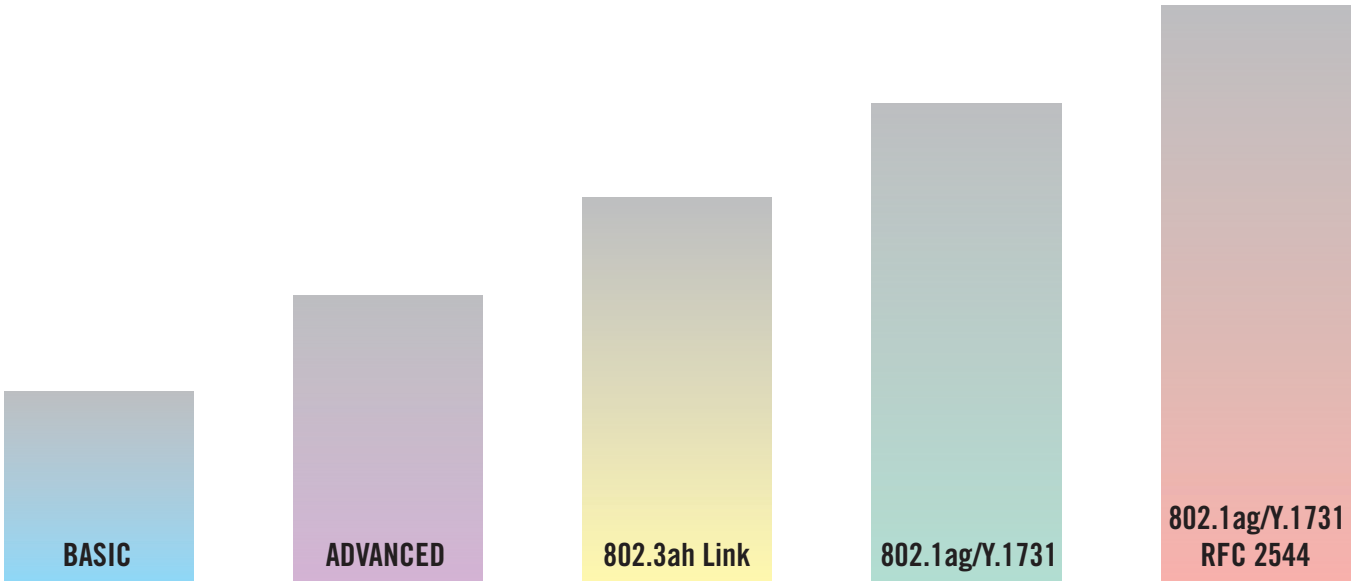


REMOTE MONITORING MATRIX

Featuring a matrix of different features that will help you identify and select which Transition products best meet your remote monitoring requirements.

Network Interface Devices

Transition Networks recognizes that service providers and enterprises have varying remote management needs depending on the specific services and support they require. To meet these requirements Transition now offers several different classes of remotely managed devices—ranging from basic remote monitoring, SNMP and Full SOAM monitoring using ITU Y.1731 and 802.1ag. Transition's Carrier Ethernet devices are built on these multiple classes of remote management for improving business agility with assured quality, maximizing your return on investment and the total cost of ownership within your network.

