ImageStream™

Network Monitoring White Paper

ImageStream Internet Solutions, Inc.
7900 East 8th Road
Plymouth, Indiana 46563

http://www.imagestream.com
info@imagestream.com

Phone: 574.935.8484
Sales: 800.813.5123
Fax: 574.935.8488

Introduction to Network Monitoring

ImageStream focuses on network monitoring as one of its OEM specialties. ImageStream offers a wide range of monitoring products including WAN and LAN monitoring taps, cards, development kits, and station hardware. This white paper is designed to introduce marketing professionals and systems engineers to network monitoring and the application of ImageStream monitoring products.

Network monitoring has been around as long as there have been networks. Most routers, switches, and intelligent hubs collect some level of network traffic statistics. This information is important to network administrators who are responsible for the operation of the network. Without network monitoring systems, it would be difficult to identify and resolve many network problems.

What Is Network Monitoring?

In short, network monitoring is the ability to collect and analyze network traffic. Most intelligent networking devices offer analysis of layer 1 traffic. At this level, the analysis typically focuses on physical network problems such as link status, CRC errors, bipolar violations, and framing errors.

Moving up from layer 1, dedicated monitoring equipment is often used to analyze layer 2 and layer 3 traffic. Layer 2 and 3 monitoring systems are commonly referred to as “protocol analyzers” because those higher level networking layers rely on special protocols to control the transmission of data.

The latest generation of network monitoring products is designed to support very specific applications. For example, some monitoring products are designed to help network administrators identify security threats; some are designed to provide law enforcement officials with tools for real-time surveillance; some are designed to analyze the performance of specific applications; and some are designed to collect raw data for intensive out-of-band analysis. Each of these specializations can yield a focused solution that is designed to address the specific requirements of a vertical market.

Monitoring Topology

There are two basic network monitoring topologies: passive or active. Passive or “non-intrusive” monitoring uses equipment that taps into a network and does not interfere with the flow of network traffic. Passive monitoring must be used in applications where a monitoring station will be moved to different locations where multiple taps are permanently installed.

Active or “intrusive” monitoring uses equipment that divides the circuit into two segments and allows the flow of traffic to be monitored, and actively transmitted from one side of the monitor point to the other. This topology must be used when a monitoring application requires active manipulation of the data stream before the data stream is transmitted across the monitor point.

The monitoring products marketed today reflect end user requirements for the network to continue operating even when the monitoring system is off-line. This means you can adopt passive or active monitoring systems as needed, but they must sustain network data flow under all conditions, and preserve the reliability of the network infrastructure. At the bottom line, monitoring devices must not bring down the network, and ImageStream offers both passive and active monitoring solutions that will satisfy these requirements.

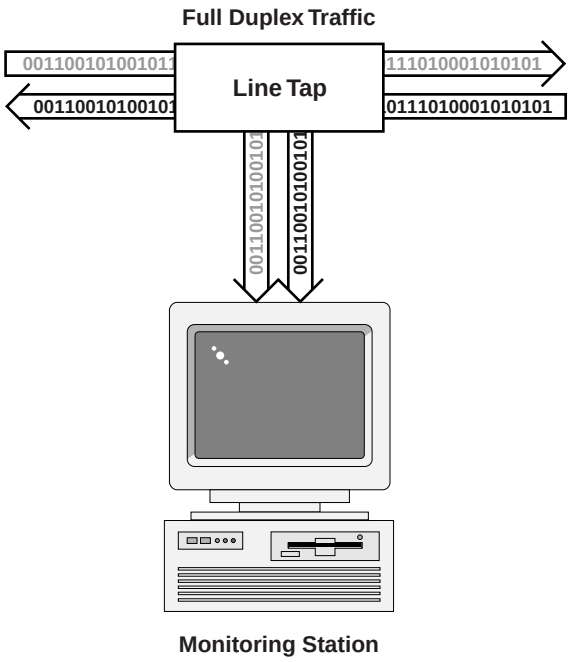

Figure 1 - Passive Monitoring

The diagram above shows an example of passive monitoring. In this design, the tap passes all of the data across the monitor point, and it passes both data streams to the monitoring station. With this kind of passive tap, data will continue to flow across the monitor point even when the monitoring station is not present.

