Agilent Technologies

Data Over SONET/SDH (DoS) Equipment - Architectures & Test Challenges.

January 15, 2003

presented by:

Hussain Qureshi
Ronnie Neil

Your Presenters Today

Hussain Qureshi

Ronnie Neil

Agilent Technologies

Data over SONET/SDH Seminar Series

Objective

- Comprehensive tutorial seminar series for engineers involved in the design, verification, manufacturing, deployment and maintenance of Data over (next generation) SONET/SDH equipment and networks.

Series Topics

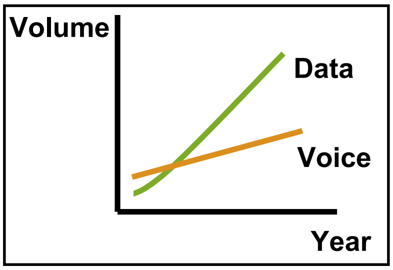
- DoS Technologies - Standards, Structures & Design.
- DoS Equipment - Architectures & Test Challenges
- SONET/SDH Jitter Measurements & Standards
- DoS Client Signal Technologies

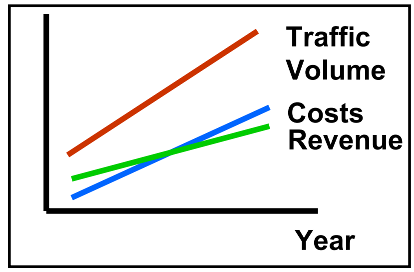
What is Data over SONET/SDH (DoS) ?

- Evolution of legacy SONET/SDH networks to transport a variety of data traffic services bandwidth-efficiently.
  - More than Packet over SONET/SDH (PoS)
  - More than Ethernet over SONET/SDH (EoS)
  - More than proprietary solutions.

“Legacy evolution not new network revolution”

DoS Market Drivers & Trends





Increase Service Revenues

- New data services, eg. Ethernet private lines, flexible bandwidth TDM private lines, SAN services.
- Enhanced existing services - eg. faster provisioning

Lower CAPEX / OPEX

- Offer new services on existing legacy network ("*legacy compatibility*").
- Maximise network bandwidth efficiency
- Reduce maintenance costs

Seminar 2: DoS Equipment

Equipment To Be Covered

- **MSPP** Multi-Service Provisioning Platform
  - aggregation & switching platform
- **MSSP** Multi-Service Switching Platform
  - switching only platform

Technologies To Be Covered

- **VC** Virtual Concatenation
  - optimum (bandwidth) sized pipe
- **LCAS** Link Capacity Adjustment Scheme
  - dynamic pipe sizing on demand
- **GFP** Generic Framing Procedure
  - standardized encapsulation for multiple services over SONET or SDH

Seminar 2: DoS Equipment

Seminar Content

- DoS technology structures recap
  - GFP, Virtual Concatenation & LCAS
- DoS equipment architectures & network topologies
  - MSPP & MSSP equipment
  - Linear, ring & mesh topologies
- DoS equipment test challenges
  - SONET/SDH error/alarm handling & protection switching
  - Payload handling including encapsulation & concatenation
- Wrap Up + question & answer session

DoS Equipment Evolution

Technology Layers & Purpose

- Client Signals
- Encapsulation Protocols
- Concatenation Processes

Encapsulation Protocols:

- **SONET/SDH is synchronous, continuous byte stream. Data signals are generally asynchronous, bursty, variable frames. Encapsulation compensates for idle time between data stream bursts.**
- **Low cost transport does not generally have OAM functionality. Encapsulation layer provides support functions to enable reliable transport of services.**

