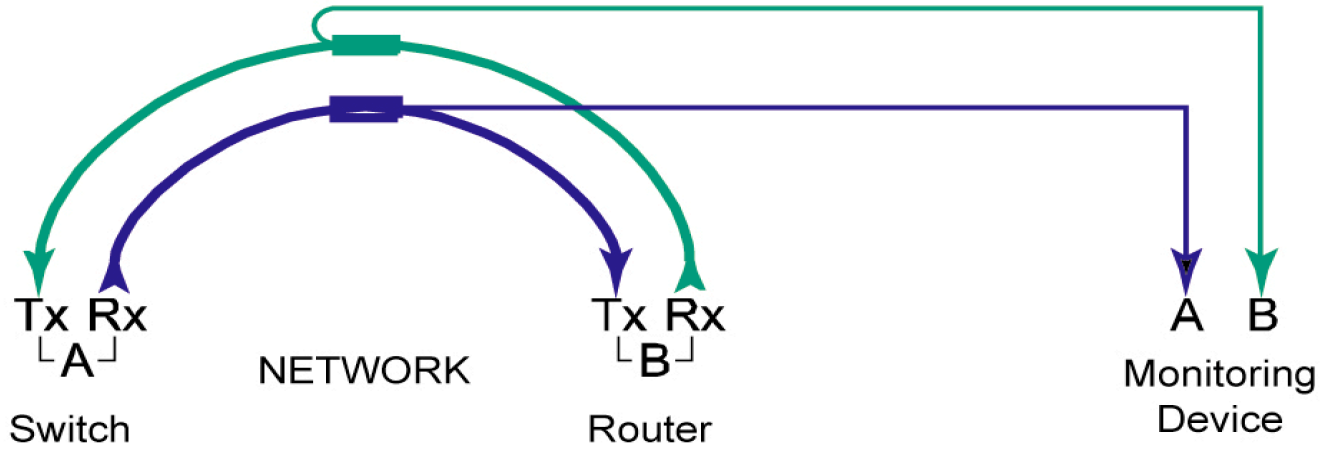
Taps
Port Aggregators
Regeneration Taps

Copper Tap Interfaces

Secure, passive network access for copper monitoring devices on copper networks.

Copper Interfaces:

- 10/100BaseT
- 10/100/1000BaseT
- 1000BaseT



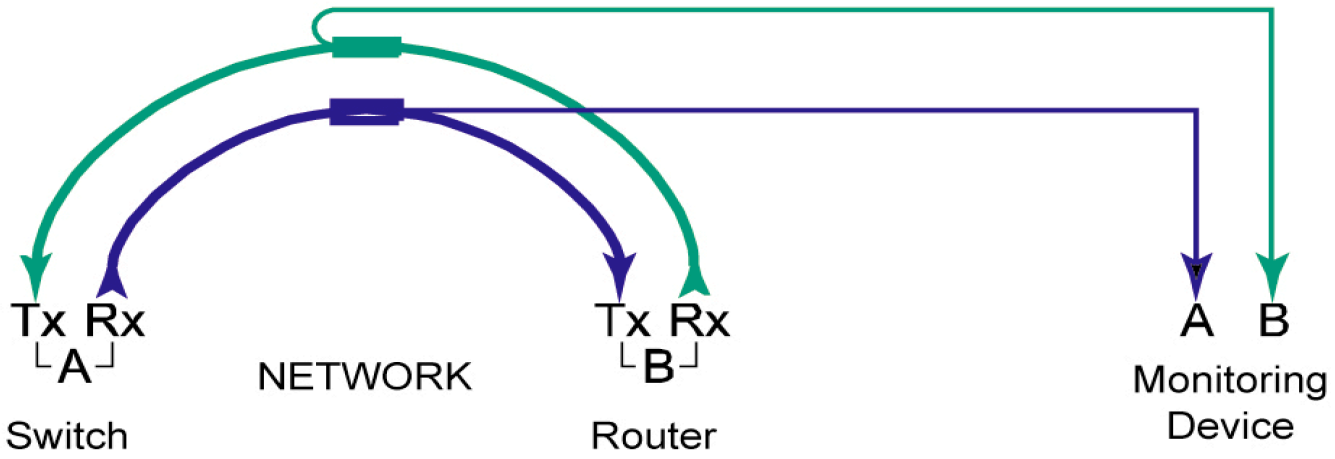
Fiber Tap Interfaces

Secure, passive network access for fiber monitoring devices on fiber networks.

Fiber Interfaces:

- Gigabit
  - SX Mutlimode
  - LX Singlemode
  - ZX Singlemode

10 Gigabit
- SR Multimode
- LR Singlemode
- ER Singlemode



Fiber Tap Split Ratios

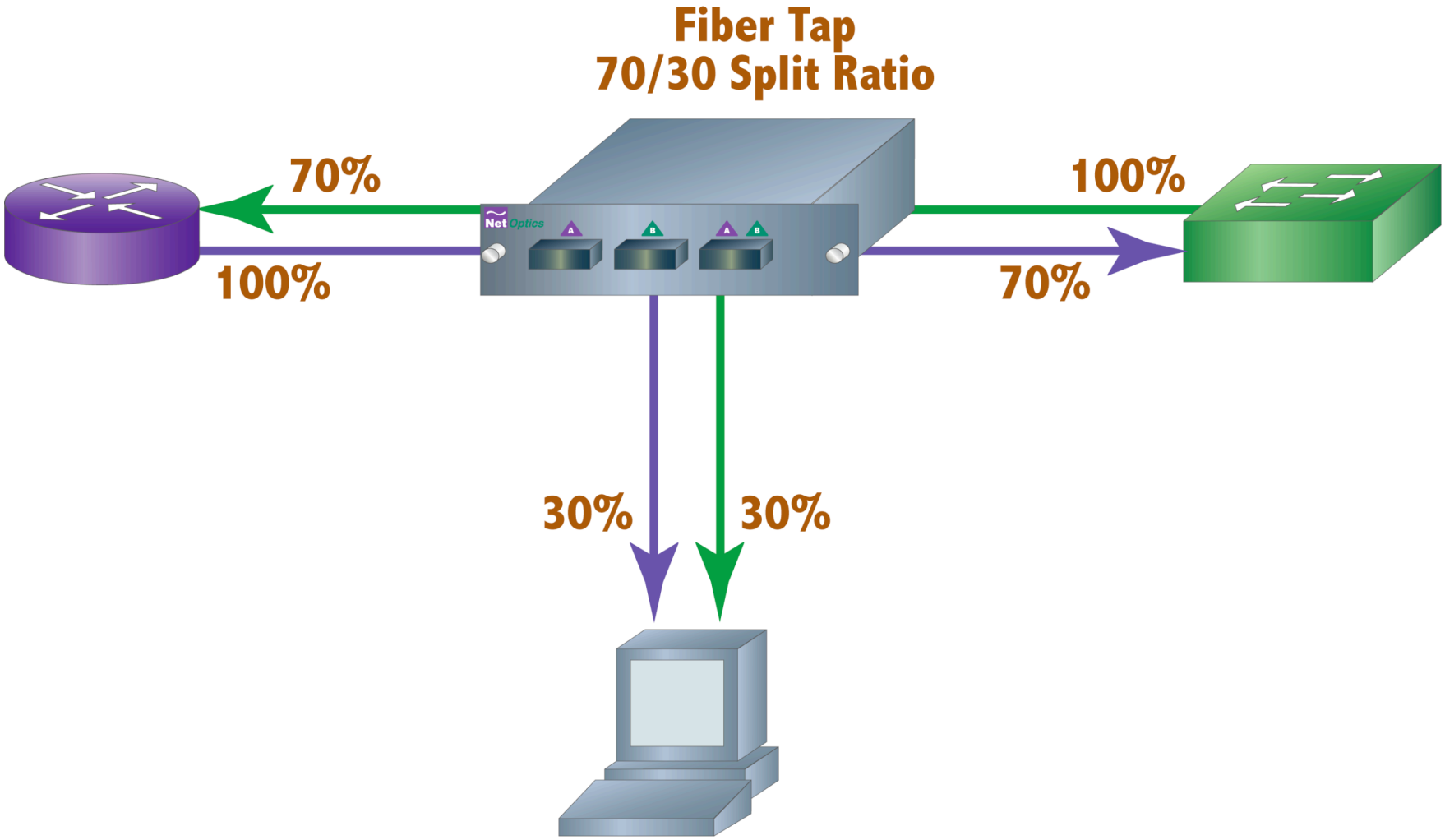
What is a Split Ratio?

A split ratio is the amount of light that is re-directed from the network to the monitor ports.

What is a Loss (power) Budget and how do I calculate it?

A Loss (power) Budget is the amount of attenuation that can be tolerated on the network and monitor links before the end-to-end data is corrupted. To calculate this, you must know the following: Link Distance, Fiber Type, Launch Power, Receiver Sensitivity, number of interconnects and splices.

