WHITEPAPER

Protect OT Network Perimeter Integrity

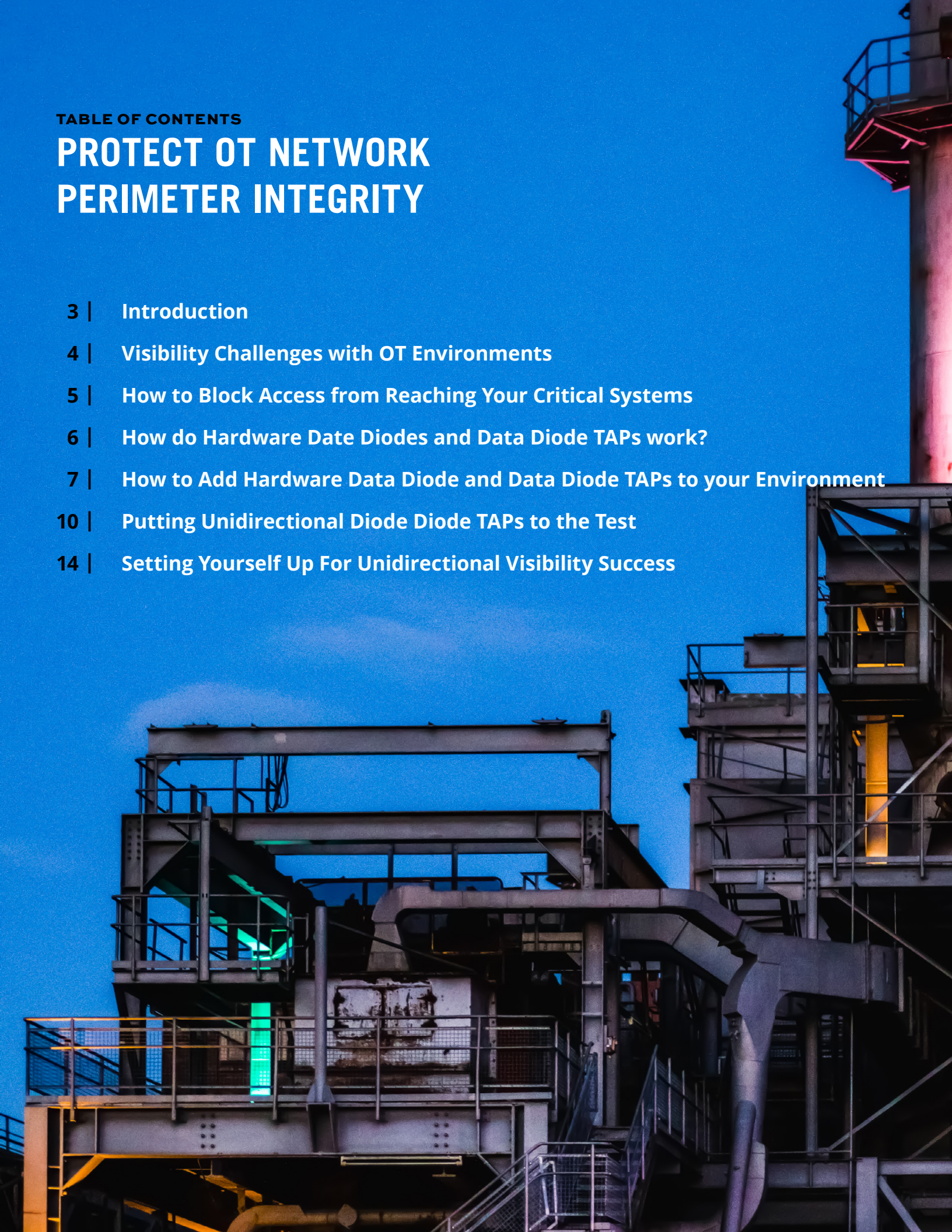
How to Secure Your Network with Unidirectional Hardware-enforced Data Diodes and Data Diode TAPs

GARLAND TECHNOLOGY

See every bit, byte, and packet®

TABLE OF CONTENTS

PROTECT OT NETWORK PERIMETER INTEGRITY



INTRODUCTION

Today's critical infrastructure landscape makes up the fundamental building blocks of the connected world we live in. From the basic communication we enjoy through WiFi, internet and telephones to resources we may take for granted like energy, water, manufacturing, and transportation systems.

Even our national security, such as the Department of Defense (DoD) and various government agencies in the US and EU, rely on similar operational technology (OT) environments. This critical infrastructure provides constant and reliable resources for our society, and it must be protected at all costs.

OT is the New Frontier for Cybersecurity Threats

In the initial draft of the NIST Special Publication (NIST SP 800-82r3 ipd) "Guide to Operational Technology," the authors describe a variety of precautions that must be taken when introducing trusted IT cybersecurity protections to OT environments. Where IT networks work to prevent cyber attacks that cause loss of data and financial losses, OT network operators must protect against loss of life and dangers to public health. Understanding the differences between IT and OT networks is the first step in implementing a cross-functional approach to solutions and personnel.