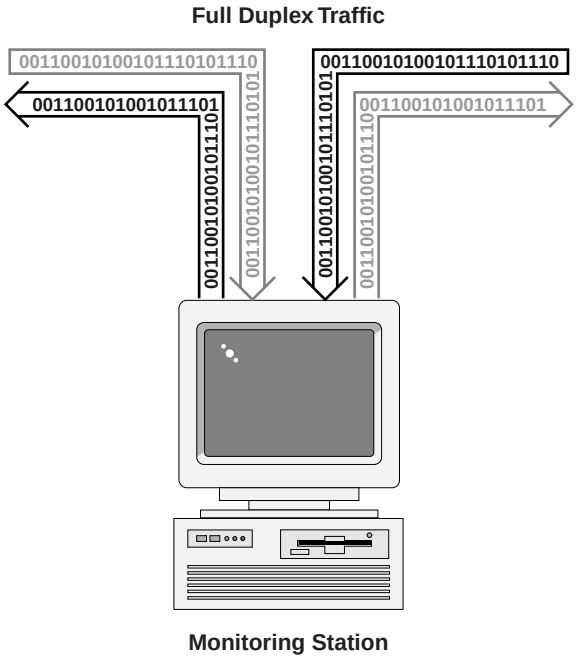

Figure 2 - Active Monitoring

Active monitoring involves equipment that not only taps the network link, but it must actively transmit the data stream from one side of the monitor point to the other. In this monitoring topology, the data flows through the equipment where it can be analyzed, processed, and modified in real time before flowing out of the device to the end point destination.

LAN Monitoring

LAN monitoring may be simple or complex, depending on the topology of the network and the design of the monitoring system. For example, it is easy to monitor ethernet traffic across a LAN that uses a hub topology. With a hub-based network, all nodes are connected to a single transmission line, which makes it possible to monitor all network traffic by connecting to any LAN port.

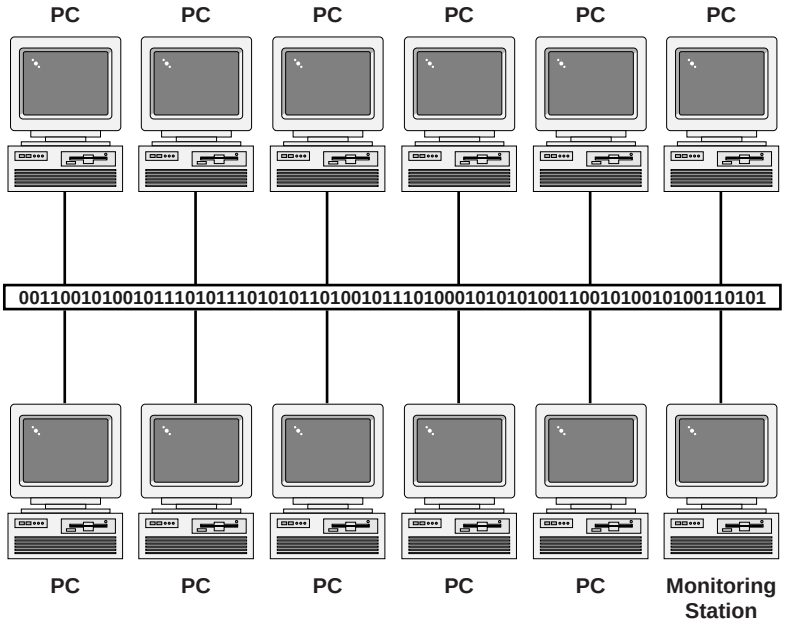

Figure 3 - Monitoring Ethernet – Hub Topology

Switched LANs present a different challenge. In a switched topology, the switch isolates network traffic to the source and destination ports. This means that if your node didn't transmit the data, and your node isn't the destination for the data, your node will never see the network traffic. This issue must be addressed when monitoring a switched LAN.

There are two different approaches to monitoring switched LAN traffic: tap every segment, or deploy a switch that supports monitoring. Some manufacturers have developed a monitoring feature for their high-end LAN switches that allows a LAN port to be reconfigured as a monitoring port. Unlike the other switched ports, the monitoring port will see all of the network traffic that is forwarded across the switch. Using this approach, the network will look exactly like the hub topology in figure 3, except the switch is responsible for delivering all traffic to the destination port, as well as the designated monitor port. This method usually provides the most cost-effective solution for applications that require a large number of switched ethernet ports to be monitored simultaneously.