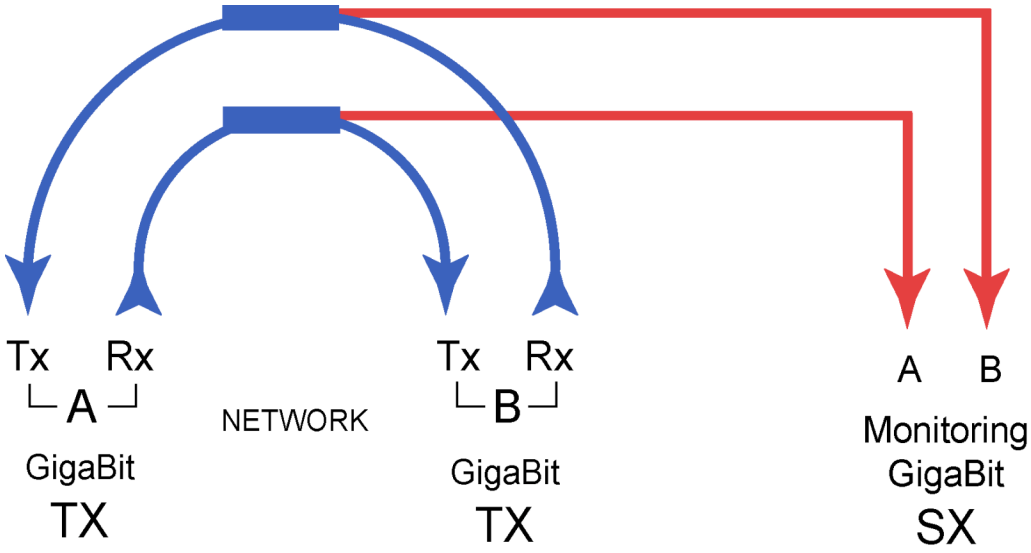
Fiber Tap Split Ratios



Converter Taps

Converter Taps offer all the advantages of a regular tap with the addition of a built-in media converter. Easily connect monitoring devices to dissimilar networks.

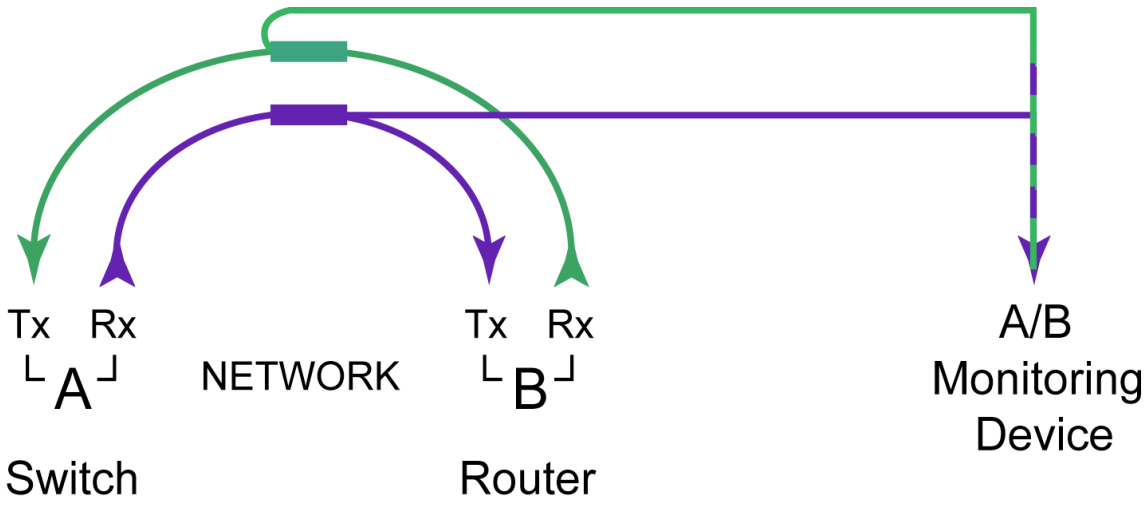
Data Flow in a Converter Tap



Port Aggregator Taps

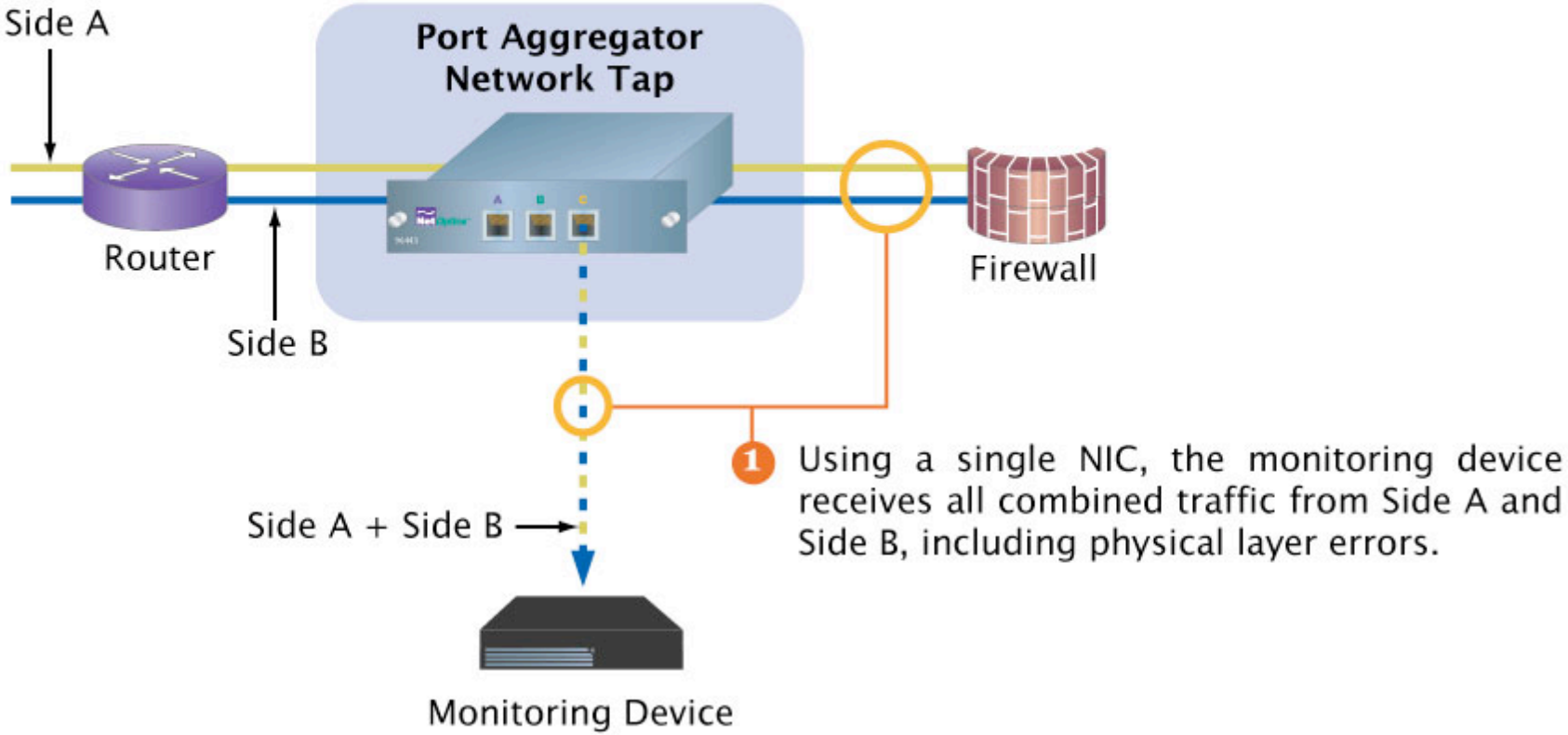
Typically, full-duplex monitoring with a network tap requires two NICs (or a dual channel NIC) – one interface for each side of the tapped full-duplex connection. A port aggregator Tap combines these streams, sending all aggregated data out a passive monitoring port.

Data Flow in a Aggregation Tap



Port Aggregator Taps

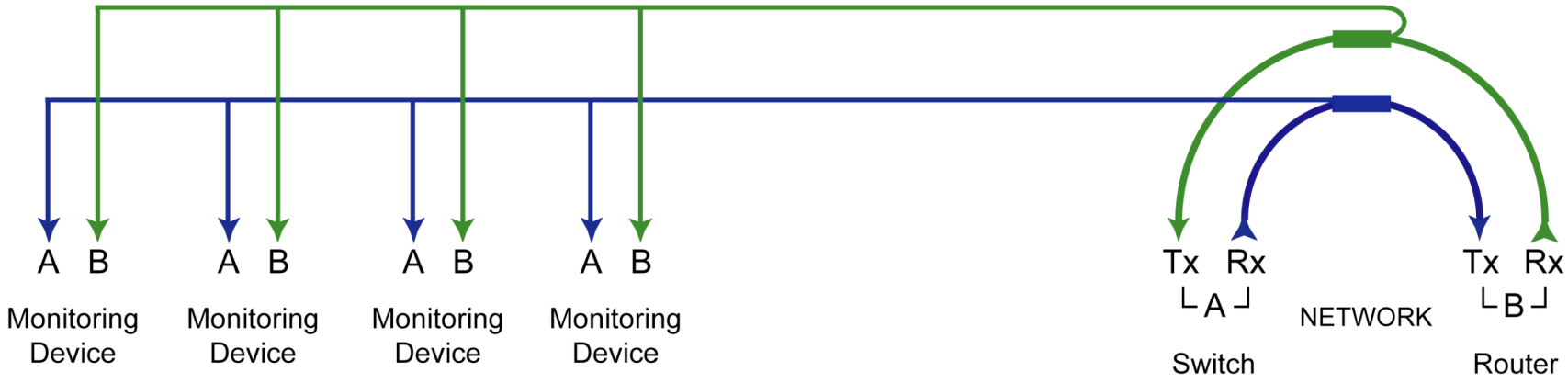
Example: On a 100 Mbps link, Side A is at 30 Mbps and Side B is at 50 Mbps. The NIC receives 80 Mbps of traffic (80% utilization), so no memory is required for the monitoring device NIC to process all full-duplex traffic.