In fact, the convergence of modern OT and IT environments and its goal to improve operations efficiency, performance, and quality of services is unfolding rapidly. This convergence is creating new cybersecurity challenges that must be addressed. Pushing organizations across the industrial spectrum to re-evaluate their network visibility to address these challenges is another critical step to tackling security challenges.

This vulnerability was illustrated recently at Bridgestone Americas and Dole. Bridgestone halted production at its tire manufacturing facilities in North and South America after disconnecting its plants from the network to contain the impact from a cyber attack. Likewise, Dole temporarily shutdown production and stopped shipping to supermarkets to deal with a cyber attack to its network. Both examples drive home the reality that IT and OT networks are interconnected and one can easily create a vulnerability for the other.

VISIBILITY CHALLENGES WITH OT ENVIRONMENTS

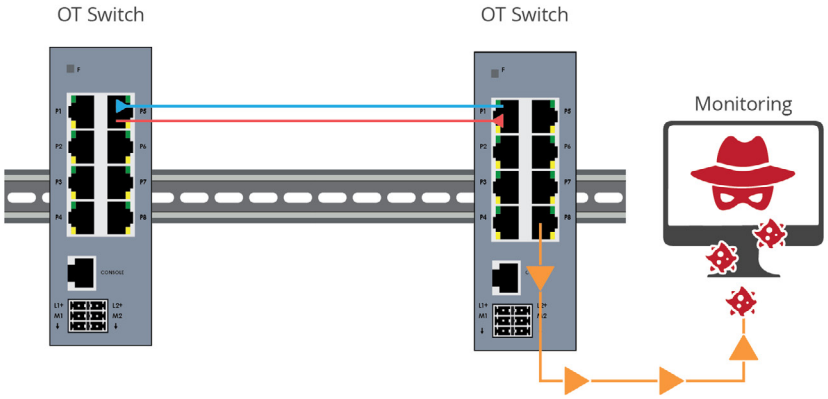
Some OT environments face challenges protecting network segments from incoming threats by way of the network infrastructure designed to protect them. These situations require a one-way data transfer between segments or facilities. Unidirectional or one-way data flow is designed to secure OT networks from external threats and maintain business continuity, adhering to OT cybersecurity compliances:

- International Society of Automation (ISA)/IEC 62443
- The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Standards - NERC CIP v5
- NIST Cybersecurity Framework
- EU's NIS2 Directive
- Nuclear Regulatory Commission (NRC) cybersecurity guidelines - NRC Regulatory Guide 5.71

A common visibility use case is to route mirrored traffic from a SPAN port on the switch to a security or monitoring tool. Port mirroring, also known as SPAN (Switch Port Analyzer), is a designated port on a network switch that is programmed to mirror, or send a copy, of network packets seen on a specific port, where the packets can be analyzed.

- Provides access to packets for monitoring
- SPAN sessions do not interfere with the normal operation of the switch
- Configurable from any system connected to the switch

The concept is simple enough — the switch is already architected into the environment. Just hook up your security solution. Done. But many times the simplest path isn't the best path.



Top Challenges SPAN visibility poses include:

- SPAN takes up high value ports on the switch
- Some legacy switches do not have SPAN ports even available
- SPAN ports can drop packets, an additional risk for security and regulation solutions

The SPAN concept may have sounded easy because it was available, but after weighing packet loss and altered frames, additional SPAN security considerations include:

- Bidirectional traffic allows back flow of traffic into the network, making switch susceptible to hacking
- Administration/programming costs for SPAN gets progressively more time intensive and costly

In critical network deployments like OT environments, if using SPAN is the only option to connect security sensors then additional security measures should be taken.

HOW TO BLOCK REMOTE THREATS FROM REACHING YOUR CRITICAL SYSTEMS

ICS environments face challenges protecting critical network segments from incoming threats by way of the very network infrastructure designed to protect them. Most OT and IT network environments send out-of-band Ethernet packet copies to security and monitoring tools to analyze and respond to threats. Many visibility architectures or fabrics flow this out-of-band traffic from the separate facilities to a centralized or enterprise network for this analysis. These IT solutions and integrated systems, connect the network to the internet, indirectly exposing this once siloed infrastructure to outside vulnerabilities and threats.

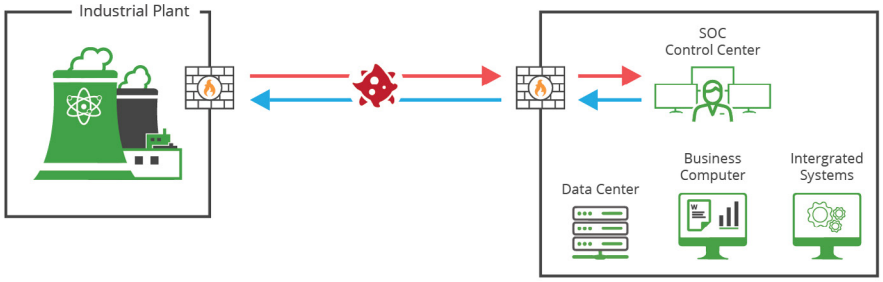


Diagram 1 illustrates how malicious activity being transmitted between different facility segments, through bidirectional traffic, can expose the network.