Remote Monitoring Capabilites	x2210/xBFTF	xSRFB	x2220/x322x xFBRM/xBFFG	x323x	S2250/ S325x
	Basic	Advanced	802.3ah Link OAM	802.1ag Service OAM	Y.1731 Performance
Basic Remote Monitoring					
Link Pass Through (LPT)	✔	✔	✔	✔	
Transparent Link Pass Through (TLPT)	✔	✔	✔	✔	
Far-End-Fault	✔	✔	✔	✔	
Automatic Link Restoration	✔	✔	✔	✔	✔
Remote Firmware Upgrade	✔	✔	✔	✔	✔
Advance Remote Monitoring					
Loopback		✔	✔	✔	✔
Dying Gasp		✔	✔	✔	✔
RMON Counters			✔	✔	✔
IEEE 802.3ah - Link OAM					
Discovery			✔	✔	✔
Dying Gasp			✔	✔	✔
Link Fault			✔	✔	✔
Critical Events			✔	✔	✔
Remote Loopback			✔	✔	✔
Local Loopback			✔	✔	✔
Fault Isolation			✔	✔	✔
IEEE 802.1ag - Service OAM					
Discovery				✔	✔
Continuity Checks				✔	✔
Loopback				*Port Level	✔
Link Trace				✔	✔
ITU Y.1731 - Performance Monitoring					
Discovery				✔	✔
Continuity Checks				✔	✔
Loopback				*Port Level	✔
Link Trace				✔	✔
AIS				✔	✔
RDI				✔	✔
ETH-TST				✔	✔
Loss Measurement				*Port Only	✔
Delay Measurement				* Roundtrip Only	✔
Delay Variation Measurement				* Roundtrip Only	
Product Features	**x2210/xBFTF**	**xSRFB**	**x2220/x322x xFBRM/xBFFG**	**x323x**	**S2250/S325x**
802.1q VLANs			✔	✔	✔
Q-in-Q VLANs			✔	✔	✔
IEEE 802.1P QoS			✔	✔	✔
Bandwidth Allocation		✔	✔	✔	✔
Jumbo Frame			* (BFFG)	✔	✔
MEF 9 certification			✔	✔	✔
MEF 14 certification			✔	✔	✔
IP addressable			✔	✔	✔
RFC2544 Tester					✔
SNMP Management	✔ (via mgmt)	✔ (via mgmt)	✔	✔	✔

Basic Remote Monitoring

Traditionally, service providers who deliver Ethernet services to customers, use a form of remote management that is designed to isolate physical fault conditions by using a technique from reverse engineering. The operator is notified of a fault condition either by a Link Pass Through (LPT) alert or by a Far End Fault (FEF) notification. In both instances the cable connectivity is disrupted, copper for LPT and fiber for the FEF—notifying the management system that this disruption may have been caused by someone disconnecting one of the ports.

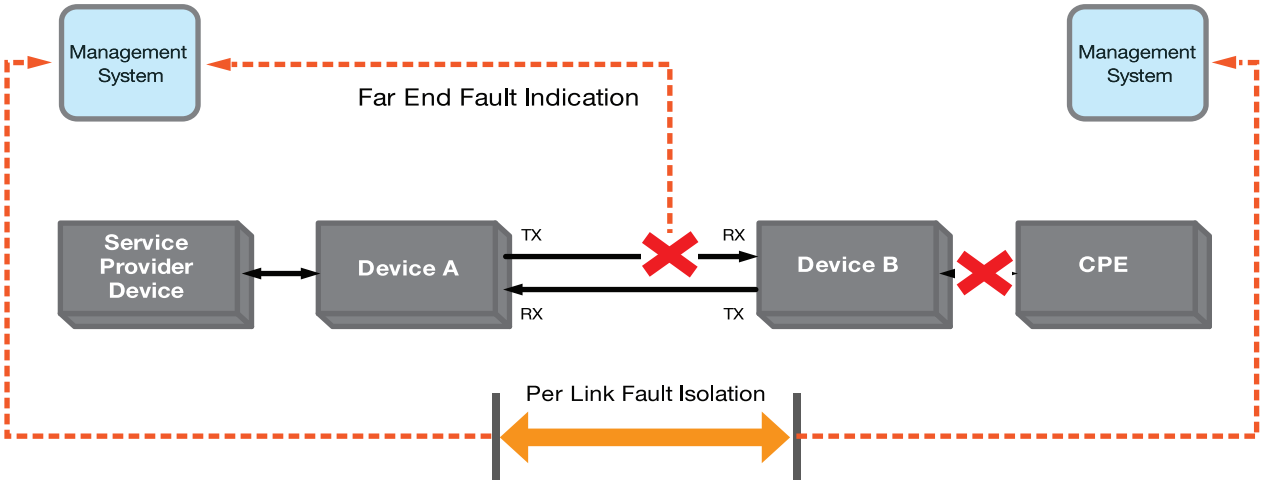
LPT states that if the copper demarcation port loses a signal, the device will then pass the link fault condition through to the next device in the sequence—which then disables the local copper port, therefore alerting the managed switch or router that the demarcation copper port is effectively disconnected. While this deployment strategy does allow for a Network Management System (NMS) to be alerted to a customer failure, it does require some additional manpower to troubleshoot each of the devices and link segments along the service path to the customer—starting with the central office device and connectivity. After the link failure condition has occurred, Automatic Link Restoration will automatically re-establish the link without the need to physically reset the device.