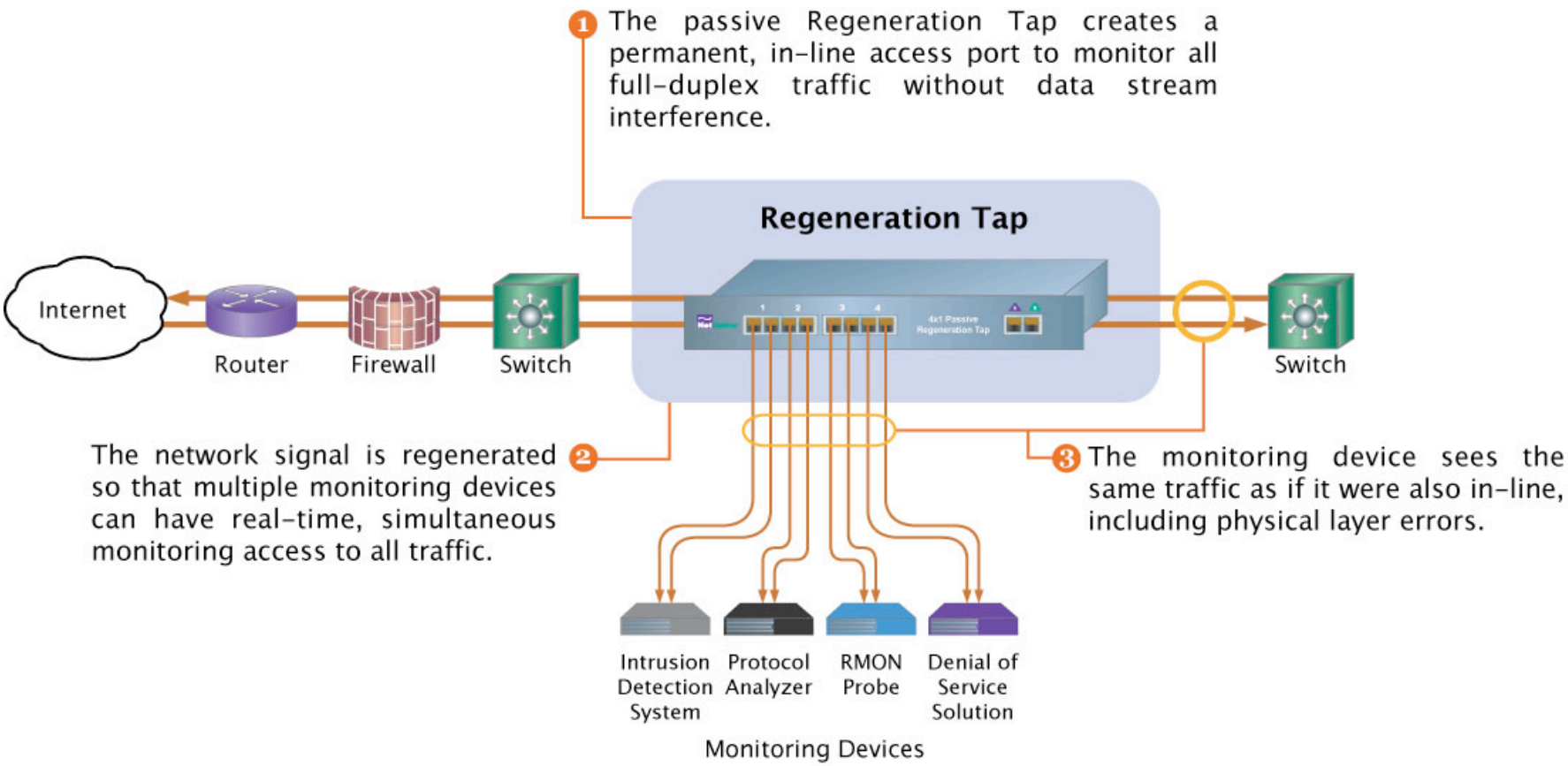
In-line Regeneration Taps

Allows passive access to a single link with multiple monitoring devices.

Data Flow in an In-line Regeneration Tap



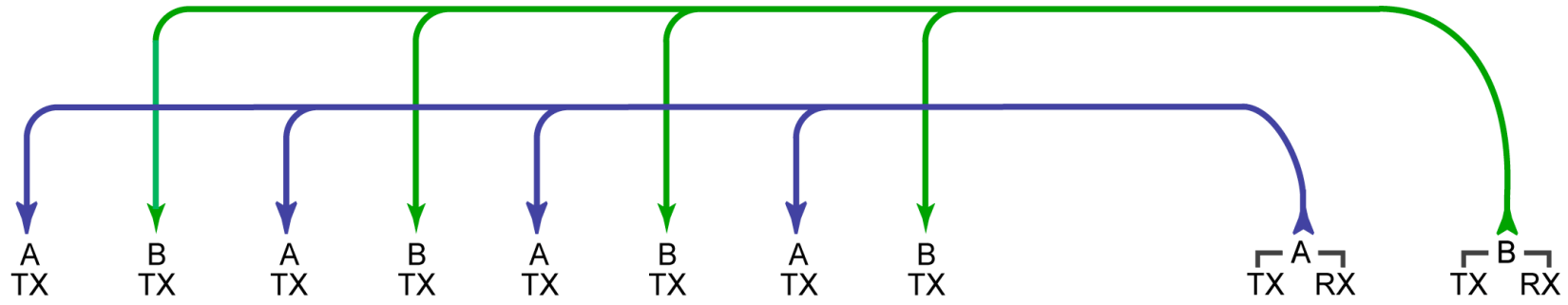
Regeneration Taps



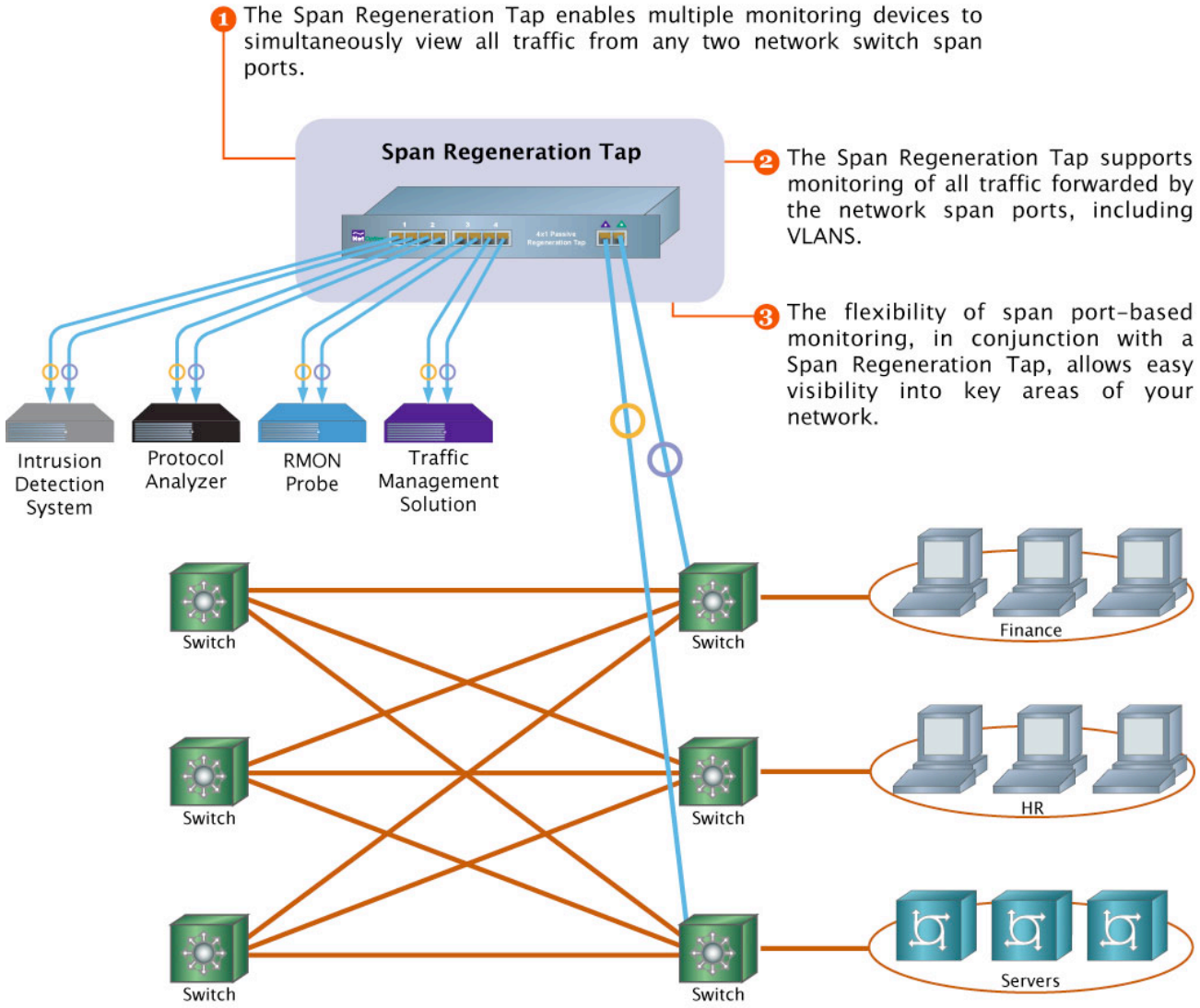
Span Regeneration Tap

Allows access to two separate Network Switch Span Port sessions with multiple monitoring devices.