As an alternative to deploying switches with monitoring support, it is also possible to tap each switched port. For example, a passive ethernet tap chassis with 20 to 40 ports may be deployed to tap each segment that is connected to the switch. With this approach, it is common to have a portable monitoring station that can be plugged into any tap as needed. This methodology can be very expensive, because each monitored node must have a dedicated tap. In addition, if you plan to monitor all nodes simultaneously, the multi-tap methodology will be much more costly, because the monitoring station will also need to provide enough ethernet ports to connect to each tap.

WAN Monitoring

When compared to LAN monitoring, WAN monitoring is considerably more complicated. LAN monitoring is primarily focused on the analysis of ethernet encapsulated data, while WAN monitoring must support a much wider range of network topologies and protocols.

Wide area networks may use a point-to-point or point-to-multipoint topology. In a WAN environment, there is no single interface to which all packets are transmitted. This means that WAN monitoring applications require a tap to be installed on each data circuit. Each tap must match the impedance of the data circuit, it must transmit network traffic from one side of the tap to the other, and it must not disrupt network traffic.

WAN monitoring software is also relatively complex. The operation of each WAN connection depends on different WAN protocols such as PPP, multilink PPP, Cisco HDLC, frame relay, and ATM. WAN monitoring software must recognize these protocols, and it must be able to interpret any virtual channelization that is encoded using protocols like frame relay and ATM. In monitoring applications, these WAN protocols must be analyzed, and then intelligently stripped away before the encapsulated data can be analyzed.

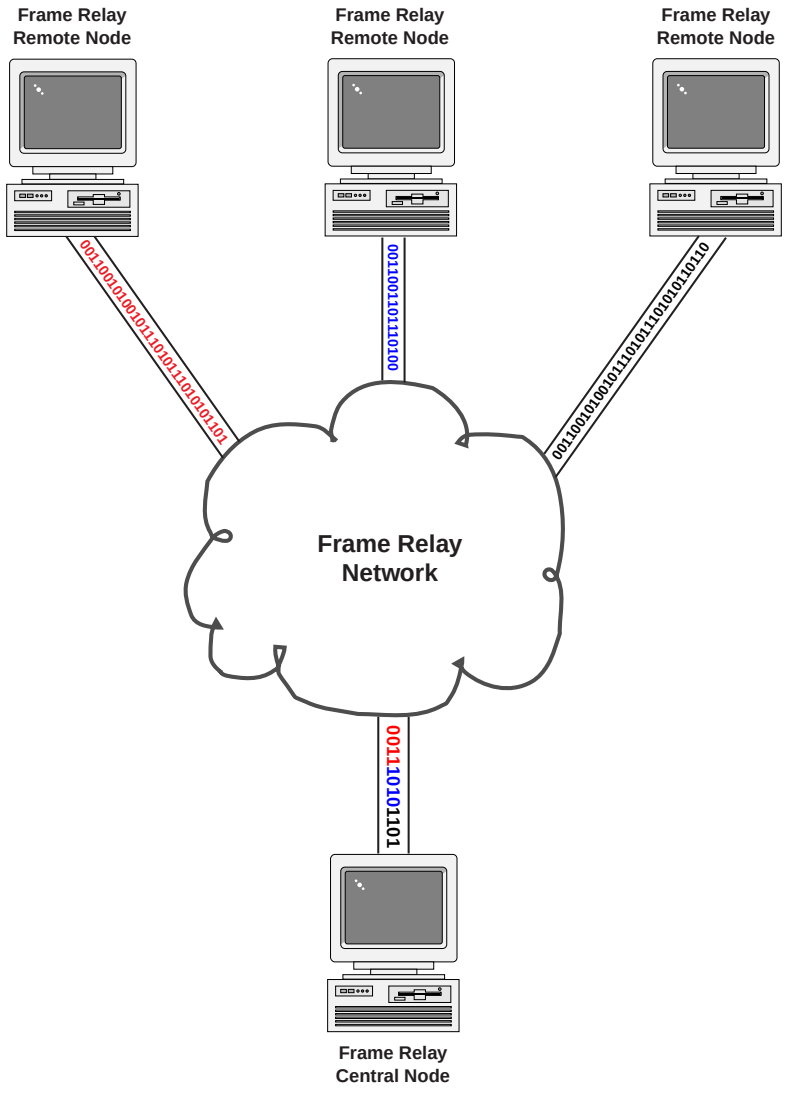

Figure 4 - Frame Relay Topology

WAN monitoring also presents challenges beyond the overall application complexity. Because WAN circuits are usually connected to the public telecommunications infrastructure, the associated monitoring equipment must meet stringent public specifications and provide the required certifications for connection to the public network. This means that once all of the technical design requirements of the monitor hardware are achieved, the equipment must still pass FCC certification.