To address these challenges, a one-way data transfer between segments or facilities may be required. In addition to modern OT/IT security tools, such as firewalls, intrusion detection systems (IDS) and Security information and event management (SIEM), there is one piece of hardware that is quickly becoming a staple of ICS critical infrastructure — data diodes. Unidirectional or one-way data flow in data diodes are designed to secure OT networks from external threats, eliminating inbound data flow and ultimately outside threats to OT network segments, while providing the needed out-of-band data flow needed to monitor.

Hardware Data Diodes and Data Diode TAPs are useful and cost-effective solutions to help provide an additional layer of security in OT networks. There are situations where the use of SPAN/Mirror ports is still needed for visibility in an OT network. In these instances, it is best practice to connect the SPAN/Mirror port to a hardware Data Diode to pass the mirrored data onto the monitoring and security sensors. Using hardware Data Diodes eliminate bidirectional traffic flow ensuring that no data is passed back into the Switch Mirror port.

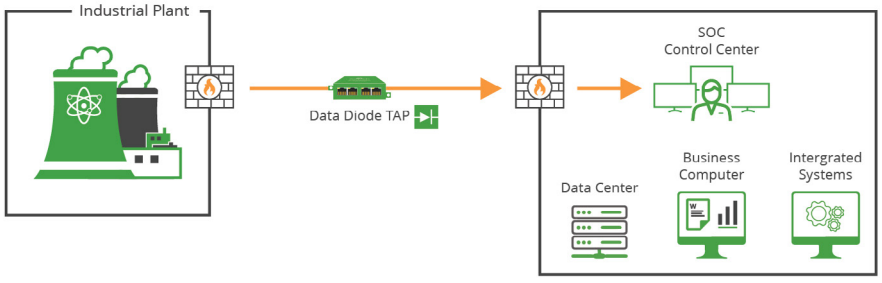


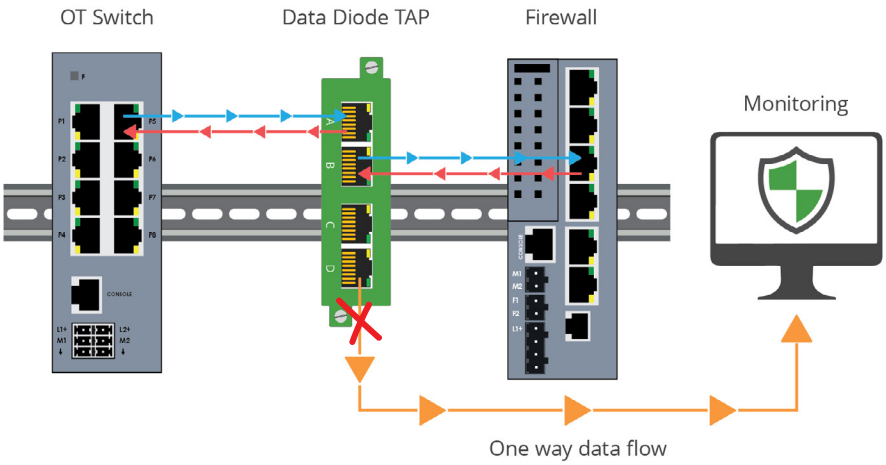
Diagram 2 illustrates how unidirectional traffic helps ensure monitoring traffic being transmitted from different facility segments remain secure.

Data diodes can be found most commonly in high security environments, such as federal defense and Industrial IoT, where they serve as connections between two or more networks of differing security classifications. This technology can now be found at the industrial control level for such facilities as nuclear power plants, power generation and safety critical systems like railway networks.

HOW DO DATA DIODE TAPS WORK?

Data diode TAPs are a purpose-built network hardware device that allows raw data to travel only in one direction. Data diode TAPs can be used as a traffic enforcer, guaranteeing information security or protection of critical digital systems, such as industrial control systems, from inbound cyber attacks.

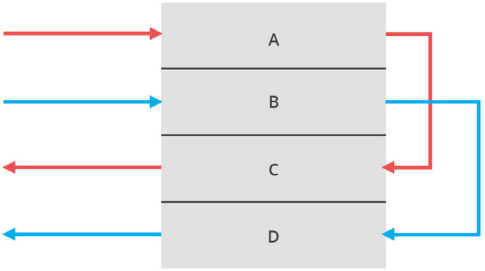
Diagram 3 illustrates how a data diode TAP is placed in a network segment, securing the traffic from the destination.