Features

- Far End Fault (FEF)
- Link Pass Through (LPT)
- Auto Link Restoration
- Remote Firmware Update

Application

This basic level of management by an Ethernet service delivery package would be deployed by a service provider that is not bound by a fixed SLA and with sufficient staff resources to troubleshoot failures.



TRANSITION NETWORKS®

+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

Advanced Remote Monitoring

Advanced Remote Monitoring, or Link Layer Monitoring, is often used by service providers for residential and business services. Advanced Remote Monitoring offers a best-effort service with the addition of Link-Monitoring, which allows for fault detection on the physical link between two devices. When implementing Advanced Remote Monitoring services, remote devices will need to share a simple lower-level protocol that can exchange information on fault conditions, along with the status of each device on a single link.

In an Advanced Remote Monitoring application, the detection of a fault condition may be all that an operator really needs for fault isolation—therefore delivering a notification for the need to restore service. Additional information, if desired, such as the duplex status of each device on the link may also be beneficial to determine limited accompanying fault isolation. For example, Advanced Remote Monitoring equipment provides information like Far End Fault (FEF) notifications—where the far-end device (endpoint) sends an error message to its immediate peer, that it is no longer receiving traffic. The exact cause of this fault could be several different factors including: a cable cut, faulty receiver, or faulty transmitter. Transparent Link Pass Through (TLPT) will then notify the end device of the failure over the fiber link instructing the remote device to shut down the copper port and thus notifying the local device of the failure.

Advanced Remote Monitoring uses an additional feature called Loopback, which is most commonly used as an aid in troubleshooting physical connection problems within the network. With this feature you can quickly pinpoint a problem between two end-points in different locations of a particular segment. By sending a test signal through the circuit in one location, and having the end device at the other location send the signal back through the circuit, you can confirm that the circuit is functioning correctly.

Features

- Far End Fault (FEF)
- Error Message Transmission
- Transparent Link Pass Through (TLPT)
- Loopback
- Dying Gasp
- Automatic Link Restoration
- Remote Firmware Upgrade

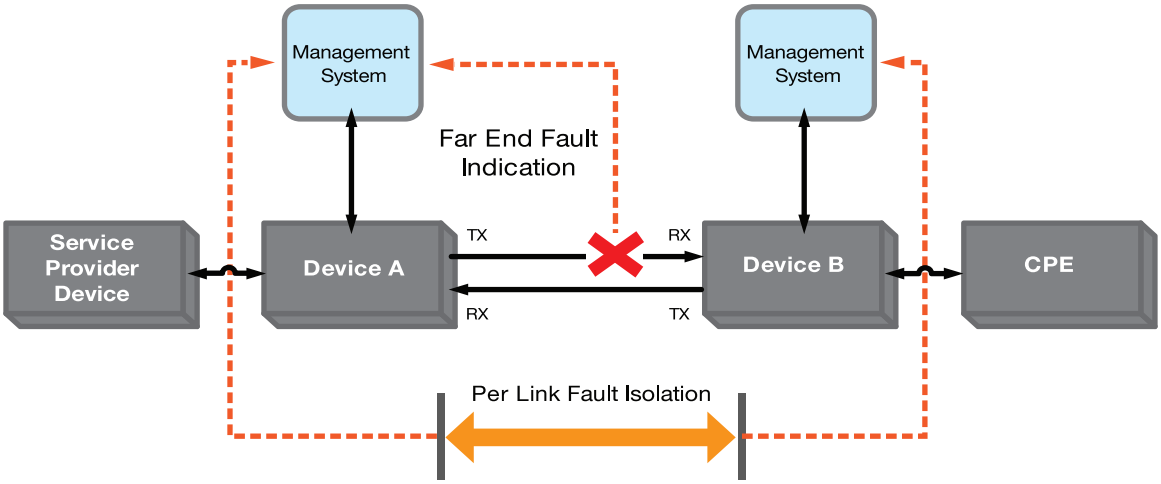
TRANSITION NETWORKS

+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

Advanced Remote Monitoring

Application

A typical Advanced Remote Monitoring application requires a user who is looking to quickly isolate physical connection faults and will probably deploy this technology with connectivity assurance only—rather than with the use of a detailed Service Level Agreement (SLA).