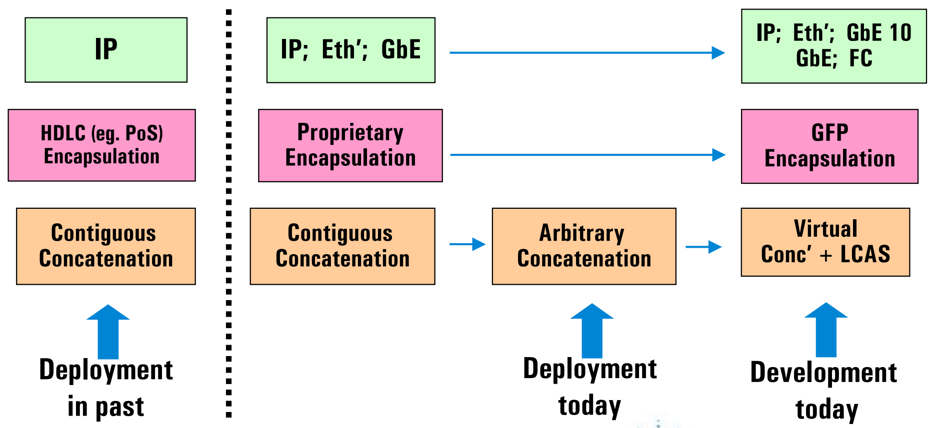
Concatenation Processes:

- **Procedure whereby multiple SONET/SDH containers can be used as one enabling transport of higher capacity signals.**

DoS Equipment Evolution

Technology Evolution (not revolution)

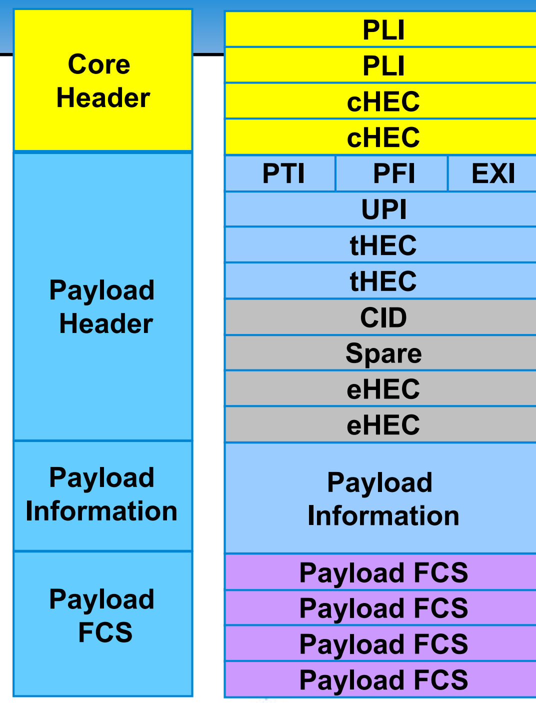
Evolution of SONET/SDH standards and equipment to more efficiently & effectively carry data traffic. *Legacy compatible*.