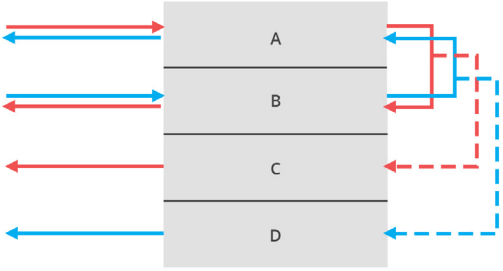
A network TAP creates an exact copy of both sides of the traffic flow, continuously 24/7/365 and does not drop packets, introduce delay, or alter the data. They are either passive or "failsafe," meaning traffic continues to flow between network devices if power is lost or a monitoring tool is removed, ensuring it isn't a single point of failure. Data Diode TAPs offer the same high quality visibility as Network TAPs, with the added security that the out-of-band traffic does not find it's way back to the network.

Different from common software based Data Diode gateways in the industry, these are hardware based. This means there is no complicated software to configure or the added risk of software failure. Data Diode TAPs are plug and play and require no management.

These devices take in traffic through the interface ports A and B. The data is flowing from Port A to Port C, but there is no connection from Port C to Port A. This also applies to Port B and Port D. This means that there is no data that can flow from Port C to Port A/B or from Port D to Port A/B.



This diagram depicts a 4 port (A, B, C, D). The Data Diode SPAN TAP shows the traffic of portA flow out of portC and PortB flow out of PortD.



This diagram depicts a 4 port (A, B, C, D). The Data Diode Network TAP shows portA flow out of portB, and sends a copy out of portC and PortB flow out of PortA, and sends a copy out of portD.

HOW TO ADD DATA DIODE TAPS TO YOUR ENVIRONMENT

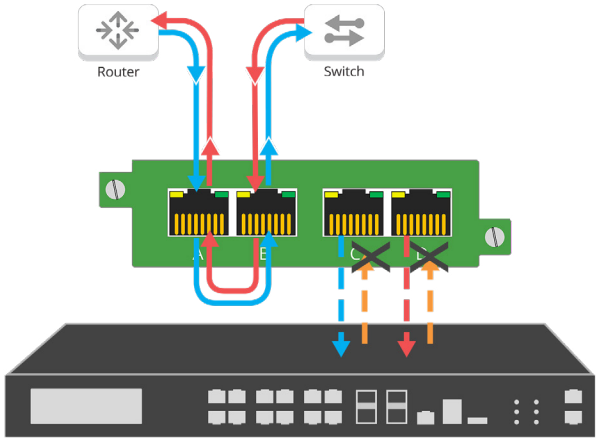
During any deployment there are different factors that go into your connectivity strategy and design. When ensuring one-way security, keep in mind the 3 main hardware based data diode TAPs: Data Diode Network TAPs, Hardware Data Diodes, and Aggregator TAPs.

Each of these address a specific visibility need for optimizing visibility for your network performance and security, but all have Garland Technology's hardware based Data Diode functionality, to keep your network traffic secure.

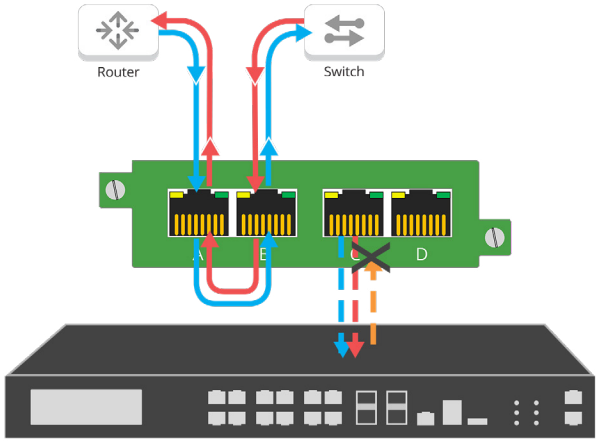
Data Diodes Network TAPs

Data Diodes Network TAPs sit in a network segment connecting two appliances like a network switch and a firewall, that support the critical link. The Data Diode TAP sends a unidirectional copy of that traffic to the out-of-band monitoring tools, the link between the two appliances is unaffected. There is no physical connection between the Data Diode monitoring ports and the network, eliminating any possible intrusion from the destination.

- Protect the source of data streams between network segments that have different security requirements
- Physical hardware separation guarantees unidirectional traffic between network segments
- Supports tap 'breakout,' aggregation, regeneration / SPAN mode



In this scenario you are able to TAP one link and provide unidirectional tap 'Breakout" copies of traffic, without packet injection back onto the network.



In this scenario you are able to TAP one link and provide unidirectional TAP copies of traffic aggregated to one or two ports, without packet injection back onto the network.