Data Flow in an Span Regeneration Tap



Span Regeneration Tap



Section 2 Summary

Simple Taps

- Inexpensive passive monitoring with 100% visibility

Aggregation Taps

- Full-duplex monitoring to a single NIC
- One or two Monitor Ports

Regeneration Taps

- Solve access contention with multiple Monitor Ports

Features to look for:

- Full-duplex monitoring for all fiber and copper interfaces
- Dual power supplies
- Zero Delay
- Link Fault Detection

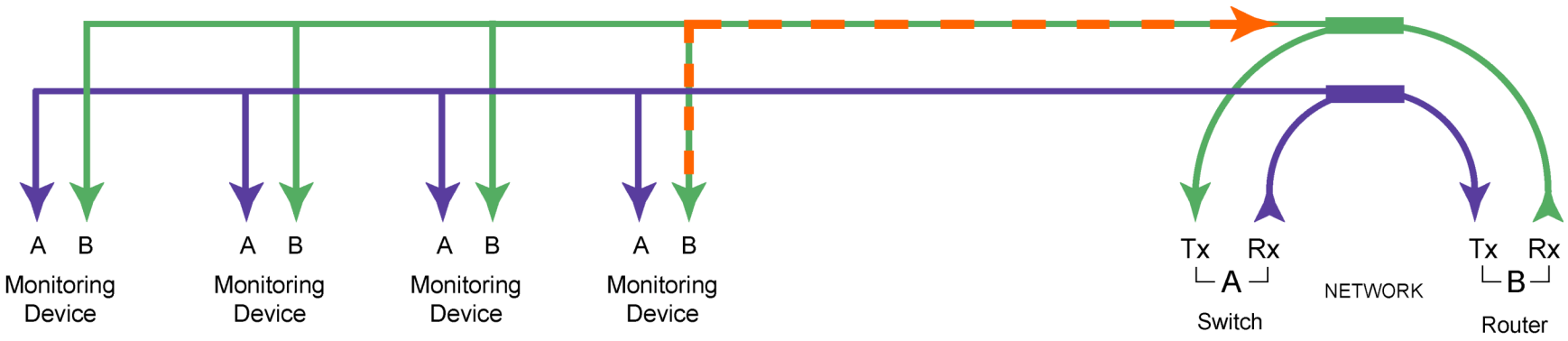
Active Response
&
Bypass Switches

Active Response Taps

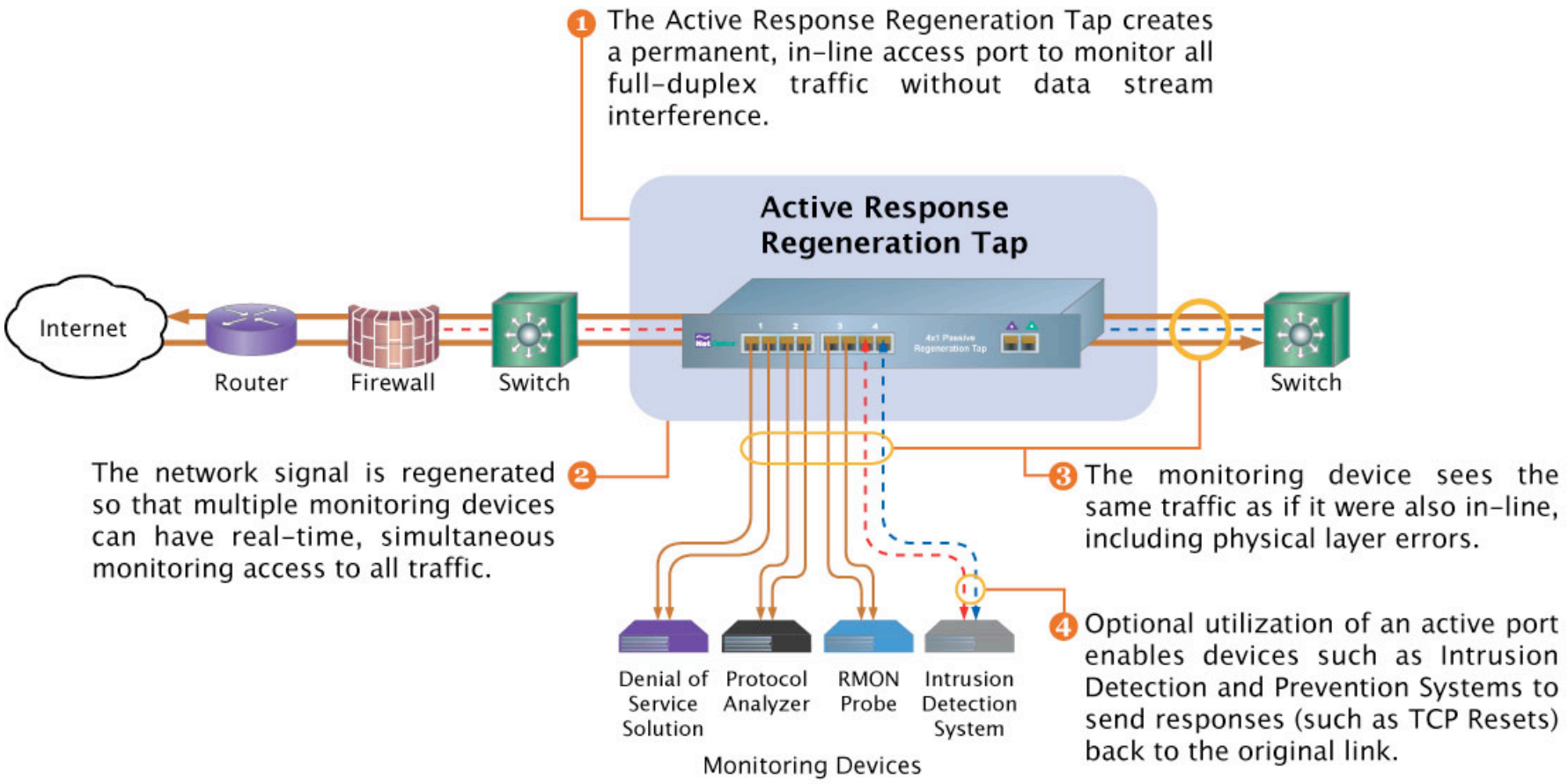
Passive network access with the option to inject responses, such as a TCP reset, into the network. Gives you the option to set one port to support bi-directional traffic.

Active Response Taps reduce the number of network ports (NICs) required for active response functionality.