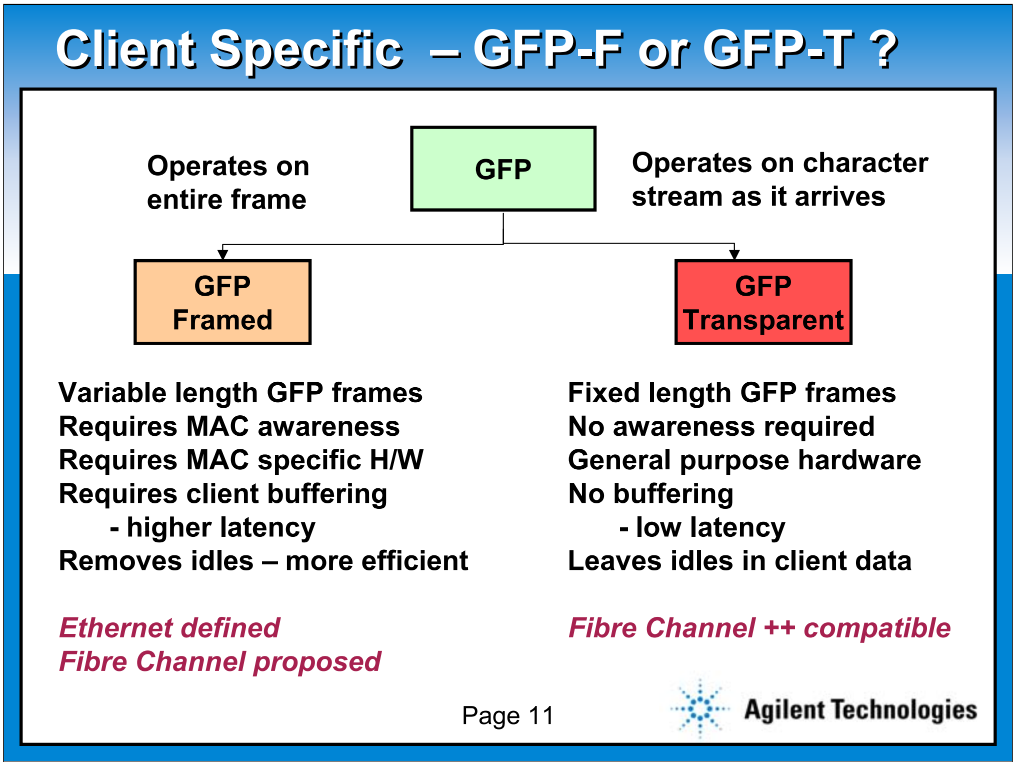


GFP Frame

The complete GFP frame.

Used for both GFP-Framed & GFP-Transparent modes of operation. (GFP-F and GFP-T respectively).





GFP supports both point-to-point and ring applications.

Currently two modes of GFP encapsulation are defined which are

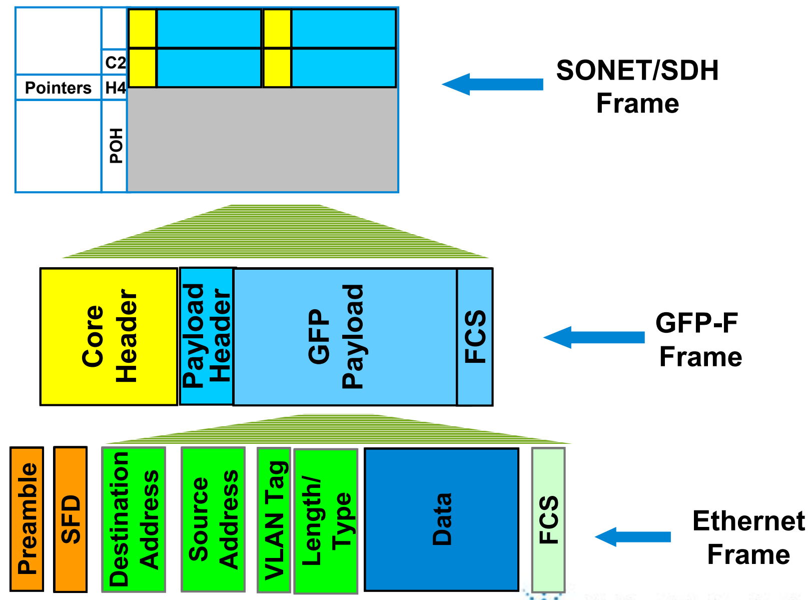
1- Frame-Mapped GFP (GFP-F) and

2- Transparent GFP (GFP-T)

Frame-Mapped GFP maps a client frame in its entirety into one GFP frame or we can also say that a single client frame is mapped into a single GFP frame. For example an Ethernet Frame mapped into a GFP Frame.

Transparent GFP is intended to facilitate the transport of block coded client signals like Fiber Channel, ESCON, FICON or even Gigabit Ethernet. The individual characters of a client signal are de-mapped from the client signal and then mapped into fixed length GFP frames. This process avoids buffering of an entire client frame for further processing into a GFP frame.

GFP-F Example - Ethernet Client



Concatenation Terminology

- **Containers**
  - **The fundamental building blocks of SONET/SDH**
- **Contiguous Concatenation**
  - **A way of ‘sticking’ together multiple containers to make one large container for carrying a larger payload**
- **Virtual Concatenation**
  - **A methodology of using multiple containers to carry a larger payload, but each container is independent when transported across the network**

What is ‘Virtual Concatenation (VC)’ ?

