Probity
Cross Domain Solutions

Understanding Data Diode Options

An Executive Summary

Data diodes have a wide range of use cases in the commercial and government spaces including:

- Critical infrastructure protection
- Intelligence Community and DoD cross domain transfers
- Physical isolation of corporate, medical, financial, and sensitive data processing

This white paper is intended to provide guidance to implementers and customers, allowing them to make informed decisions about the type of diode that best meets their mission requirements (e.g., device, kit, appliance).

Traditional commercial data diodes have an assortment of limitations that typically only support a small number of protocols. This paper offers a more comprehensive look at these limitations (e.g., speed, file sizes, file types) as well as some solutions offered by Probity to address a wide range of mission needs.

Fastback features and benefits are discussed, including its most recent capability to provision channels. Finally, we highlight key differentiators between our suite of Fastback products and other vendor products.

Data Diode Options and Selection

Data diodes have been a part of cross domain systems for many years, but recently, they have become the critical component of a CDS providing physical domain separation between two networks. Data diodes provide defense-in-depth, preventing an adversary from physically accessing sensitive cross domain system components where content detection, inspection, and data transformation occurs, before being transferred to other networks. Diodes also provide physical separation of high threat networks to closed environments (e.g., software

development environments) where there is a need to move data into the isolated environment, but no way to systematically transfer data out of that isolated environment.

There are many different data diodes available on the commercial market, but this white paper focuses on providing CDS integrators and customers with information allowing them to select the data diode that best meets their mission needs. First, it's important to understand what types of products are available and how to go about narrowing down the options that will work for your implementation.

Currently, there are over a dozen data diodes listed on the National Cross Domain Strategy and Management Office's (NCDSMO's) official list of data diodes. Some vendors will state that their data diodes are "approved" by the NCDSMO, but that is not accurate. More accurately, the NCDSMO assesses data diodes for their "one-wayness". What does one-wayness actually mean? It means a vendor can submit a device, card kit, or appliance to the NCDSMO for assessment. The NCDSMO then uses a set of internally developed standard tests and/or instructions/directions/test procedures provided by the vendor to verify the "one-wayness" of the diode. As part of the assessment, the NCDSMO attempts to transmit data in both directions (i.e., sender to receiver and receiver to sender). Assuming the tests pass, a report is prepared by the NCDSMO with the assessment results and the vendor's product is added to the official diode list.

Outside of speed, why does it matter which diode I choose? While there are quite a few options on the NCDSMO's list, not all data diodes are created equal. We have broken down the available data diodes into three types and they're described below.

Data Diode Devices – This category of diodes are physical devices allowing light to travel in a single direction. If the requirement goes beyond just moving User Datagram Protocol (UDP) packets across the diode the implementor will likely need to develop software to make sense of the packets of data being transmitted through the device. A typical data diode device is only one part of a data diode solution.

Data Diode Card Kits – Card Kits may include just the Network Interface Cards (NICs) or they may include a fiber coupler, SFP+, etc. Card kits are intended to be installed on a customer's host computers (sender and receiver) and the hosts can vary widely. Each vendor will typically provide some minimum specifications for the host computers and performance of the diode may vary depending on the amount of memory, type of processors, and how fast the host computer can read from source end-point and write to the destination end-point. The card kits on the NCDSMO's list include software to run on the sending and receiving host computers to make sense of the data being transferred and each vendor supports specific protocols or connectors to transfer data.

Data Diode Appliances – Appliances are typically fully functioning 1U or 2U servers or a single 1U server with two host computers and a diode in a custom chassis.

Before reaching out to different data diode vendors, you can quickly narrow down your search by answering the following questions.

1. Will your data diode be part of a Raise the Bar (RTB) compliant Cross Domain System (CDS)? If the answer is yes, you'll likely want to consider a diode that can easily integrate with the cross domain guard you select.
2. Does your application require specific protocol adapters for accessing source and destination end-points (e.g., SFTP, NFS, SNMP, SMB, UDP, TCP, SMTP, FTP/S, REST)? If yes, card kits and appliances are likely the most viable option.
3. What are your throughput requirements? Card kits and appliances are typically designed for enterprise workloads (e.g., multiple TBs per day).
4. Do you have the resources and time to develop software that will make sense of the data you are sending on the destination network? If not, Card kits and appliances are the better choice.
5. Do you have a need or desire to run your business applications on the sending and/or receiving host computers? If yes, selecting a card kit may provide you with more flexibility if the appliance you are considering is only capable of being a data diode.
6. Do you have a need for an all-in-one data diode that you can plug a sending and receiving host computer into to transfer data in one direction, without the need to run other business applications on the data diode? If yes, selecting an appliance may be the best option for your use case.