Data Flow in an Active Response Regeneration Tap

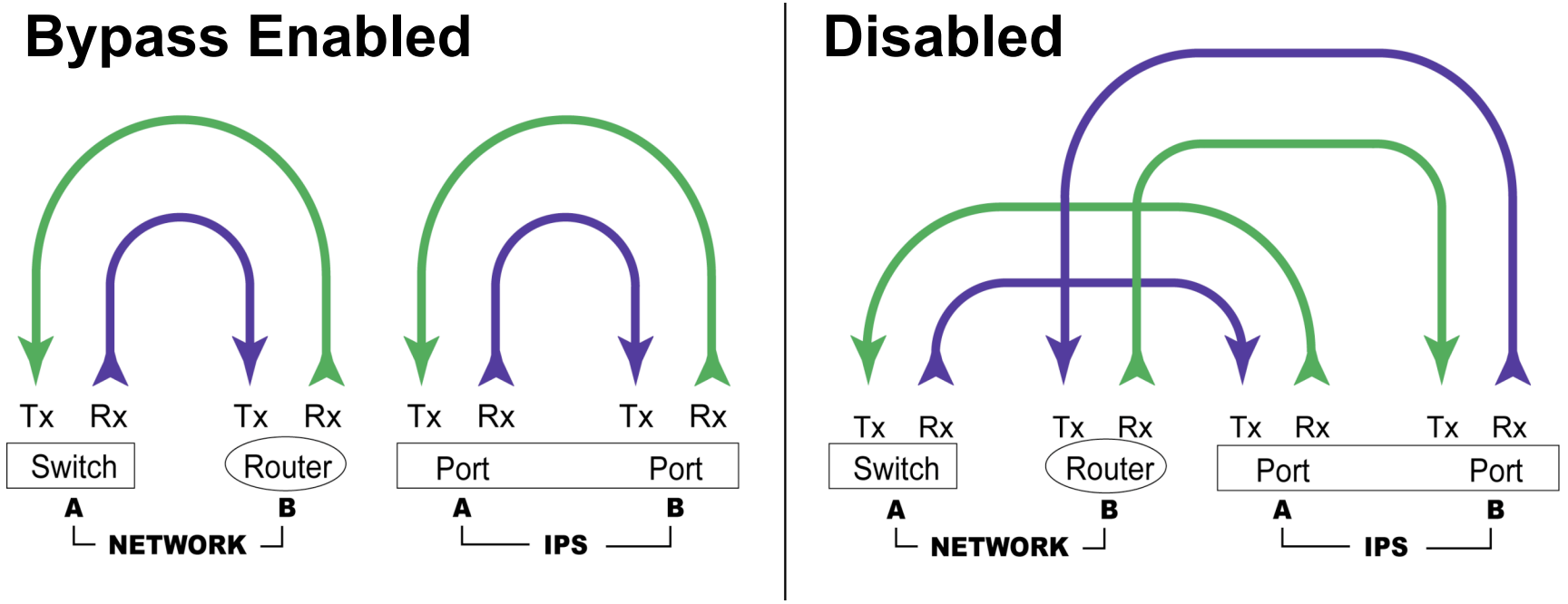


Active Response Taps

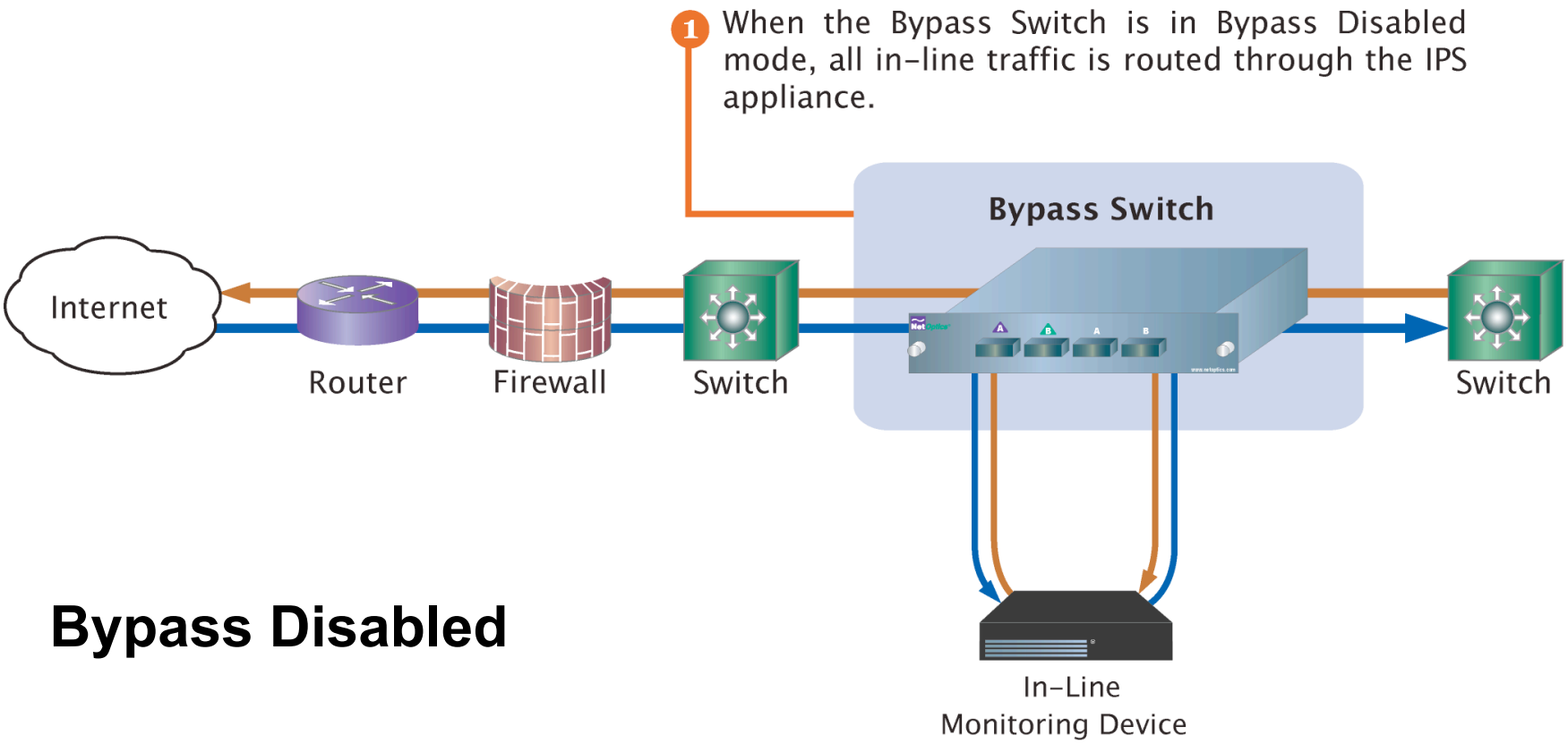


Bypass Switches

Bypass Switches are specialized Taps that provide fail-safe link protection when you connect in-line devices such as Intrusion Prevention Systems (IPS) to your network. Bypass Switches enable appliances to be inserted or removed without downtime, eliminating risks from hardware failure.

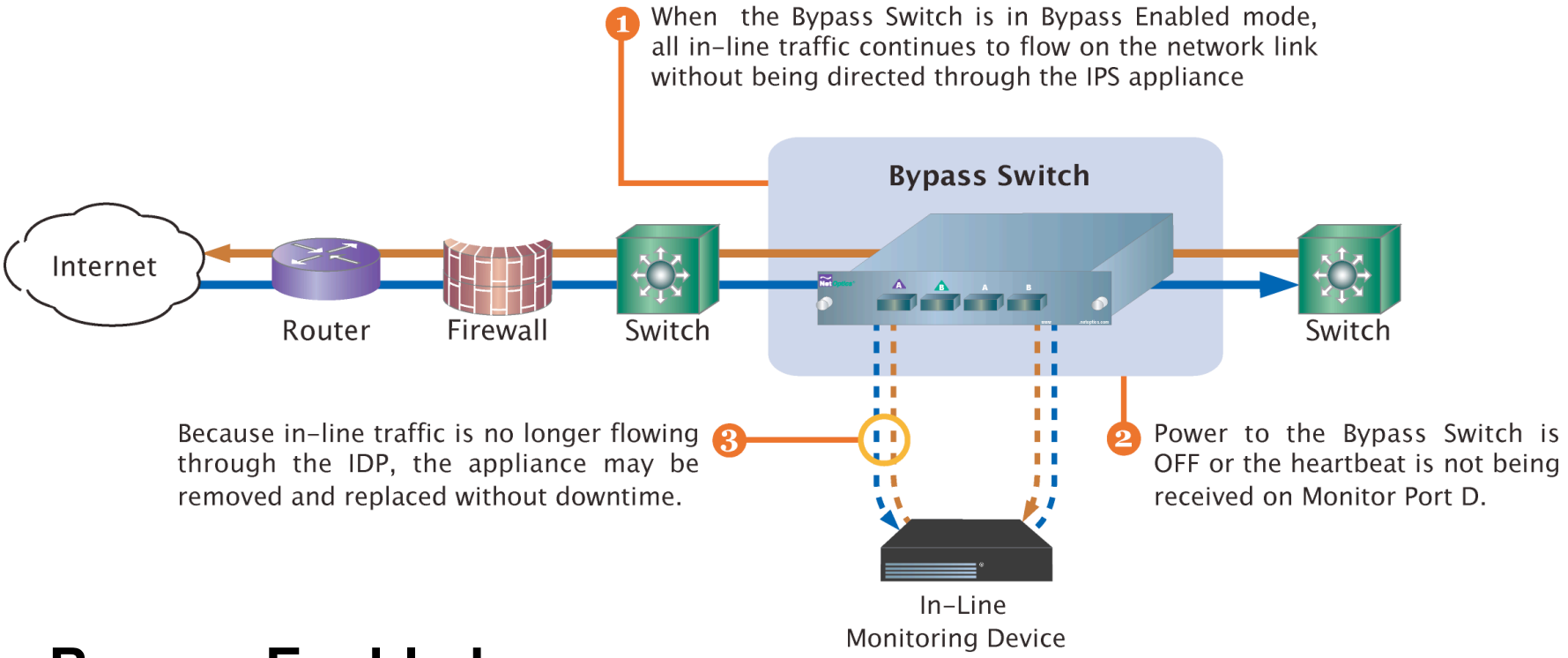


Bypass Switches



Bypass Disabled

Bypass Switches



Bypass Enabled

Section 3 Summary

Active Response

- Available in 10/100 Taps & Regeneration Taps
- Ability to inject data into the network for TCP Resets
- Creates a 2-way monitoring port