To determine and fix the actual fault will require several steps that could involve a service dispatch, but the fault has been isolated along the transmitted path and allows the operator to focus their resources on correcting the identified fault conditions.

TRANSITION NETWORKS®

+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

802.3ah Link OAM

IEEE 802.3ah remote management is tailored to deliver services to small and medium sized businesses. IEEE 802.3ah Link OAM was developed by the IEEE as a standard for detecting link failures on the first hop, point-to-point physical Ethernet links. Often referred to as "Ethernet in the First Mile" (EFM) describes that any Ethernet device that has IEEE 802.3ah capabilities can learn each others OAM capabilities via a 'Discovery' mechanism performed either at the MAC or IP address level. IEEE 802.3ah in addition to discovery capabilities, incorporates Remote Fault Detection, which allows one end-point device to inform the other in both bidirectional and unidirectional links that a link failure has been detected. Once the failure is detected, it can set a device in a loopback mode that will clear when it recovers. An example of IEEE 802.3ah fault detection is Dying Gasp. A Dying Gasp condition occurs if there is an interruption in the end-point's power source. Prior to the device power failure, there is enough power reserved for a Dying Gasp alert to be sent to the network operator's network management system. This helps a service provider identify and isolate the end-point device that has experienced a power failure. IEEE 802.3ah also includes Remote Monitoring capabilities. This allows network operators to collect real-time and historical near and far-end link performance statistics similar to those found in SONET/SDH networks.

Although IEEE 802.3ah can provide valuable information to network operators on critical events, IEEE 802.3ah does not provide a method or mechanism for repairing faults as they occur. Moreover, because of the wide range in equipment capabilities, fault isolation may require a network operator to establish conditions and traffic for that specific fault condition. An example of such a generated traffic packet is an IEEE 802.3ah Loopback Message (LBM) packet, which is designed to address and isolate performance issues on specific links within a service provider's network.

Features

- Discovery
- Far End Fault (FEF)
- Dying Gasp
- Fault Isolation
- Per Link Fault Isolation
- Critical Events
- Local Loopback
- Remote Loopback