Passive Monitoring Components

ImageStream offers the industry's most extensive line of hardware and software for passive network monitoring. Passive monitoring elements include network taps, network monitoring cards, cables, driver software, and software development kits.

Network Taps: A network tap is used to transparently tap into a data circuit. The tap allows the network traffic to flow from one side of the monitor point to the other, like a "Y" cable or repeater, and it delivers two network data streams to the network monitoring card via a purpose-built cable.

Network Monitoring Cards: A network monitoring card is installed in a computer system that runs the application software which is used to analyze network traffic. The monitor card provides two data reception channels for monitoring both data flows in a full-duplex transmission, and it provides power to the tap through the tap cable.

Network Monitoring Cables: Network monitoring cables are used to connect a network tap to a network monitoring card. This cable must be able to carry power to the tap.

Driver Software: Driver software is designed to work with a specific operating system to allow the network monitoring card to receive network data into memory for analysis by the network monitoring software.

Software Development Kits: Software development kits are cross-platform function libraries which simplify the process of developing low-level interfaces between network monitoring cards and network monitoring software.

Monitoring taps are passive, so they can be installed at different locations throughout a network without the need to have a monitoring device attached. In this way, the end customer can install multiple taps, and then move the monitoring equipment from one tap to another as needed.

The most important element of a network monitoring system is the software used to analyze network traffic. This is the application software that differentiates one network monitoring product from the other. ImageStream does not supply this data analysis software because it is the software that defines the product, and it is the one critical piece of software puzzle that each OEM must develop.

Active Monitoring Components

ImageStream also offers hardware and software solutions for active network monitoring. Active monitoring components include network monitoring cards, cables, driver software, and software development kits. These components are similar to the passive components described above, except each segment of a tapped line is directly connected to the monitoring card. The monitoring card must remain in-line for the data circuit to operate properly. Active monitoring cards must also provide pass-through "relays" that complete the data circuit when the monitoring station is shut down.

Ethernet Monitoring

ImageStream's ethernet monitoring solutions cover both passive and active applications. ImageStream offers passive monitoring systems that include full-duplex ethernet taps with IEEE 802.3af power-over-ethernet, multiport monitoring cards, and driver software. ImageStream also offers high-density powered rackmount solutions for networks that require a large number of taps.

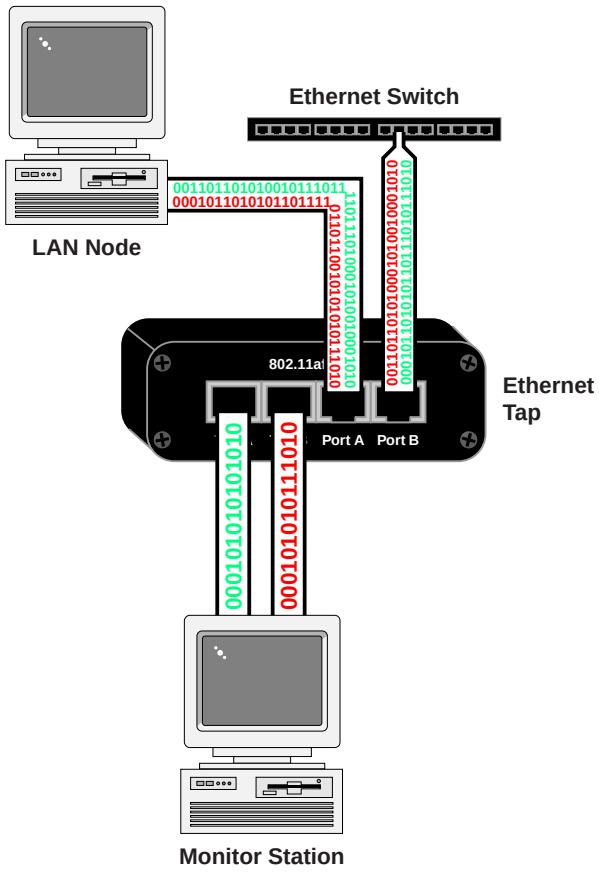

Figure 5 - Passive Ethernet Monitoring (Full Duplex)

In addition to passive solutions, ImageStream offers active monitoring systems for ethernet applications. Active monitoring uses a monitor card with linked pairs of ethernet ports that connect directly in-line with the ethernet cabling (no external tap is required). The ethernet segment is split into two pieces, with each of the two pieces connected directly to a pair of ports on the monitor card. When the monitoring station is on-line, the application software must forward the full duplex traffic from one port to the other. When the monitoring station is powered off, the monitoring card closes its pass-through "relays" to allow the full duplex network traffic to flow without interruption.