Power-loss Bypass Switch

- Shares the same power source as the in-line device
- Preserves link when power to the in-line device is off

Bypass Switch with Heartbeat

- Sends a heartbeat packet through the in-line device
- Preserves the link when the in-line device fails
- Protects against power, link, and application failure

Section 4

Link Aggregators And Matrix Switches Leveraging Assets

Leveraging Assets

Network Professionals are faced with increasing challenges:

- Network complexity creates the potential to miss critical data
- Too few access point to use network equipment and monitoring tools efficiently
- Limited budgets drive innovation for greater efficiency of existing equipment

For a Defensible Network you need to:

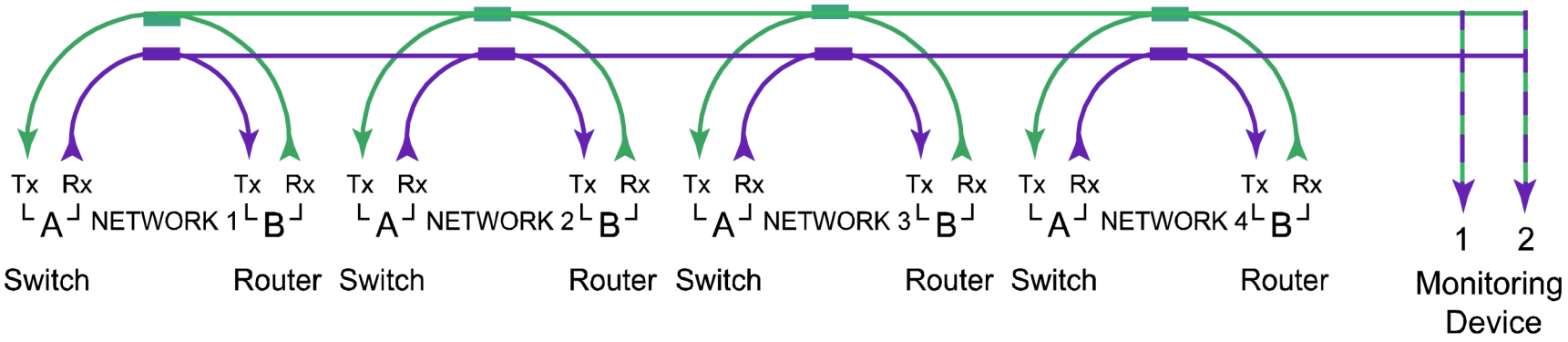
- Monitor 24/7
- Use tools simultaneously
- Be proactive
- Access all links

What can you do to maximize the usefulness of the tools you already have?

In-line Link Aggregator Taps

Provide permanent access when you need to monitor multiple 10/100 links with one GigaBit device. Four 10/100 network ports to GigaBit monitor port will not drop packets even when network ports are at maximum bandwidth.

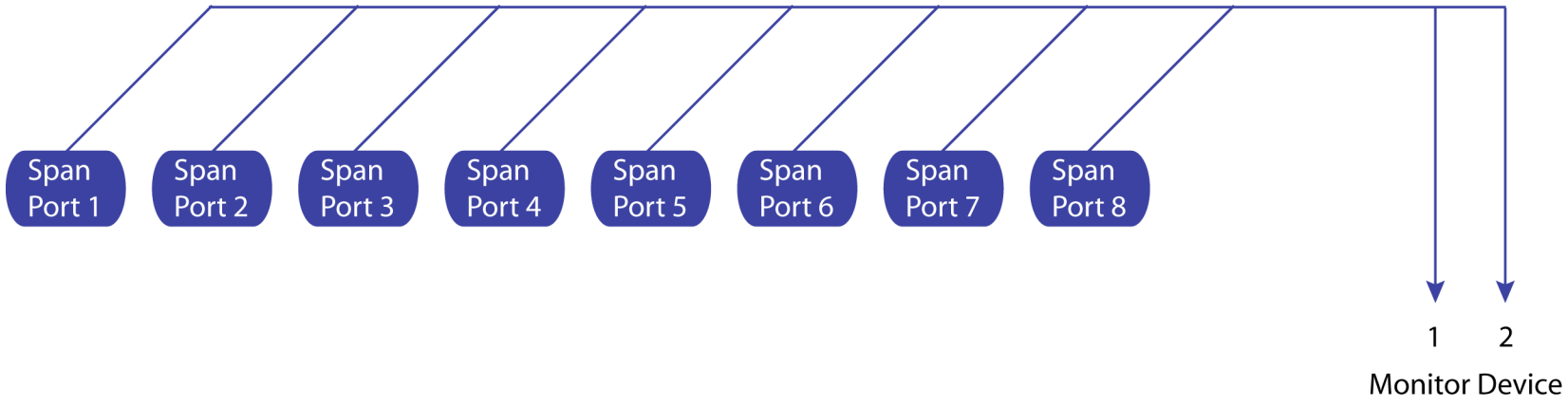
Data Flow in an In-Line Link Aggregator Tap



Span Link Aggregator Taps

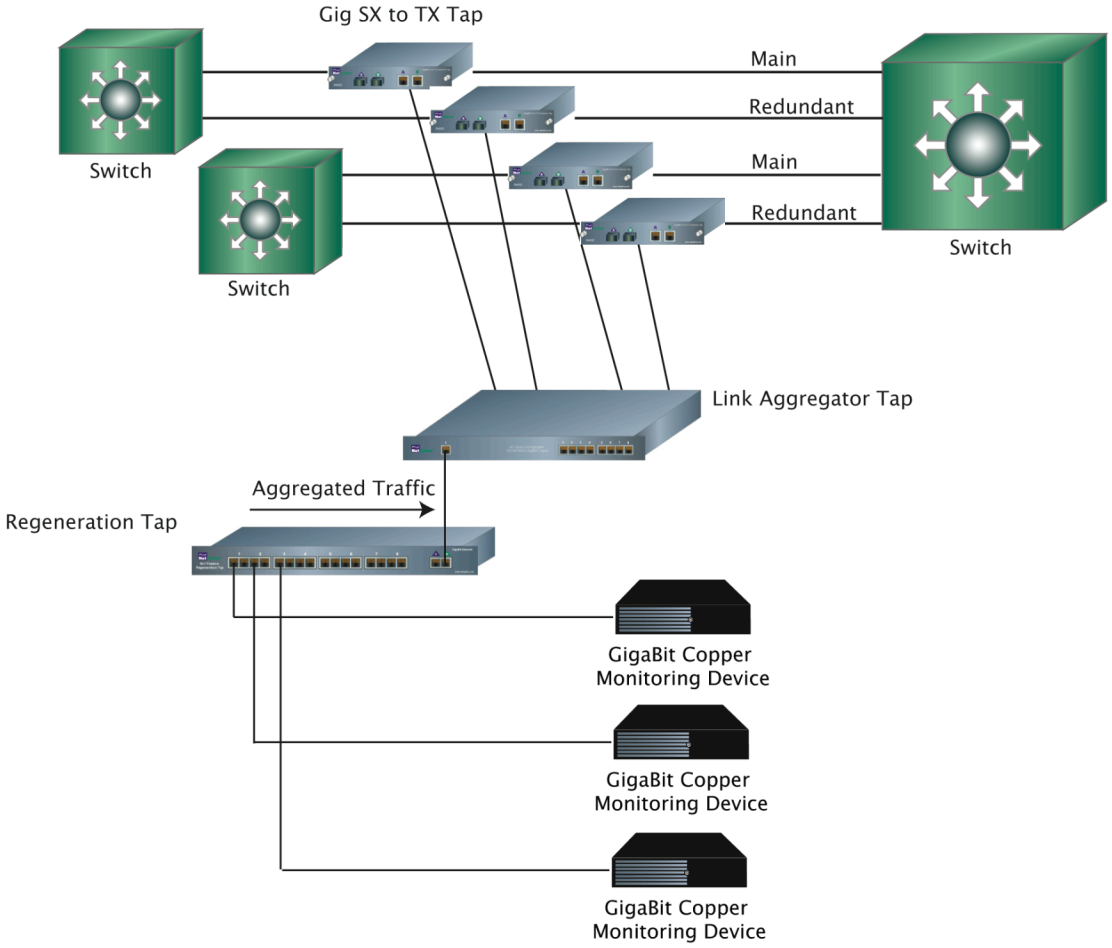
Span Link Aggregator Taps extend the reach of GigaBit monitoring devices to traffic from multiple Span ports. Aggregating Span traffic from multiple switch Span port greatly increases the Span traffic covered by your monitoring device.