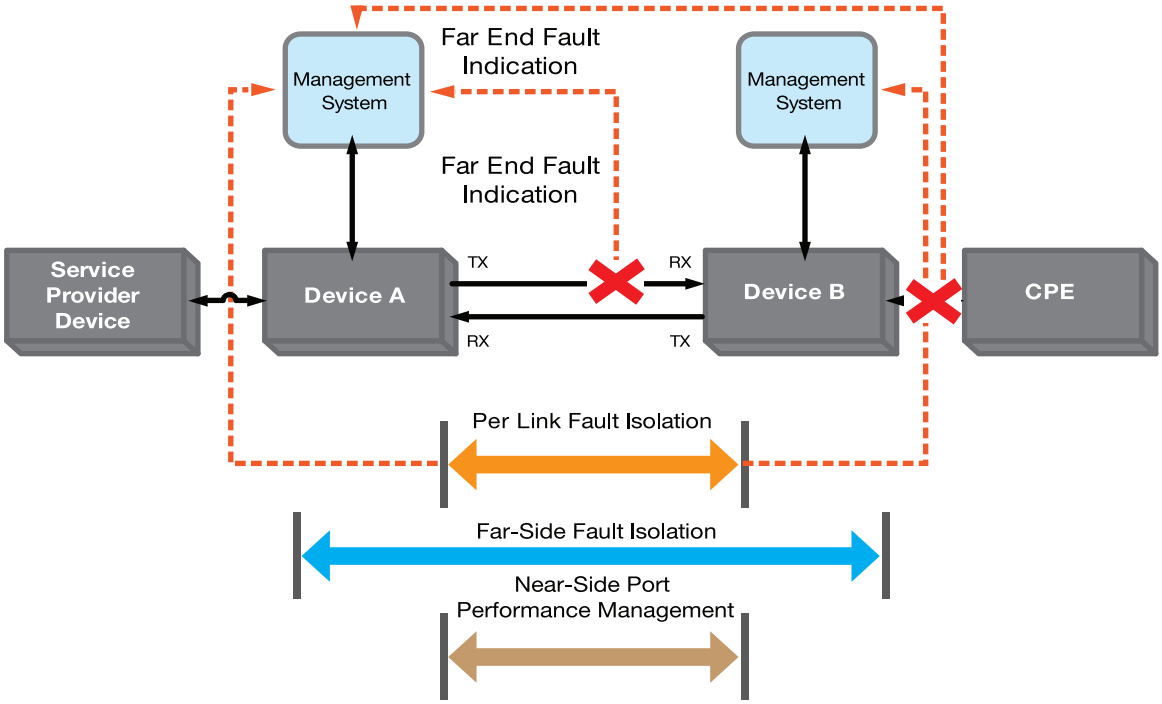
Application

Link OAM users generally have very basic SLA requirements and will tend to use IEEE 802.3ah in isolating faults efficiently and quickly. Link OAM devices need to be used at both the service provider's point of presence and at the customer premise (CPE) for effective link reporting.

TRANSITION NETWORKS®

+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

802.3ah Link OAM



Additional Capabilities

Link OAM also has another option that does not require the deployment of IEEE 802.3ah to receive all of the reportable information. In this option, management reporting is done through the IP address of the NID. This means that rather than a book-end IEEE 802.3ah type deployment—an operator can simply connect the fiber coming from an Access Node switch to a remote NID and manage all of the features and capabilities of the NID, through an individual IP address that is assigned by the operator carrier. This set-up provides an operator with increased visibility beyond IEEE 802.3ah reporting and does not require both items in the link to have IEEE 802.3ah capability.

+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

802.1ag/Y.1731 Service OAM

IEEE 802.3ah OAM is applied specifically to the physical link between an endpoint and a directly connected peer device, whereas IEEE 802.1ag Continuity Fault Management (CFM) takes this function to the next level and examines the logical flows, not only between directly connected links, but also across the path of any two points in an entire network. IEEE 802.1ag provides visibility into the VLAN traffic and uses special continuity check messages that are sent periodically from one end-point to the other, checking availability of the connections. Link Trace is another on demand IEEE 802.3ag tool used by operators to trace the path towards a specific MAC address destination. This is in the form of a MAC layer traceroute, which allows the network operator to detect if a peer is available and what intermediate stations are between the end-point and the detected peer on the network path. The end-point and peer can then decide what is needed for fault isolation and diagnostics—including on demand loopbacks between specific devices. Once a method has been determined, it can then start a loopback between the two end-points on the VLAN path. This provisioning allows users to generate specific per-VLAN continuity checking, loopback, and link trace frames. IEEE 802.1ag also defines the use of maintenance domains. These are simple network areas defined by the service provider in a hierarchical order that will be monitored. These areas or boundaries within the domain are further broken out into messages from one end-point to the other, checking the availability of the connections.

The introduction of ITU Y.1731 Frame Delay (FD) and Frame Delay Variance (FDV)—requires peers to exchange timestamp information every time a peer handles a packet along the logical path. ITU Y.1731 defines both one-way and two-way frame delay. One-Way frame delay requires that there is a unified clock between the two endpoints and is measured in a single direction, such as upstream. The two-way frame delay is done with a round trip calculation and only requires a single clock at the source. Frame Delay (FD) is measured by an end-point transmitting an SOAM frame periodically and having the destination peer report any variance upon receiving the frame.

Features

- Far End Fault (FEF)
- Loopback
- Dying Gasp
- Critical Events
- Link Trace
- Discovery
- Per VLAN Continuity Checking
- AIS / RDI / TST
- FD - Frame Delay
- FDV - Frame Delay Variance
- Advanced Fault Isolation