Synchronous Serial Monitoring

Synchronous serial monitoring solutions for data speeds from 1 to 4 Mbps must support a wide range of synchronous serial standards. This is because different DSU product manufacturers in different parts of the world have adopted different serial standards for different reasons. As a result, three popular synchronous serial signaling standards have emerged including V.35, RS232 and RS422. RS422 has several physical connector standards including EIA530 which uses a DB25 connector, RS449 which uses a DB37 connector, and X.21 which uses a DB15 connector.

Each of the different synchronous serial signaling standards is supported in hardware by the model 410 multi-interface monitoring card. The model 410 has two operating modes which support the V.35 and RS422 signaling standards. In RS422 signaling mode, the model 410 supports different physical connectors by using a special “Y” cable that is connected to the tap. This “Y” cable provides the required RS232/EIA530, RS449 or X.21 connectors.

The diagram below shows how this monitoring solution would be cabled.

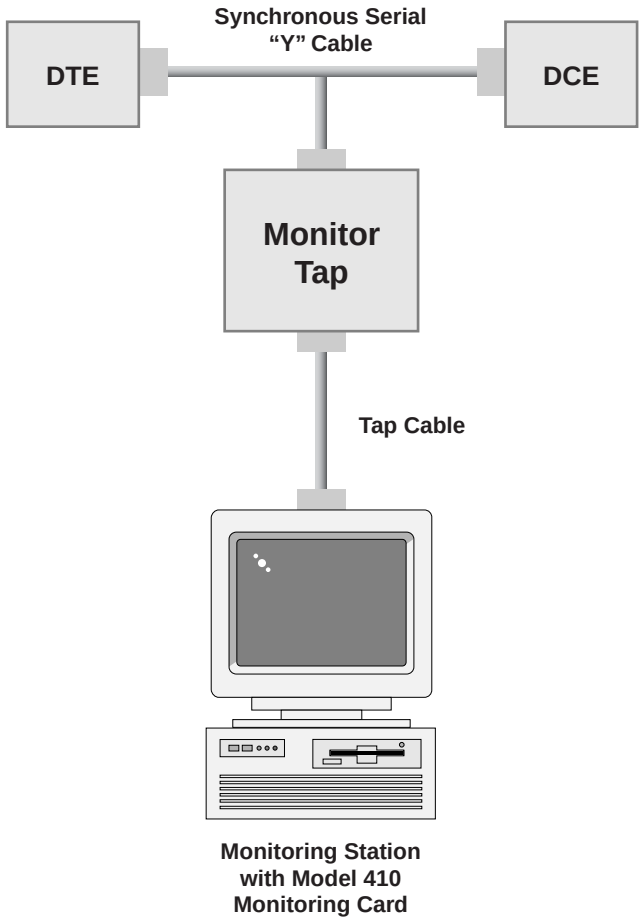

Figure 6 - Passive Synchronous Serial Monitoring (Full Duplex)

With synchronous serial interfaces, there is a unique connector for DCE and DTE device connections. This orientation is preserved by all system components, including the appropriate cable gender for DCE and DTE connections.

T1/E1 Monitoring

ImageStream’s passive monitoring solution for T1/E1 applications includes a monitoring card, tap, cables, and driver software. The T1/E1 tap provides two pairs of RJ48 jacks and two pairs of bantam jacks that are used to connect up to two T1 or E1 circuits for monitoring. A DB25 connector and tap cable are used to connect the tap to the DB26HD connector on the monitor card. The monitor tap and cable are compatible with ImageStream’s 4-port and 8-port T1 and E1 cards, which can be used to monitor two or four data circuits respectively.