Data Flow in an Span Link Aggregator Tap



Case Study 1

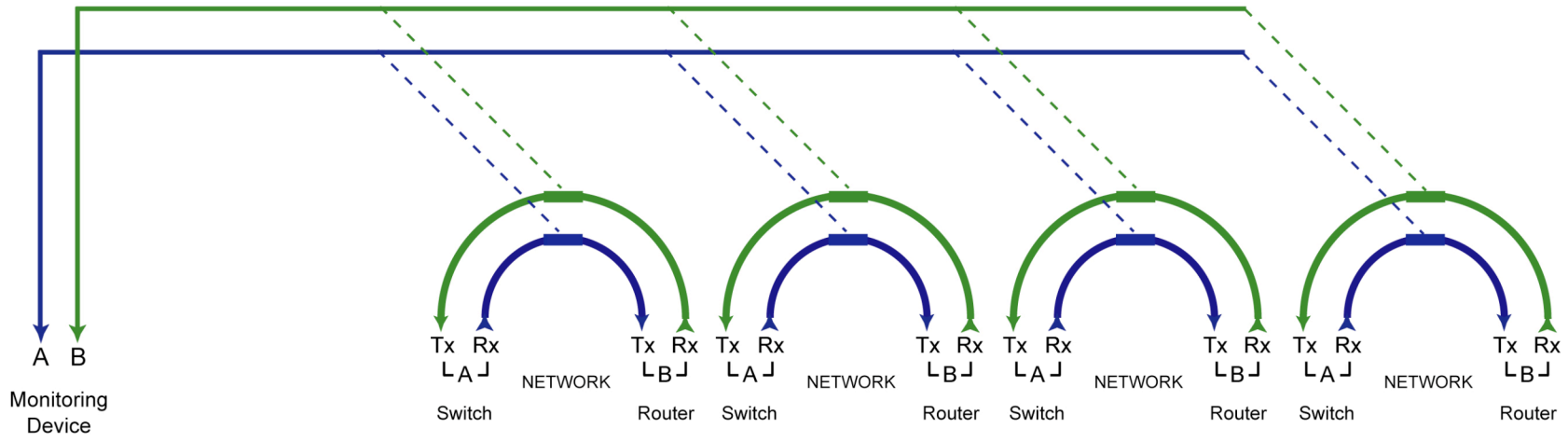
Goal: Convert fiber to copper, aggregate links and regenerate aggregated traffic for multiple monitoring devices.



In-Line Matrix Switches

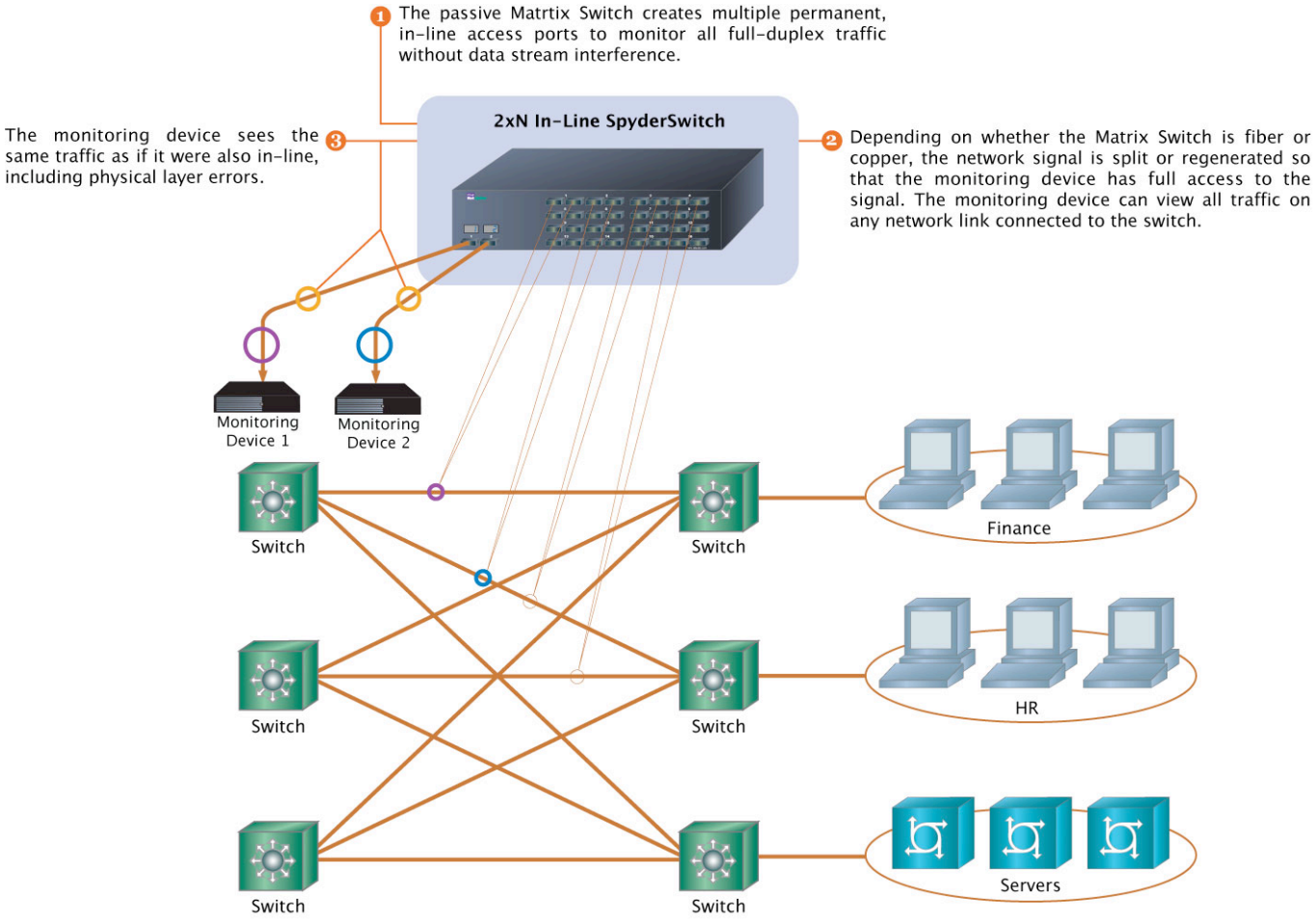
The physical layer connections through a matrix switch eliminates the need to reconnect and reconfigure analyzers for each new monitoring task. This flexibility improves ease of use and return on investment.

Data Flow in an In-Line Matrix Switch



Matrix Switches

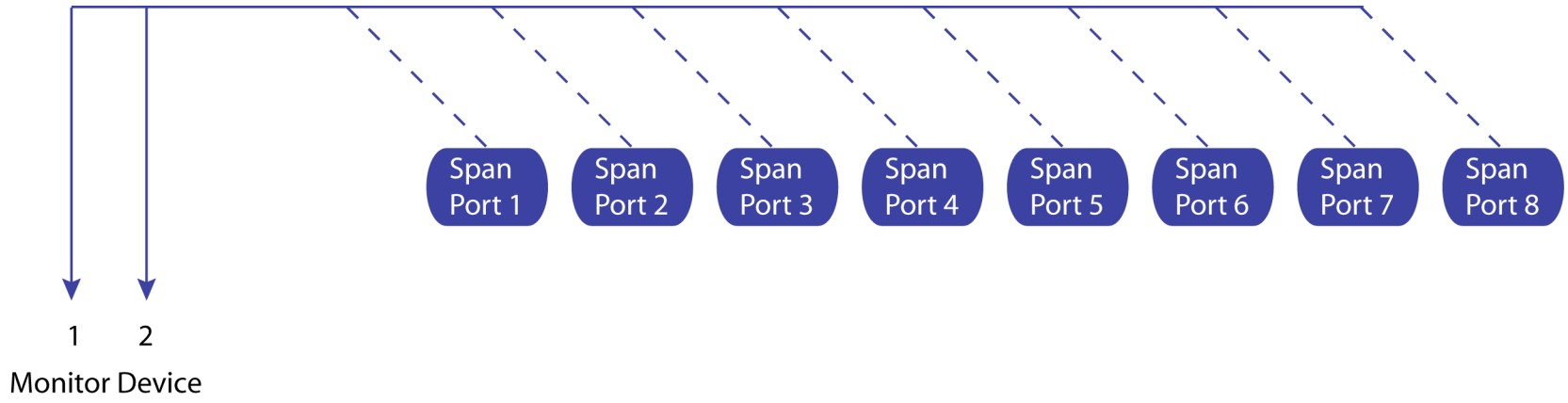
Enhance LAN visibility by providing access across multiple network links for one or two distributed analyzers.