TRANSITION NETWORKS®

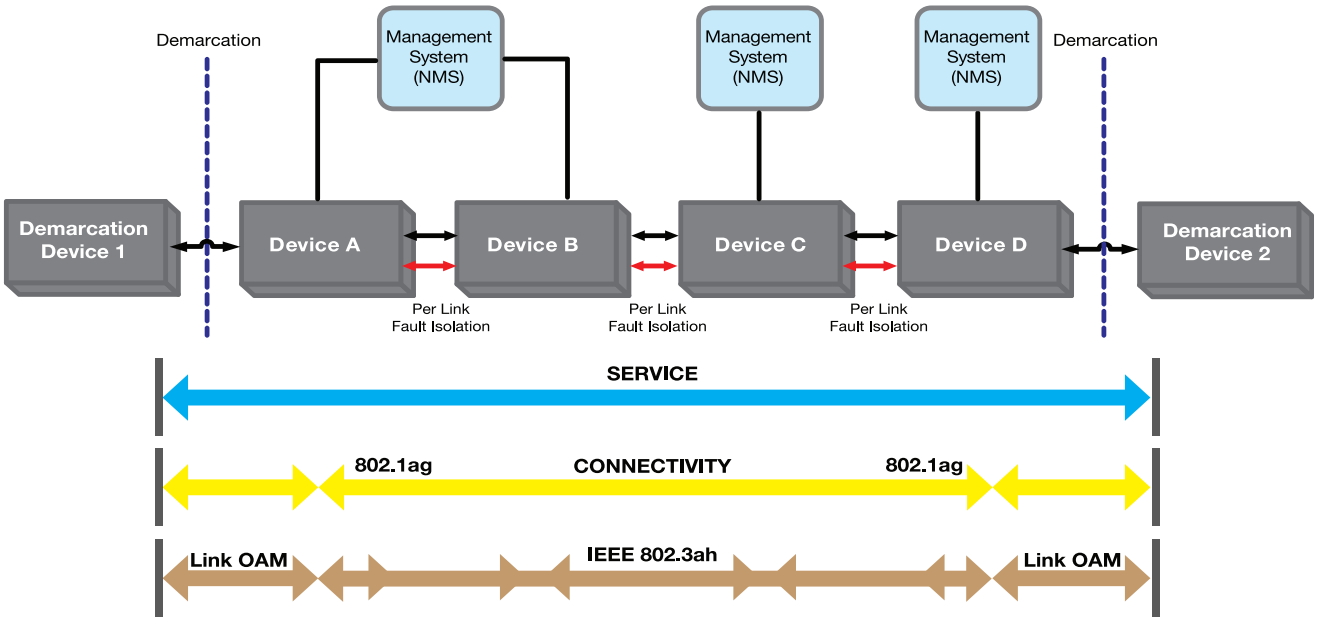
+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

802.1ag/Y.1731 Service OAM

Frame Delay Variance (FDV) measures the changes or variance in the delays between different packets and determines an average calculation. FD and FDV helps in real-time to determine if the data path is adding excessive or unwanted time variances in each frame delivery. ITU Y.1731 also defines Far End Fault (FEF), which uses an Alarm Indication Signal (AIS) for fault notifications. FEF is complementary to 802.1ag, and allows an end-point to asynchronously inform a peer of a fault condition across a network.

Application

802.1ag is generally used to deliver SLA services to small businesses all the way up to large enterprise applications—for advanced fault isolation. This class also adds some logical flows and frame delay monitoring of Ethernet traffic to ensure SLA assurance.



TRANSITION NETWORKS®

+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

802.1ag/Y.1731 w/RFC 2544

In ITU Y.1731 the Frame Loss Ratio (FLR) and the Frame Delay Variance (FDV) counters—were designed to monitor traffic that had been generated by applications on the path. Most service providers are required to know what the throughput of a path is at any given time. Monitoring traffic throughput is important to a service provider for diagnostic, monetary and regulatory reasons. Y.1731 defines Test Frames (TST) for monitoring the actual traffic throughput. ITU Y.1731 TST frames are injected by an end-point into a data path and then removed by a designated peer, which can then report back to the Network Management System (NMS) on the number of frames received and the rate at which they were received.

When used in combination with RFC 2544, TST frames can effectively test the entire circuit's bandwidth at different packet (MTU) sizes. The maximum injection rate can be the maximum known capacity of the path or equal to the Committed Information Rate (CIR). For example: If two devices are connected at 100mbps, the injection rate could be anything up to but not exceeding 100mbps. Most RFC 2544 tests are done out of service because it is preferred that the injected traffic does not interfere with real applications running on the network. To avoid disrupting real traffic, Transition's performance management products with RFC 2544 use an in-service injection of test frames that is purely supplemental to the real traffic rate, up to the defined limit on the path. The amount of real traffic is measured by the end-point and any excess is filled with ITU Y.1731 TST and RFC 2544 frames.

The TST frames are counted and removed from the path at the designated peer. The designated peer then reports the number of real and test frames received for a given interval of time. With this information the designated peer can then compare the received frames to the actual number of transmitted frames, to see if the path is performing as expected. If the number of received frames is different than the number of transmitted frames, predefined alarms or events can be sent to the operator to indicate there is a throughput issue that will need to be resolved.