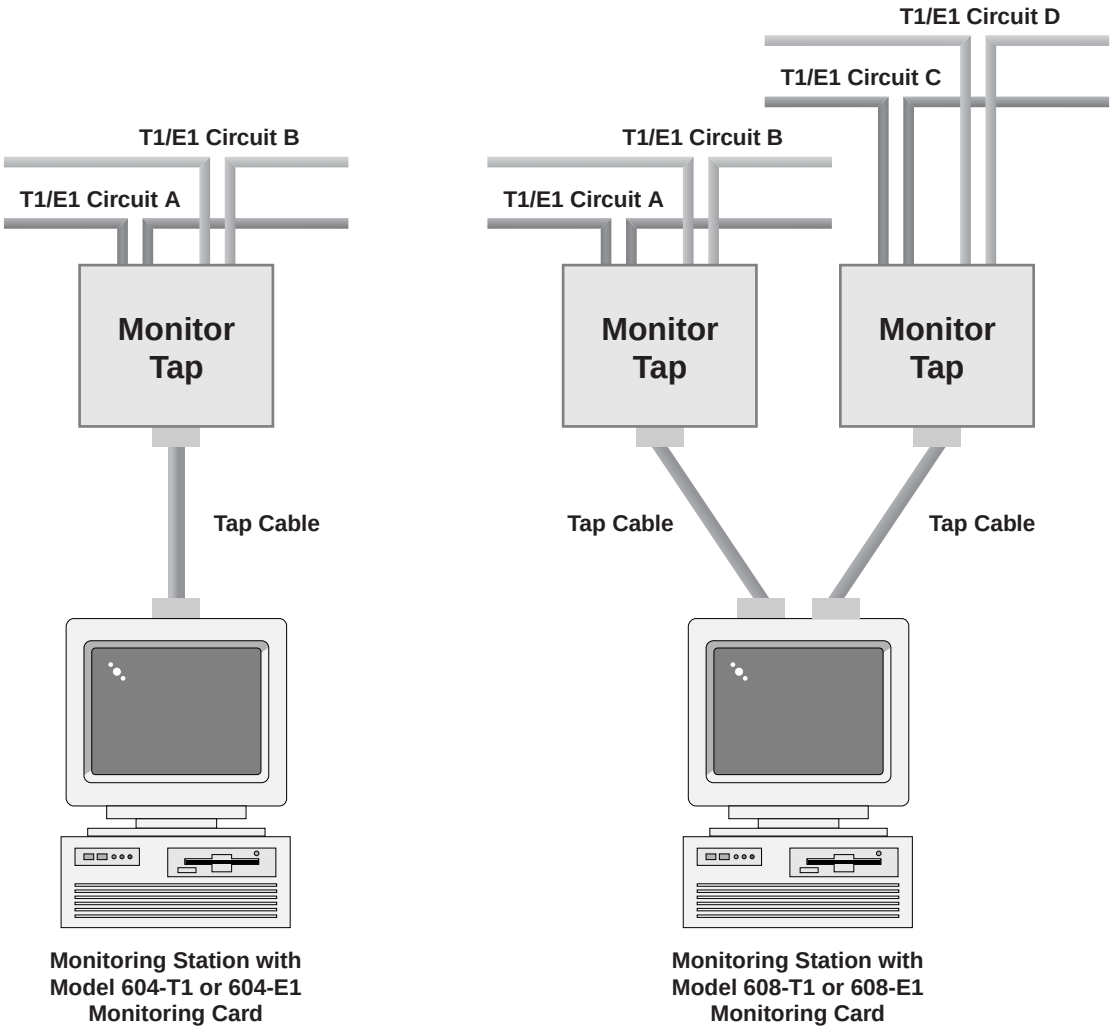

Figure 7 - Passive T1 and E1 Monitoring (Full Duplex)

The tap has a DIP switch to select T1 or E1 operation, and a DIP switch to select between the RJ48 and bantam jack inputs. The tap circuitry includes a long-haul receiver and a T1 transmitter. The receiver has circuitry capable of equalizing cable loss up to 36 dB at 722 kHz, which corresponds to 6300 feet using 22 AWG twisted-pair cable.

The 604 and 608 T1 and E1 cards can also be used in active monitoring applications without the passive tap. These cards do NOT provide automatic pass-through when the monitor station is powered down, so the monitor station must remain in service to avoid disruption of the data circuit.

HSSI Monitoring

ImageStream's passive monitoring solution for HSSI applications includes a monitoring card, tap, cables, and driver software. The HSSI tap provides two HSSI connectors that are used to connect to the DTE device on one side of the tap and the DCE device on the other. The tap also provides a DB26HD port that is used to connect the "Y" tap cable to the monitoring card. The tap provides high-impedance connections to the tapped HSSI link, and supplies enough power to drive the HSSI signal up to 50 feet as required by the HSSI specification.