Span Matrix Switches

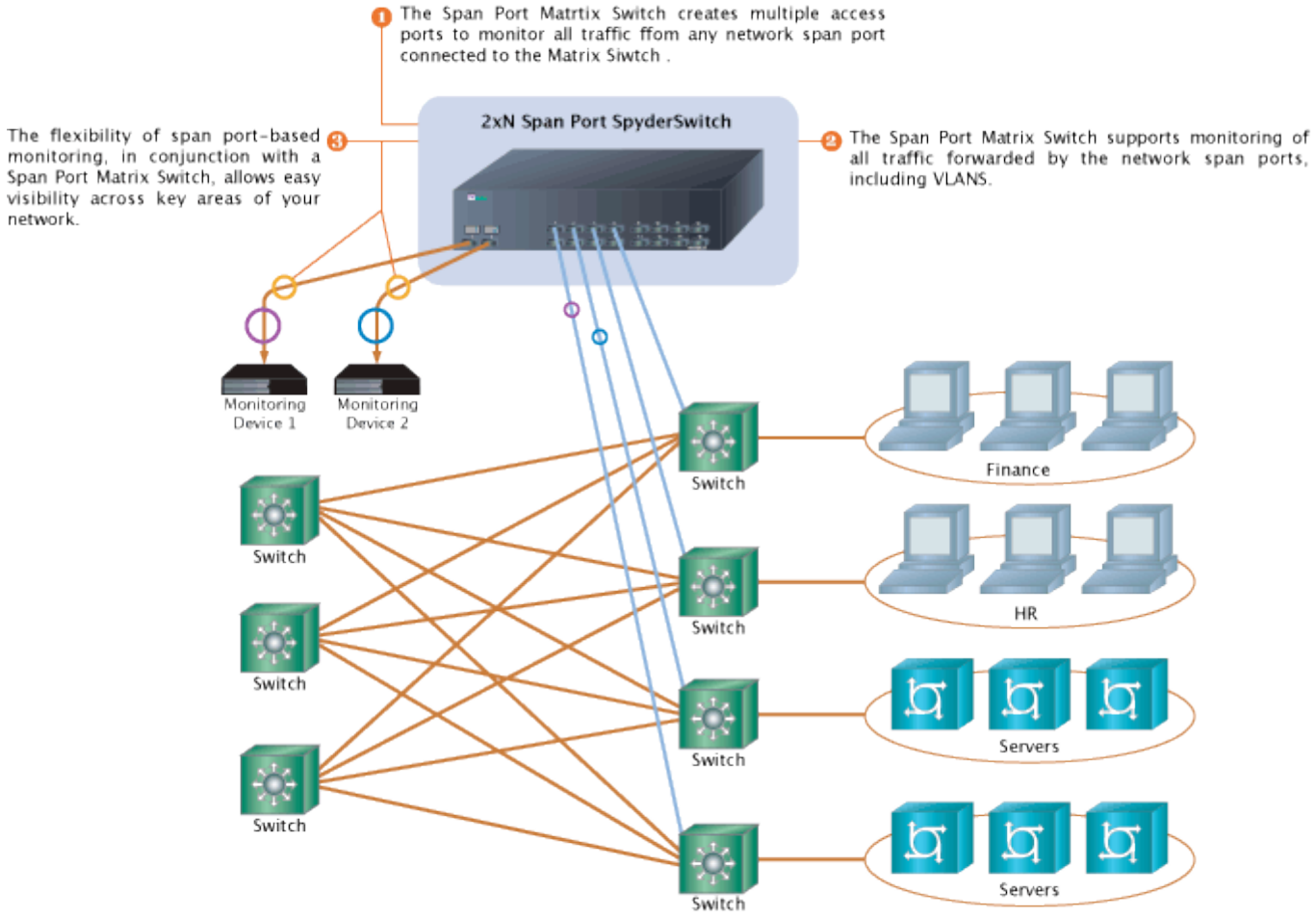
The Span matrix switches support simultaneous passive monitoring of Span ports connected to the matrix switch, each with a separate distributed analyzer. Monitored Span ports can be selected statically, for automatic roaming, or for a custom monitoring pattern.

Data Flow in a Span Matrix Switch



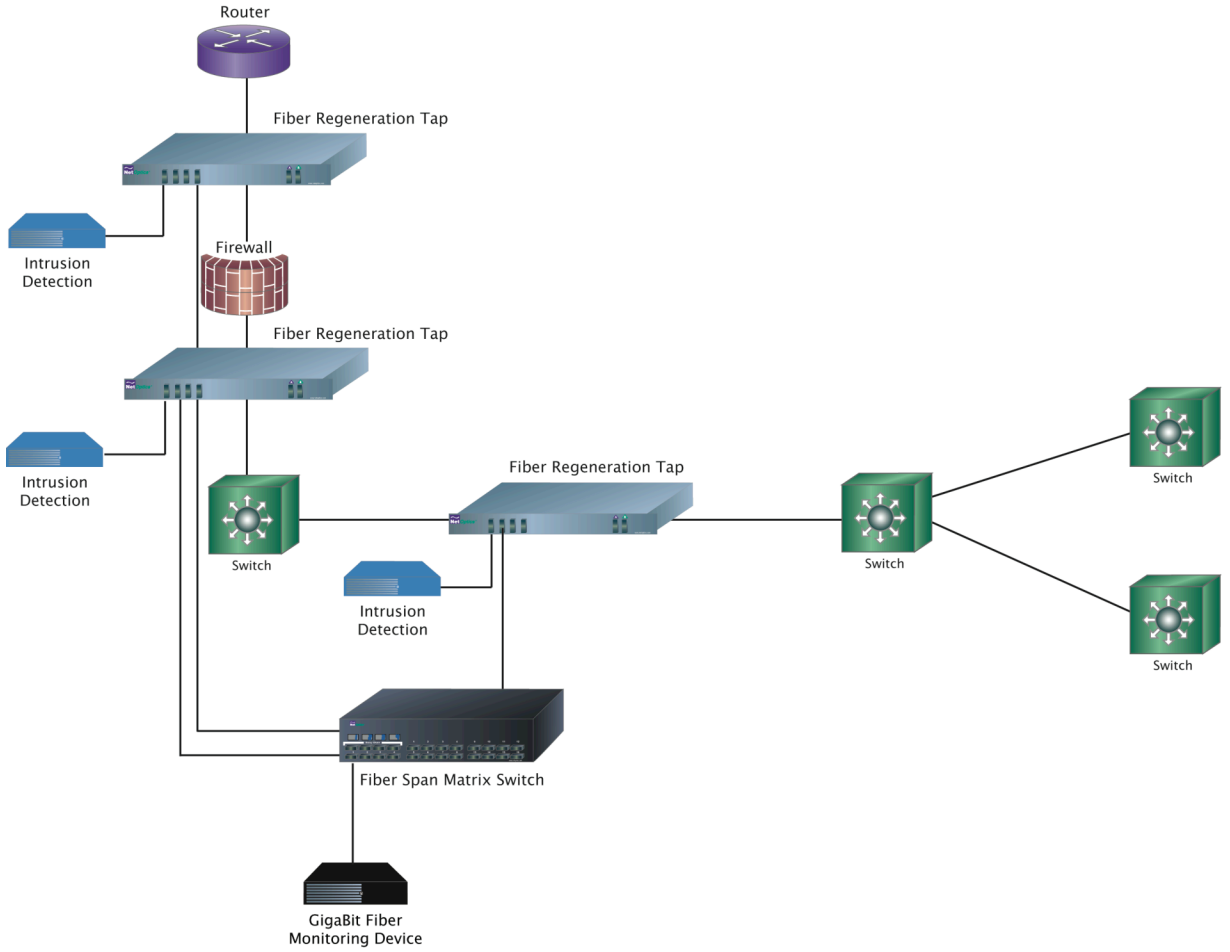
Span Matrix Switches

Enhance visibility by providing access to multiple network switch span ports for one or two distributed analyzers.



Case Study 2

Goal: Gain visibility to critical network links for a protocol analyzer using existing regeneration taps.



Section 4 Summary

Link Aggregator

- Aggregate up to (8) Span sessions to 1 GigaBit NIC
- Aggregate up to (4) 10/100 full-duplex links to 1 GigaBit NIC
- Available in Single/Dual monitor ports
- Monitor ports can be copper/fiber or a combo of 1 each

Matrix Switch

- In-Line Matrix Switches use Tap technology to provide complete cross-link visibility without data stream interference
- Span Port Matrix Switches Serve as end-station monitoring, do not split the signal, and can be daisy chained for doubled or tripled coverage
- Management software provides control over which links are monitored, including the ability to program and save custom monitoring patterns
- Expand coverage of your monitoring device
- Add scalability to your monitoring solution

Section 5

Taps with Intelligence and Remote Access

Intelligence Defined

Information - Gives a look into network health.

- Displays link utilization rates and peaks without having to install more expensive network analysis devices

Security and Control - the ability to control the Tap is built-in.

- Turn on/off the management and monitoring ports
- Turn on/off the front panel display

Remote Access and Management

- Access a Tap with a Web browser and SNMP tools

Intelligent Tap Management

Information

- Real time utilization levels for each side of link traffic
- Size and time of the greatest traffic peaks
- SNMP traps for system, link, power, and threshold
- Counters for total packets, bytes, CRC errors, collisions, and more
- Status for system, link, and power

Security and Control

- Turn off Management and Monitor Ports
- Set utilization alarm thresholds
- Reset statistics counters and peak data
- Turn off LCD information

Intelligent Tap Summary

- Creates the pervasive network awareness required to build a defensible network
- Baseline information from the Tap allows network managers to deploy security and monitoring devices more effectively over more links
- Scalable system provides more flexibility in network infrastructure for no additional cost!
- Efficient management of multiple Intelligent Taps from a single location

Additional Information

For more information please visit
www.netoptics.com
ts-support@netoptics.com

Joy Weber
Senior Technical Specialist
Joy@netoptics.com
408-737-7777