- Uses groups of independent SONET/SDH containers.
- Containers take different routes to destination. Different route have different delays
- Destination must remove (buffer) delay, and re-align arriving containers

	SDH	SONET
Low Order	VC groups Tributary Units VC-1/2-Xv (e.g. VC-12-5v)	VC groups Virtual Tributaries VTn-Xv (e.g. VT-1.5-7v)
High Order	VC groups Virtual Containers VC-n-Xv (e.g. VC-4-7v)	VC groups SPEs STSn-Xv (e.g. STS-1-2v)

Agilent Technologies

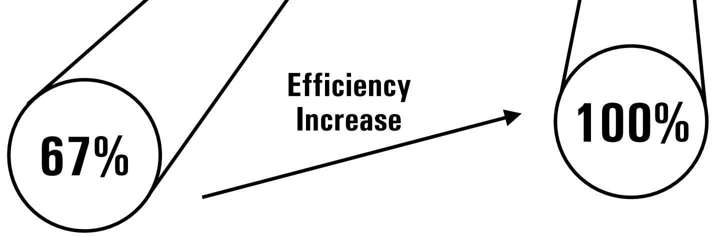
For any network equipment in the transit path that does NOT support virtual concatenation, this causes no problem whatsoever as the container is passed through transparently with no processing of the path overhead. This is a significant point when considering a migration to Virtual concatenation since only the path end points need to be Vcat ‘aware’.

A major benefit of allowing the containers to follow different routes, it is easier to utilize ‘stranded’ bandwidth. However, the downside of this is the need to buffer data at the receiver to re-align the incoming data.

Bandwidth Efficiency

Virtual Concatenation

Service	Data Rate	Contiguous Concatenation		Efficiency	Virtual Concatenation		Efficiency
		SONET	SDH		SONET	SDH	
Ethernet	10Mb/s	STS-1	VC-3	20%	VT-1.5-7v	VC-12-5v	~90%
ATM	25Mb/s	STS-1	VC-3	50%	VT-1.5-16v	VC-12-12v	98%
Fast Ethernet	100Mb/s	STS-3c	VC-4	67%	STS-1-2v	VC-3-2v	100%
Fiber Channel	200Mb/s	STS-12c	VC-4-4c	33%	STS-1-4v	VC-3-4v	100%
Gbit Ethernet	1000Mb/s	STS-48c	VC-4-16c	42%	STS-1-21v	VC-4-7v	95%