Description of Problem with Most Commercial Data Diodes

Below is a list of common challenges with traditional data diodes.

- Traditional data diodes lack flexibility to schedule or allocate dedicated resources for data transfers
- Lack ability to prioritize mission critical dataflows
- Limits on number of concurrent dataflows
- Large files delay processing and delivery of small files
- All customers are treated the same (i.e., no prioritization of critical dataflows)
- No ability to dedicate resources to customers with special needs
- Perception of intermingling of customer data
- One customer could potentially impact the delivery of other customer data
- Customers with infrastructures that don't support > 10Gbps can't leverage capabilities of a 25Gbps or 100Gbps data diode
- Management and Data plane share the same diode resources

Solution

Probity offers robust data diode solutions in the form of kits and appliances. Our products offer maximum flexibility, allowing customers to purchase a kit where they can leverage customer owned or purchased hardware or appliances that come pre-configured with a DISA STIG applied. Probity's Fastback product line includes:

- **Data Diode Kits** (Rates of 1Gbps, 10Gbps, or 25Gbps)
- **Data Diode Appliances/Turnkey Solutions** (Rates of 1Gbps, 10Gbps, 25Gbps, or 100Gbps)

We offer an upgrade path on our 1Gbps and 10Gbps data diodes. Our most recent partnership is with Patton® Electronics, leveraging Probity's Fastback software with Patton's® FiberPlex SFP data diode devices. Patton SFP diode devices are now available with the purchase of Fastback 10Gbps data diode kits or appliances.

Probity's Fastback Data Diode Features and Benefits

Probity's Fastback data diode is listed on the NSA's National Cross Domain Strategy and Management Office's (NCDSMO) official diode list and has one of the widest selections of connectors/protocol adapters to customer source and destination end-points. Protocol adapters supported by Fastback include:

- HTTPS
- NFS
- SMB
- SFTP
- REST API
- JSON API

- SMTP
- SNMP
- SCP
- FTP/S
- UDP
- TCP

Fastback connector end-points include:

- AWS S3
- MS Azure Blob
- Google GCP Buckets
- Email
- Network Traffic
- JSON
- File Systems
- Streaming
- Everfox® Hunchback
- Everfox® Phoenix
- Everfox® AST
- Everfox® Hydra
- AFRL X-ARBITOR API

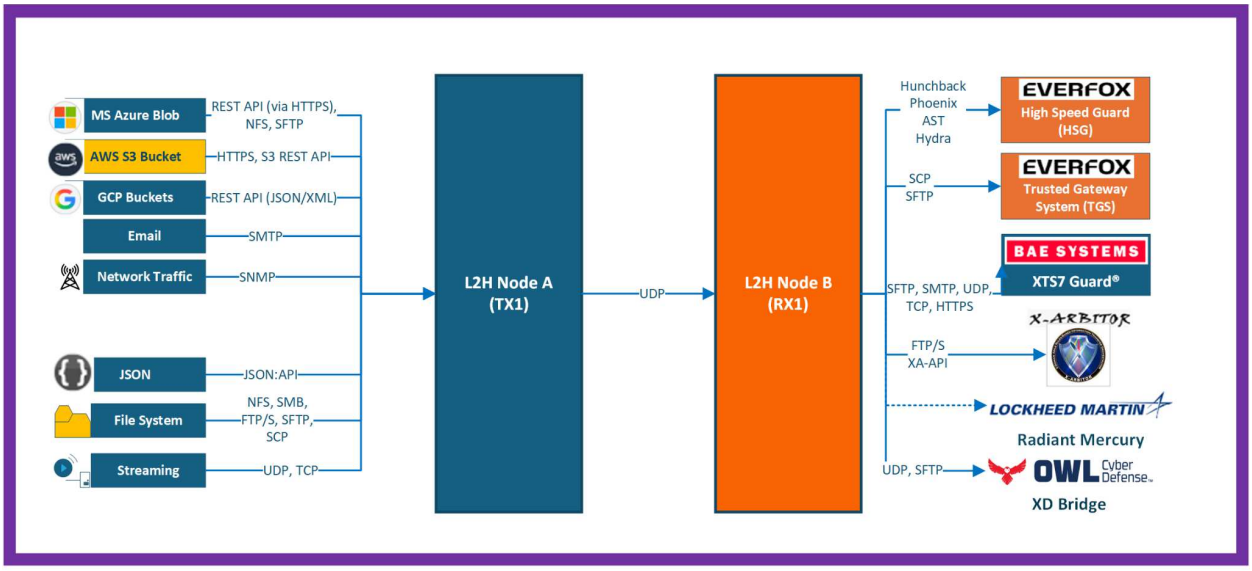
Fastback seamlessly integrates with the following NSA National Cross Domain Strategy Management Office's (NCDSMO) Raise the Bar (RTB) cross domain guards as all of them support standard protocols.