Product Details

Data Diode Network TAP
10M/100M/1000M (1G) Unidirectional data diode circuitry design
Model # PT100
Model # P1GCCB
Model # P1GCCAS
Model # P1GMCA
Model # P1GMSA
Model # P1GSCA
Model # P1GSSA
Model # P100FXCA

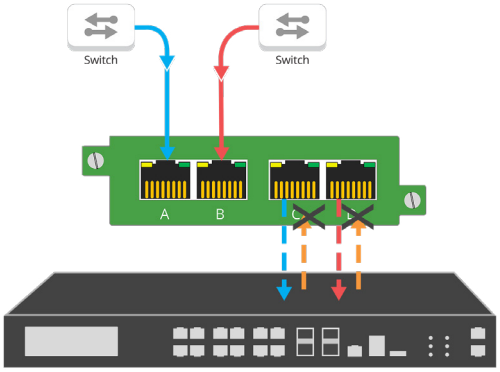
Hardware Data Diodes

Hardware Data Diodes provide network traffic for out-of-band monitoring, specifically designed not to send traffic back onto the network. These purpose-built network hardware devices enforce one-way data flow for switch SPAN links with physical hardware separation, guaranteeing protection of critical digital systems, such as industrial control systems (ICS), from inbound cyber threats.

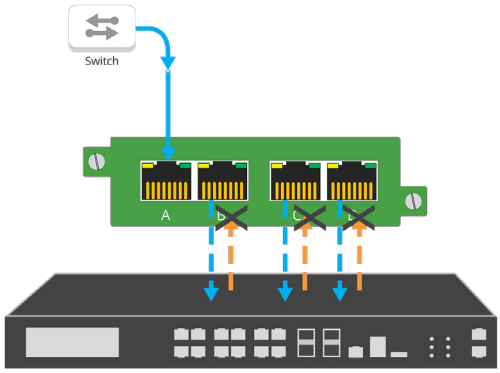
- Protect the source of data streams like switch SPAN ports between network segments that have different security requirements
- Physical hardware separation guarantees unidirectional traffic between network segments
- Supports regeneration / SPAN mode
- Ensures any ethernet packet flows in one direction out the hardware Data Diodes' monitoring ports

Product Details

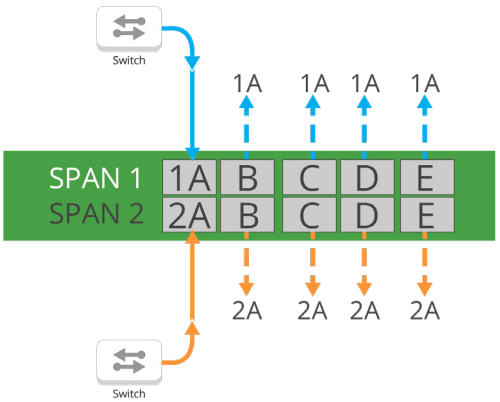
Data Diode SPAN TAP
10M/100M/1000M (1G) Unidirectional data diode circuitry design
Model # P1GCCAS-Custom
Model # CTAP-P1GCCREG
Model # INT10G10SP1



In this scenario you are able to ensure 2 SPAN ports provide 1 copy of unidirectional traffic each, without packet injection back onto the network.



In this scenario you are able to ensure 1 SPAN port provides 1-3 copies of unidirectional traffic, without packet injection back onto the network.



In this scenario you are able to ensure 2 SPAN ports provide 1-4 copies of unidirectional traffic each, without packet injection back onto the network.

Aggregator TAP: Data Diodes

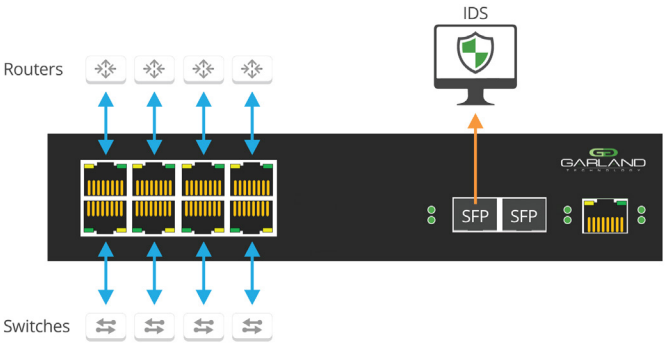
Aggregator TAP Data Diodes provide network traffic for out-of-band monitoring, specifically designed not to send traffic back onto the network. These purpose-built network hardware devices enforce one-way data flow from multiple network segments to a monitoring destination, with physical hardware separation, guaranteeing protection of critical digital systems, such as industrial control systems (ICS), from inbound cyber threats.

- Protect the source of data streams between network segments that have different security requirements
- Aggregate up to 4 TAP links to 1 or 2 monitoring ports
- Aggregate up to 8 SPAN Ports to 1 or 2 monitoring ports

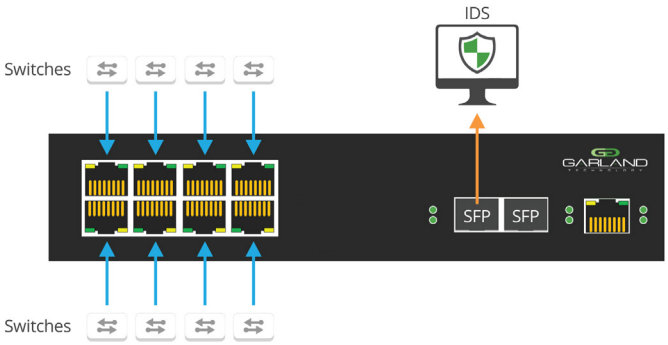
Product Details

AggregatorTAP: Data Diode
10M/100M/1000M (1G)
1U ½ rack | Aggregation & Regeneration | Unidirectional data diode circuitry design
Model # INT1G10CSA
Model # INT1G10CSA-DC
Model # INT1G10CSASP
Model # INT1G10CSASPDC

Provides a physically secure one-way communication path to the monitoring ports - securing SPAN.