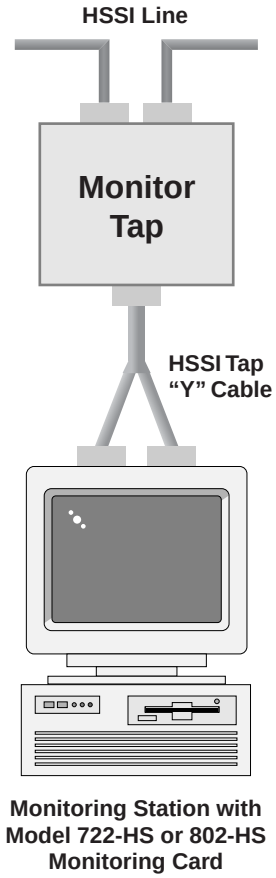

Figure 8 - Passive HSSI Monitoring (Full Duplex)

ImageStream offers two different HSSI cards for passive monitoring applications. The 802-HS is a low-cost HSSI monitoring card that can monitor full duplex HSSI data at speeds up to 52 Mbps with 256-byte or larger packets. The 722-HS card is a co-processed card that is used when wire-speed HSSI performance is required with small 64-byte packets. The 802-HS is an appropriate choice in cost-sensitive applications where typical Internet data will be monitored. The 722-HS is used in applications where the data traffic will consist of a large percentage of small 64-byte packets, or in products that must be able to monitor any HSSI data stream.

For active HSSI monitoring applications, ImageStream also offers the PCI 722VN. The 722VN is an active monitoring card with two HSSI ports (one for DTE and one for DCE). To ensure network availability, the 722VN is designed to automatically pass through network traffic from one port to the other when power to the monitor station is turned off. In active monitoring applications, the monitor station software must actively forward data packets from one port to the other to maintain the flow of network traffic while the monitor station is on-line.

DS3/E3 Monitoring

Like the company's other passive monitoring systems, ImageStream offers DS3 and E3 solutions that include a monitoring card, tap, cables, and driver software. The DS3 and E3 taps each provide four coaxial connectors to connect each side of the full duplex DS3 or E3 circuit. The tap also provides a DB15 connector that is used to connect the tap cable to the monitor card. Like ImageStream's other passive monitoring solutions, the DS3 and E3 taps are powered by the monitor card.

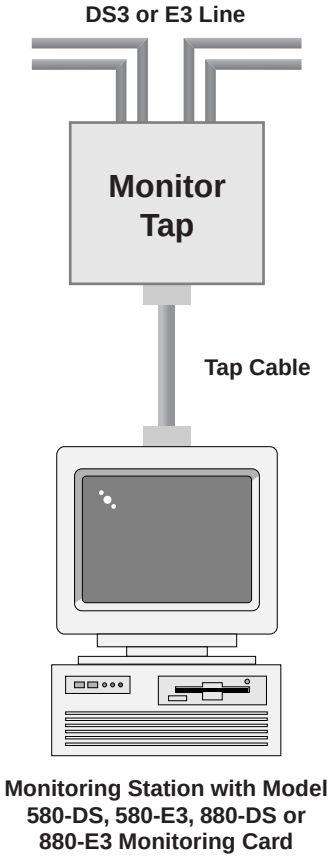

Figure 9 - Passive DS3 and E3 Monitoring (Full Duplex)

Conclusions

ImageStream offers the industry's most comprehensive line of active and passive LAN and WAN monitoring solutions. Active monitoring systems can be developed using standard network cards that provide at least two ports, but the best active monitoring solutions provide a pass-through feature which allows the network traffic to flow without interruption when the monitor station is powered down. With passive monitoring, an external tap sustains traffic flow through the tapped circuit even when the monitor station is disconnected from the tap. This design makes it possible to install a large number of taps at different locations, and connect a portable monitoring station only when needed.

ImageStream provides passive monitoring solutions for 10/100 ethernet, gigabit ethernet, synchronous serial, T1/E1, HSSI, DS3 and E3 applications. ImageStream also provides active monitoring solutions with pass-through for 10/100 ethernet and HSSI, as well as monitoring cards without automatic pass-through for gigabit ethernet, sync serial, T1, E1, HSSI, DS3 and E3 data circuits.