- Everfox® High Speed Guard
- Everfox® Trusted Gateway System
- BAE XTS7® Guard
- AFRL X-ARBITOR
- OWL XD Bridge

Fastback is currently not integrated with Lockheed Martin's Radiant Mercury. However, we are confident that Fastback can easily be integrated with this product.

The diagram below (see Page 6) illustrates how Fastback leverages various protocols to connect to source and destination end-points. It's important to note that while the diagram only shows cross domain guards on the receive side of the diode, all end-points on either side of the diode can be guards or any of the end-points shown on the send side of the diode. Furthermore, Fastback's flexibility allows customers to configure dataflows that retrieve data

from one type of end-point on the source side (e.g., AWS S3) and deliver data to a different type of end-point on the destination side of the diode (e.g., Azure Blob, SFTP).



Everfox, BAE Systems, Lockheed Martin, and OWL Cyber Defense are Registered Trademarks of the respective companies.

Furthermore, Fastback dataflows may be configured as polling (i.e., pull) dataflows where Fastback monitors an end-point for the presence of data to transfer or request driven transfers (i.e., push). For enterprise implementations, multiple Fastbacks can be clustered to operate seamlessly, providing load balancing and failover capabilities.

Probity's Fastback Data Diode Supports Customizable Channels

Below are the benefits of Probity's implementation of channels with their 25Gbps and 100Gbps data diode solutions. Not only can channels be created for items below. The size or bandwidth dedicated to a channel is also customizable. As an example, one channel might be configured with 5Gbps bandwidth while another channel is configured with 10Gbps. Each channel can be configured for up to 10Gbps of throughput and the sum of all channels' throughput cannot exceed the maximum throughput for the data diode license (e.g., 25Gbps data diode license cannot have a total of allocated bandwidth greater than 25Gbps). If a data type needs more than 10Gbps, additional channels may be configured to support that requirement.

- Dedicating channels for video feeds
- Dedicating channels for file transfers
- Dedicating channels for management plane data and data plane data
- Allocating channels for small files
- Allocating channels for large files
- Allocating channels by:

- Customer
- Data sensitivity
- Protocols
- Source and destination end-points
- Distributing custom traffic by cross domain guard type
- Priority

The diagram below provides an example of how a single Fastback 100Gbps data diode appliance may be configured, allocating dedicated channels for different use cases. There are virtually no limits to the number of dataflows that can run within a single channel. Probity has implementations of Fastback where a 10Gbps data diode is configured with 5,000 streaming video dataflows while other customers use Fastback to transfer files greater than 1TB.

Fastback Differentiators

- Request driven transfers provide an inversion of control, allowing customers to schedule and prioritize transfer requests
- Simple, elegant, easy, not a complicated process (It just works)
- Commodity hardware
- Largest selection of protocol adapters and connectors to end-points
- Mix/Match protocol adapters
- Protocol translator
- Customers can run their own apps on Fastback send and receive servers, regardless of whether it's implemented at a kit or appliance
- Clustering
- RegEx Filtering
- Polling allows you to set frequency of transfers as well as number of threads
- Perpetual license
- Warranty included with purchase for one year and renewed O&M extends the warranty on diode components
- Number of concurrent dataflows is only limited by the number of threads a single process can handle and available memory
- Channels
- Cleared professional services

Conclusion

Identifying the type of data diode your mission needs starts with understanding the three types of diodes (i.e., devices, kits, appliances). Selecting the type is a relatively straightforward process, based on needed functionality and desired platform. Once you've selected the type of data diode, you are now able to further isolate the options available to you. This paper

proposes a product line from Probity Inc., with headquarters in Herndon, VA. For those customers that need something more than a UDP data diode transfer device.

Probity's Fastback kits and appliances provide solutions for simple office requirements where data needs to be transferred from one environment to another or feature rich enterprise solutions for high performance data transfers and protocol adapters/connectors to a wide range of customer source and destination end-points.

Probity 754 Elden Street Suite 201 Herndon VA 20170

571-730-0020 fastbacksales@probity.com

probity.com fastbackdatadiode.com