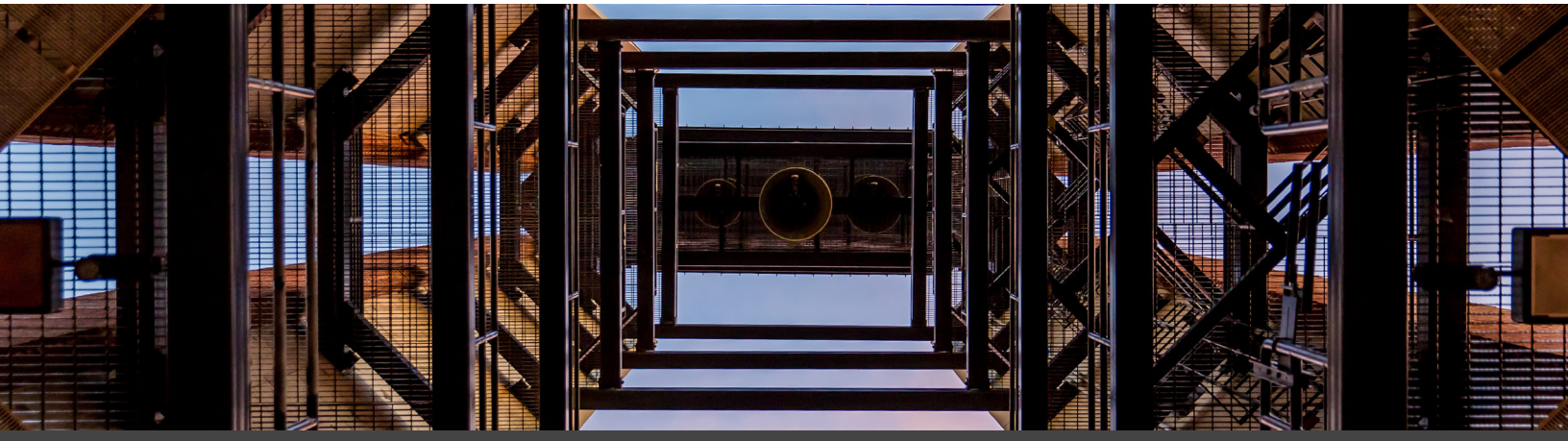


In this scenario you are able to TAP 4 links and provide unidirectional TAP copies of traffic aggregated to one or two ports, without packet injection back onto the network.



In this scenario you are able to ensure 8 SPAN ports provide copies of traffic aggregated to one or two ports, without packet injection back onto the network.

These specifically designed TAPs provide reliable visibility for 10/100/1000M networks and aggregate copies to one or two security sensors - helping centralize solutions. The hardware based data diode design ensures no Ethernet packets can physically be sent to the live Network TAP ports or SPAN ports via the monitoring ports on the TAP. Both monitoring ports cannot send any traffic back into the network ports of the TAP.



PRODUCT TESTING

PUTTING UNIDIRECTIONAL DIODE TAPS TO THE TEST

Commitment to Total Quality: Garland Technology ensures our unique testing and acceptance phase passes all quality checks. Since we don't believe sample testing provides an adequate level of oversight, we test every device with live network traffic before shipping to the client. Leading to an overall return rate is less than 0.5% and our first-time pass rate (FTPR) is 0%.

In security tests conducted to verify one-way data transfer, we set out to confirm if Garland Technology's Hardware Data Diode and Data Diode TAPs did not inject packets back into the network ports.

DATA DIODE TEST 1: 4 PORT

Connect **all** ports up to the test equipment.

