AROW Data Diode

High Availability One-way Network Cyber-security

Operational Outline

Somerdata's AROW Data Diode Optical Wormhole ***provides a high-speed, reliable unidirectional barrier between networks.***

AROW is a new generation of Data Diode, designed from scratch to perform the vital task of High security network protection. First generation data diodes have often been difficult to manage, require significant administrative effort and can be very unreliable

Traditionally, overcoming this unreliability required often complex schemes with a lot of processing and data duplication. This makes Data diodes expensive and reduces the bandwidth of the link.

Somerdata's AROW is designed to be a high availability, high bandwidth system which takes care of the hard work of reliably sending data in a single direction.

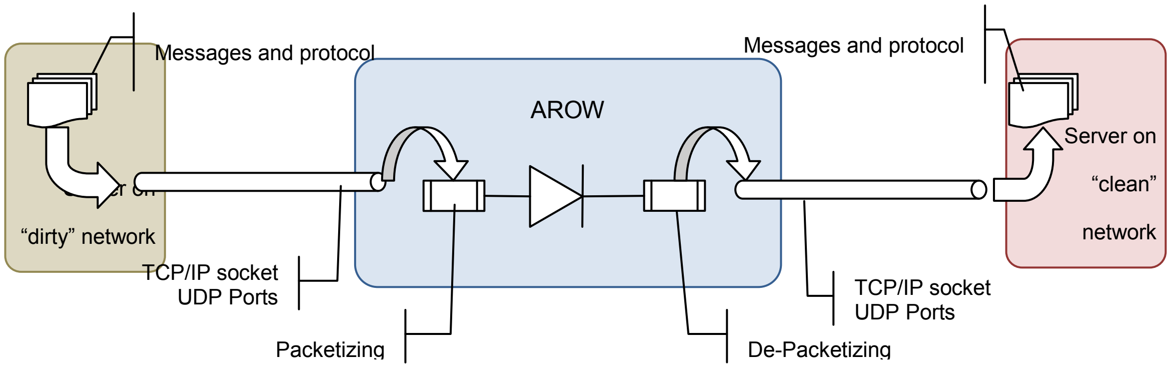
AROW operates on the principle of a unidirectional stream of data. This stream of data is fed on the low side through a TCP/IP Socket and/or multiple UDP ports . On the high side, a server can connect to these streams of data through a separate TCP/IP /UDP socket.

Data from the low side stream is fed to the high side on a high reliability, high bandwidth unidirectional optical link.

This enables full bandwidth Gigabit Ethernet communication from low side to high side protocols.

System Description

AROW is made of 4 sub systems: the Live and Backup Low side Packet Drivers and Live and Backup High Side Packet Receivers



somerdata

specialist surveillance and datacomms solutions

Low side packet drivers

The live low side packet driver (LLSPD) will accept a IPV4 TCP/IP socket connection from the low side server. Once this socket is established, all data successfully sent over that socket is framed and sent to the live and backup high side packet receivers with unidirectional optical data links. The optical data links are of higher bandwidth than Gigabit Ethernet to cope with the packet overhead and ensure no packet loss.
The TCP/IP socket data and status is also sent to the backup Low side packet driver (BLSPD) over a high bandwidth data link. In the case of a LLSPD failure, the BLSPD can assume the TCP/IP "identity" of the LLSPD and continue the TCP/IP socket connection where it left off, becoming the LLSPD.
The BLSPD also sends the packets it receives to the High side Packet Receivers.

UDP data is accepted on any valid port, the packet is encapsulated with its intended destination port, and inserted into the internal data stream

High Side Packet receivers

When a IPV4 TCP/IP socket connection is formed with the High Side Packet Receiver (HSPR) it extracts the data from the packets it receives over the unidirectional optical links and sends it over this socket.
If packets received from the LLSPD go missing, the packets from the BLSPD can be used instead.
The Backup HSPR can provide a full copy of the stream for processing by a backup server. If the live HSPR or High side server goes down the backup server can continue where the live one left off.

UDP data is similarly extracted and presented at the intended destination port.

Each sub system has its own control and status 10/100 Ethernet port used to configure the network parameters of the system and provide system health status without compromising the security of the design by creating a possible stealth back channel.

Direct Streaming

AROW is capable of Direct Streaming of TCP and UDP streams and does not encrypt or modify the data in any way. This means that it is transparent to data formats, encryptions or proprietary encoding. The high level of dedicated buffering ensures that normal network delays associated with TCP links can be accommodated. In this way, AROW acts very much like a normal TCP router.

Routing and Security

AROW can (and normally should) be configured to operate on two independent networks. Gateway addressing is supported to allow normal routing functions to be established. However AROW remains anonymous on the network and will not respond to PINGs or port scanners. AROW's in-built hardware TCP stack also rejects malformed or inconsistent packets, providing defence against attacks.