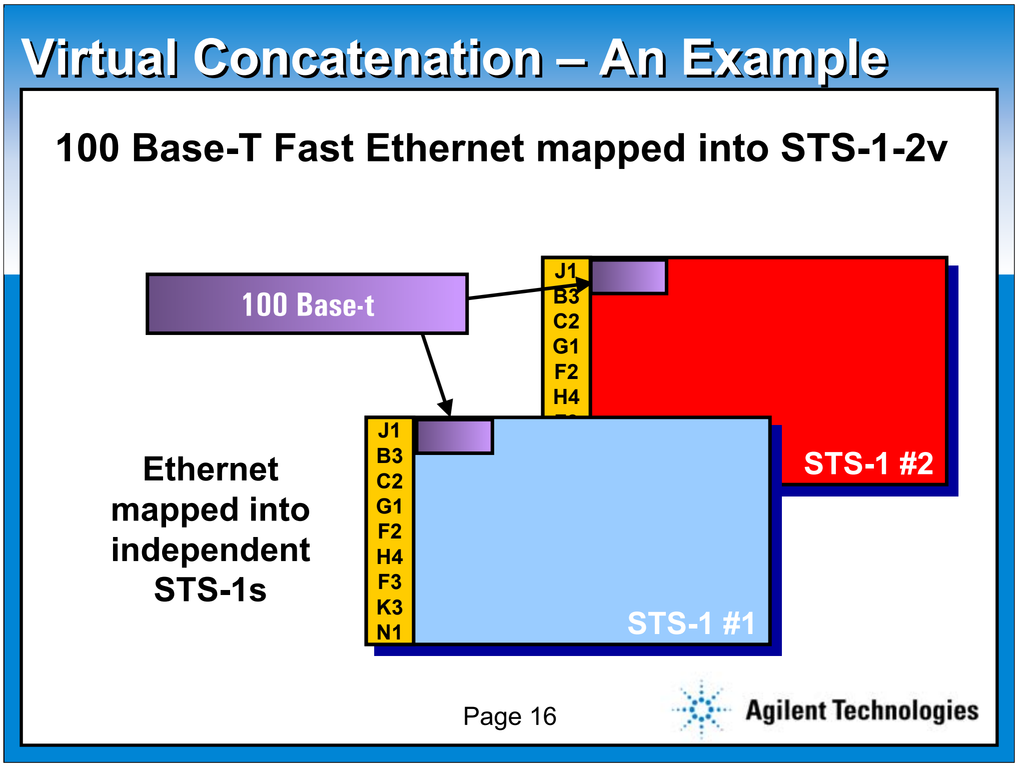
Agilent Technologies

This table shows the improvements in bandwidth efficiency that can be made by using virtual concatenation instead of contiguous concatenation.

I mentioned that an STS-3c is often used to transport 100 Mb/s fast Ethernet services. This results in a bandwidth efficiency of 67%.

By using virtual concatenation, we can use 2 STS-1s to carry the same service and the bandwidth efficiency rockets to 100%!

Even larger efficiency improvements can be made with other data services.



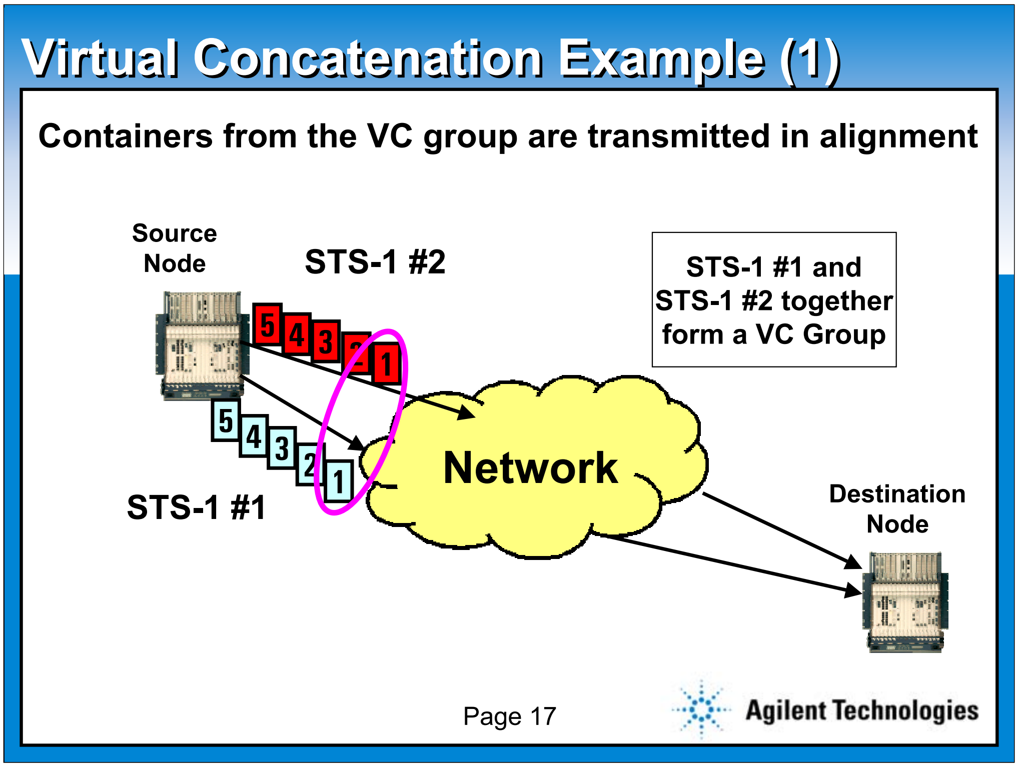
Let's look at an example of transporting a 100 Base-t, fast Ethernet service using virtual concatenation.

Two STS-1s are generally sufficient to provide enough client bandwidth to carry a 100 Base-t data stream. This is a virtual container group of size 2, and the correct term for this is an STS-1-2v.

The two STS-1s are numbered STS-1 number 1 and STS-1 number 2.