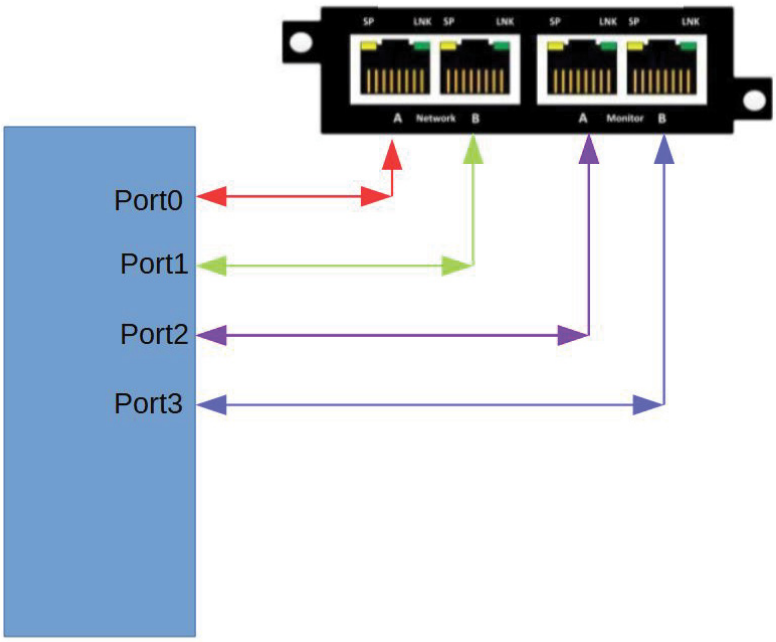
1. Send 1000 packets into port A and show that 1000 packets ONLY egress port C

2. Send 1000 packets into port B and show that 1000 packets ONLY egress port D

3. Send 1000 packets into port C and show that those packets are not allowed to flow through our box

4. Send 1000 packets into port D and show that those packets are not allowed to flow through our box

TEST SETUP



Xena Ethernet Tester

Test #1 – transmit 1000 packets from Xena port0.

Expected results = 1000 packets received on Xena port2 only.

Main Port Traffic Statistics

Name	TX (%	TX L1 (bit/s	TX L2 (bit/	TX (pps)	TX (bytes)	TX (packets)	RX (%)	RX L1 (bit/s)	RX L2 (bit/	RX (pps)	RX (bytes)	RX (packets)
P-3-0-0	0.000	0	0	0	4,447,393	1,000	0.000	0	0	0	0	0
P-3-0-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-2	0.000	0	0	0	0	0	0.000	0	0	0	4,447,393	1,000
P-3-0-3	0.000	0	0	0	0	0	0.000	0	0	0	0	0

Test #2 – transmit 1000 packets from Xena port1.

Expected results = 1000 packets received on Xena port3 only.

Main Port Traffic Statistics

Name	TX (%	TX L1 (bit/s	TX L2 (bit/	TX (pps)	TX (bytes)	TX (packets)	RX (%)	RX L1 (bit/s)	RX L2 (bit/	RX (pps)	RX (bytes)	RX (packets)
P-3-0-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-1	0.000	0	0	0	4,447,393	1,000	0.000	0	0	0	0	0
P-3-0-2	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-3	0.000	0	0	0	0	0	0.000	0	0	0	4,447,393	1,000

Test #3 – transmit 1000 packets from Xena port2.

Expected results = 0 packets received on any Xena port.

Main Port Traffic Statistics

Name	TX (%	TX L1 (bit/s	TX L2 (bit/	TX (pps)	TX (bytes)	TX (packets)	RX (%)	RX L1 (bit/s)	RX L2 (bit/	RX (pps)	RX (bytes)	RX (packets)
P-3-0-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-2	0.000	0	0	0	4,447,393	1,000	0.000	0	0	0	0	0
P-3-0-3	0.000	0	0	0	0	0	0.000	0	0	0	0	0

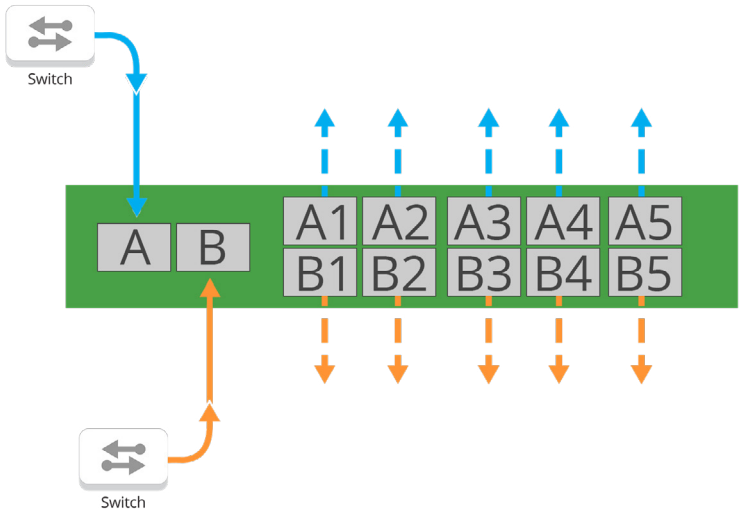
Test #4 – transmit 1000 packets from Xena port3.

Expected results = 0 packets received on any Xena port.

Main Port Traffic Statistics

Name	TX (%	TX L1 (bit/s	TX L2 (bit/	TX (pps)	TX (bytes)	TX (packets)	RX (%)	RX L1 (bit/s)	RX L2 (bit/	RX (pps)	RX (bytes)	RX (packets)
P-3-0-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-2	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-3-0-3	0.000	0	0	0	4,447,393	1,000	0.000	0	0	0	0	0

DATA DIODE TAP TEST 2: MULTI-PORT



All SFP+ ports are connected up to the test equipment.