Control and Status

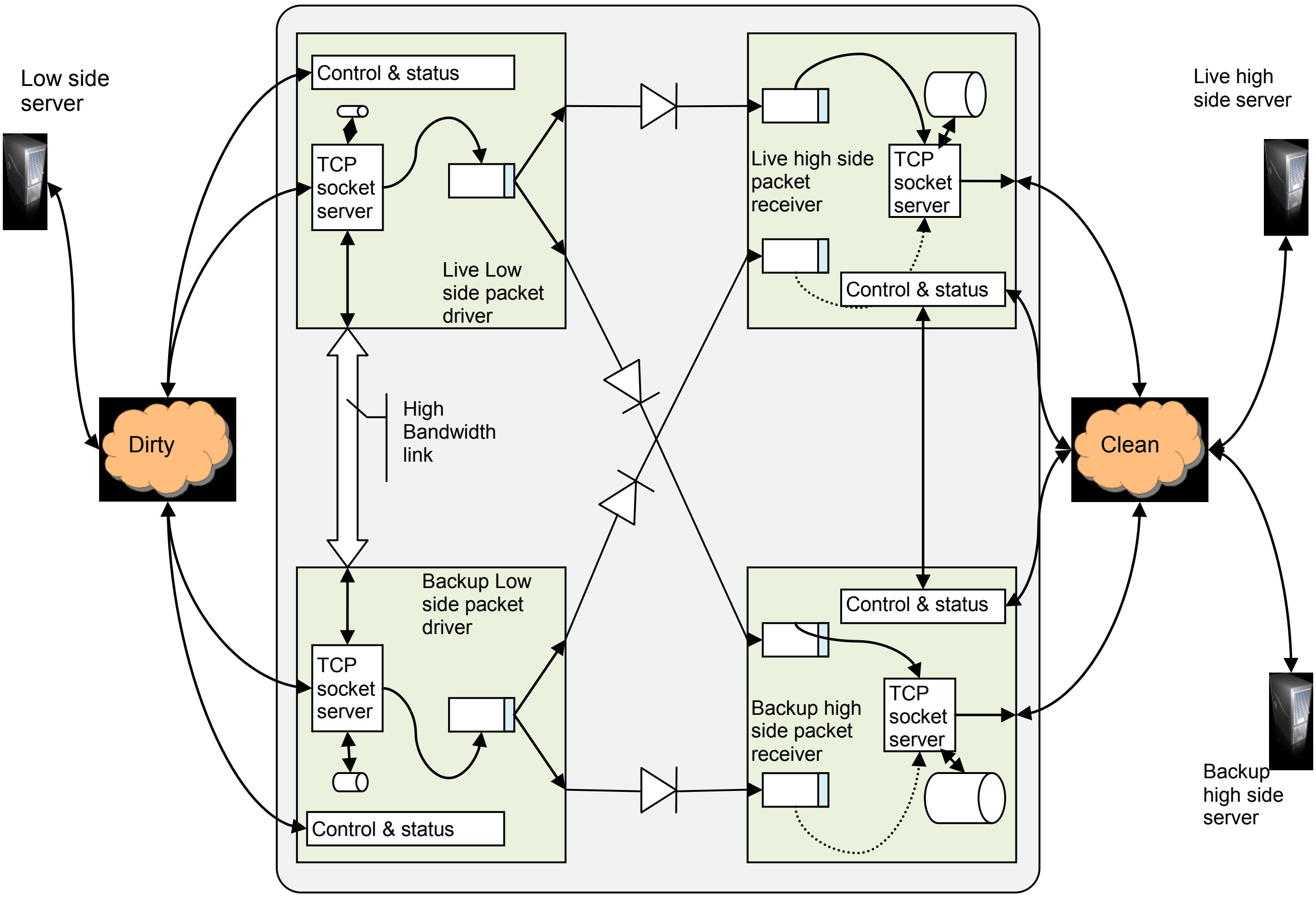
Each of AROW's data modules contain a separate control and status port. This should normally be operated from a network entirely separated from the high and low data networks, and protected from unauthorised access. These ports are used to set AROW's operating parameters, principally the Data network address assignments, but can also give status information about the internal buffers, allowing early indication of data flow limitations as well as attached network or internal module failures. However, for the highest security, these should not normally be attached, since AROW retains all its settings in hardware non-volatile storage, so once set up these ports are not needed.

Limitations

Of course AROW cannot replace other security measures such as Firewalls and Anti-intrusion methods, it is designed to prevent data egress from a network. It also cannot do this without penalty. This takes the form of user inconvenience – users on the protected side cannot demand data from the unprotected side, by definition. So a Network Administrator must create the conditions that allow data into the protected network. This requires discipline for all users and a system of communication from users to Administrator that can provide data with the minimum of administrative effort.

Since AROW is data- agnostic, any diode management software can be used, or AROWBftp open source software can be used. This supports File data transfer and UDP data transfer as well as multiple TCP stream transfer. This is described in a separate document, AROWSoftware, available on request or to download.

Block Diagram


Low side server
Control & status
TCP socket server
Live Low side packet driver
High Bandwidth link
Backup Low side packet driver
TCP socket server
Control & status
Dirty
Live high side packet receiver
TCP socket server
Control & status
Control & status
Backup high side packet receiver
TCP socket server
Clean
Live high side server
Backup high side server