TRANSITION NETWORKS®

+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

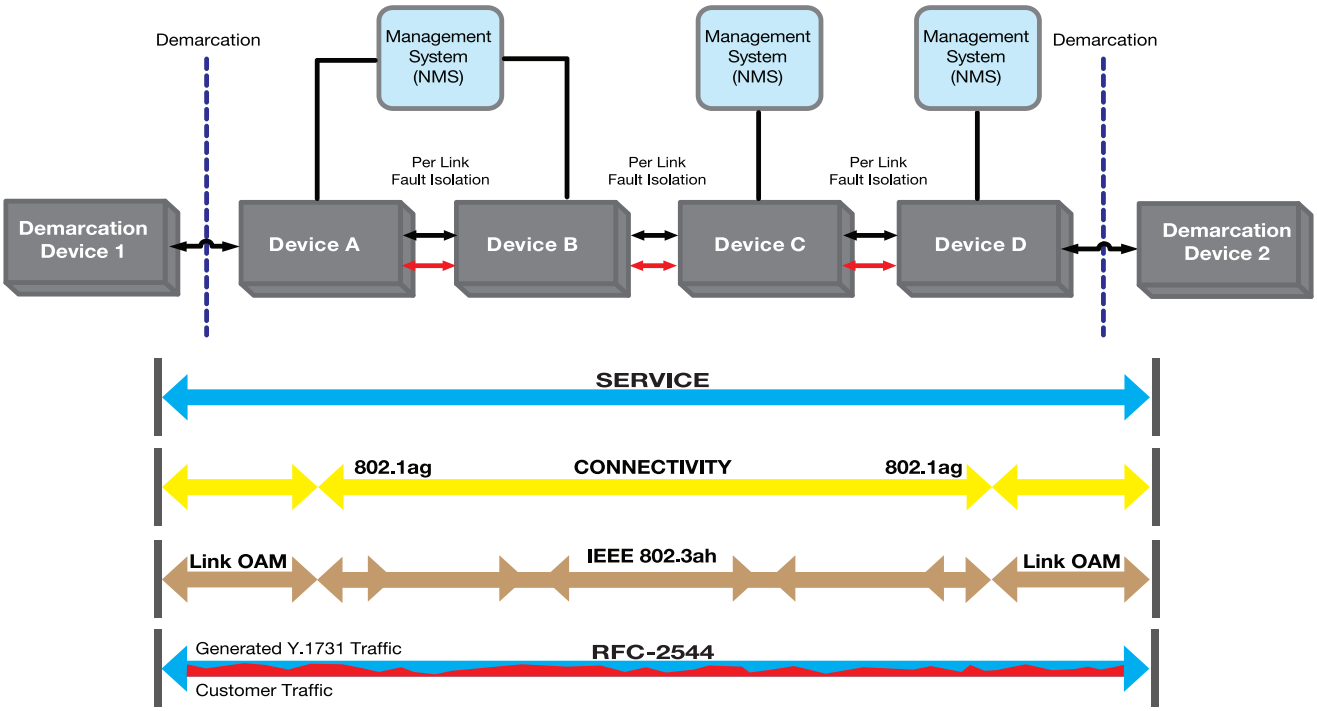
802.1ag/Y.1731 w/RFC 2544

Application

Performance Management is generally used for enterprises who require a guaranteed level of SLA performance and monitoring. For example, a financial institution that needs to have up-to-date information with no delay—as latency can mean the difference in the success of the institution. In these types of SLA agreements, legal contractual obligations are defined and agreed upon by both parties.

Features

- Frame Loss Ratio (FLR)
- Frame Delay Variance (FDV)
- Throughput Monitoring
- RFC2544 Test Frames



TRANSITION NETWORKS®

+1-952-941-7600
1-800-526-9267
info@transition.com
www.transition.com

Worldwide Headquarters & U.S. Sales

Transition Networks, Inc.
10900 Red Circle Drive
Minnetonka, MN 55343 USA
tel: 952-941-7600
toll free: 800-526-9267
fax: 952-941-2322

sales@transition.com
info@transition.com
techsupport@transition.com
www.transition.com

Part Number 900999 (0210)