1. Run 1000 packets into the top left port which is the input port.

- Show that all 1000 packets only egress the 4 ports to the right of that port.

2. Run 1000 packets into the bottom left port which is the input port.

- Show that all 1000 packets only egress the 4 ports to the right of that port.

3. Run 1000 packets into the 8 monitor ports and show that those packets are dropped clearly indicating that they are not allowed to flow through our box.

All (10) ten ports are 10G SFP+ cages.

All ports on the TAP are connected to the Xena 10G Test Set as shown in the table below:

Xena 10G Test Set Port Number	INT10G10SP1 Port Number
P-0-4-0	1A
P-0-4-1	1B
P-0-4-2	1C
P-0-4-3	1D
P-0-4-4	1E
P-0-5-0	2A
P-0-5-1	2B
P-0-5-2	2C
P-0-5-3	2D
P-0-5-4	2E

1. Transmit 1000 packets into Port 1A. All 1000 packets are only egressed out ports 1B, 1C, 1D, and 1E.

Main Port Traffic Statistics

Name	TX (%)	TX L1 (bit/s)	TX L2 (bit/s)	TX (pps)	TX (bytes)	TX (packets)	RX (%)	RX L1 (bit/s)	RX L2 (bit/s)	RX (pps)	RX (bytes)	RX (packets)
P-0-4-0	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-4-1	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-4-2	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-4-3	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-4-4	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-5-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-2	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-3	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-4	0.000	0	0	0	0	0	0.000	0	0	0	0	0

2. Transmit 1000 packets into Port 2A. All 1000 packets are only egressed out ports 2B, 2C, 2D, and 2E

Main Port Traffic Statistics

Name	TX (%)	TX L1 (bit/s)	TX L2 (bit/s)	TX (pps)	TX (bytes)	TX (packets)	RX (%)	RX L1 (bit/s)	RX L2 (bit/s)	RX (pps)	RX (bytes)	RX (packets)
P-0-4-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-1	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-2	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-3	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-4	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-0	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-1	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-5-2	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-5-3	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000
P-0-5-4	0.000	0	0	0	0	0	0.000	0	0	0	100,000	1,000

3. Transmit 1000 packets into each of the (8) eight monitor ports (1B, 1C, 1D, 1E, 2B, 2C, 2D, and 2E). All packets are dropped which shows that they are not allowed to flow through the TAP.

Main Port Traffic Statistics

Name	TX (%)	TX L1 (bit/s)	TX L2 (bit/s)	TX (pps)	TX (bytes)	TX (packets)	RX (%)	RX L1 (bit/s)	RX L2 (bit/s)	RX (pps)	RX (bytes)	RX (packets)
P-0-4-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-4-1	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-4-2	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-4-3	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-4-4	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-0	0.000	0	0	0	0	0	0.000	0	0	0	0	0
P-0-5-1	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-2	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-3	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0
P-0-5-4	0.000	0	0	0	100,000	1,000	0.000	0	0	0	0	0

Testing Conclusion

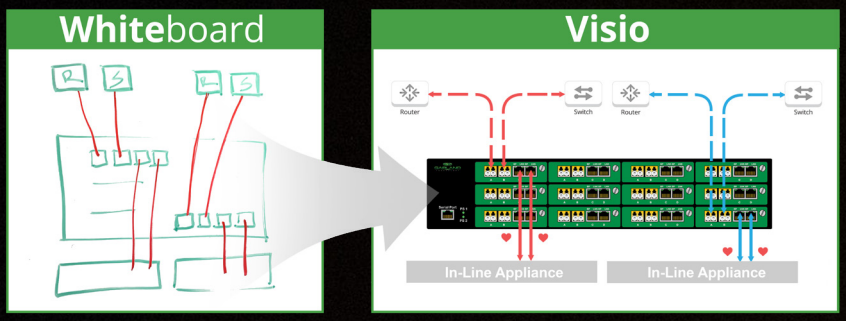
Testing concludes that the Garland Technology 4 Port and Multiport Data Diode TAPs are successful in allowing traffic unidirectionally (one way). This applies to our data diode portfolio, including: CTAP-P1GCCREG, INT10G10SP1, INT1G10CSASP, INT1G10CSASPDC, INT1G10CSA, INT1G10CSA-DC, P1GSCA, P1GCCAS-Custom.

THE ULTIMATE GOAL FOR DATA DIODE TAPS

are to feed OT/IT security monitoring solutions “every bit, byte, and packet,” to ensure the network is properly analysed and protected without introducing additional vulnerabilities from incoming traffic in the process. And that is why modern ICS security strategies are incorporating them alongside their network TAP and packet broker visibility fabrics.

Setting Yourself Up for Visualization Success

Looking to add TAP visibility to your deployment, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it’s what we love to do.



For more info, please visit: https://www.garlandtechnology.com/design-it

GARLAND TECHNOLOGY

See every bit, byte, and packet®