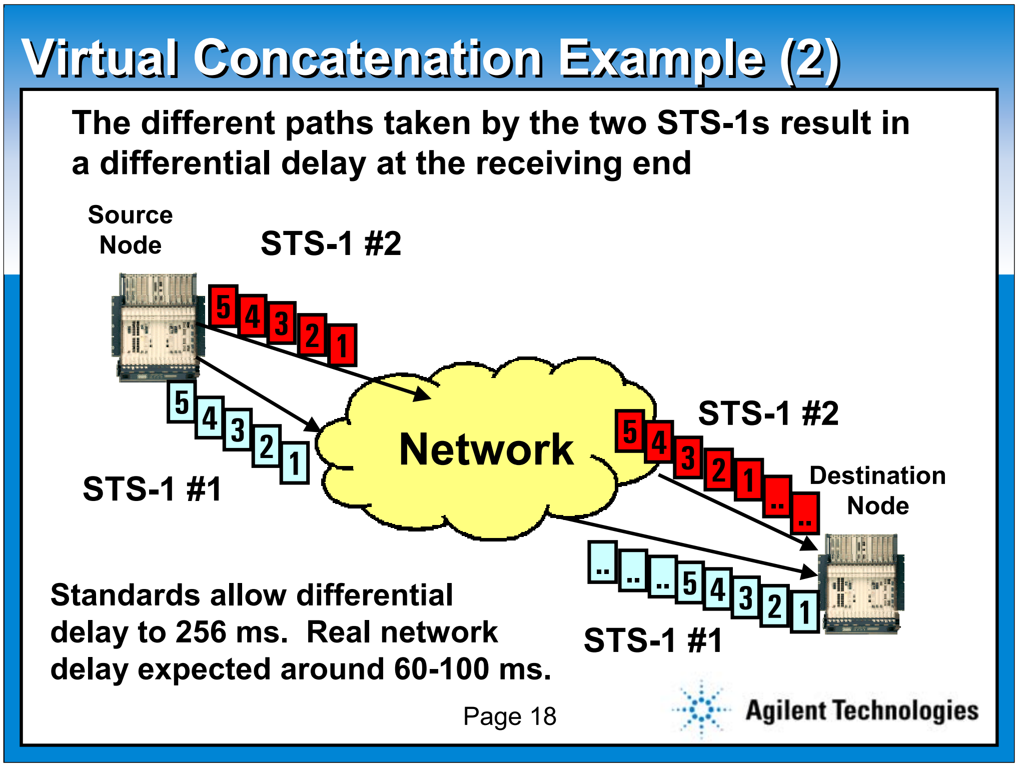
Each virtual container is filled a byte at a time, and the containers transmitted simultaneously on two different ports of a network element.

Note that in this diagram STS-1 number one is colored pale blue and STS-1 number 2 is colored red.



The pale blue boxes represent the SONET frames carrying the containers for STS-1 number 1 while the red boxes represent the SONET frames carrying the containers for STS-1 number 2.

You should note that the numbers in the boxes signify that frames with the same number on the different paths are transmitted at the same time. So, frame 1 of STS-1 number 1 is transmitted at the same time as frame 1 of STS-1 number 2 and so on.



The two STS-1s in our virtually concatenated signal have taken different routes through the network and you will see that at the destination node, frame 1 of STS-1 number 1 arrives 2 frames sooner than frame 1 of STS-1 number 2.

In order for the network element to correctly re-create the original 100 Base-t data stream, it needs to buffer Frame 1 of STS-1 number 1 until frame 1 of STS-1 number 2 arrives. When this happens, the original signal can be re-created and the process continues so long as data is sent across the network.

From this example, it can be seen that there are two key things that need to be achieved.

Firstly, the receiving equipment needs some method of re-aligning the containers arriving on the different paths.

Secondly, some storage area, or buffer memory, is required to compensate for the differential delay between the two paths.

It can also be seen that as the delay, or the number of members of the Vcat group increases, more data needs to be stored. It is likely that the buffer memory size in real equipment will result in some trade-off between delay compensation and Vcat group size.

Removing VC Differential Delay

- The receiving equipment must re-align the arriving SONET/SDH containers.
- This is accomplished by
  - buffering the incoming data.
  - using a sequence indicator in the H4 byte in the path overhead of all members of the high order VC group to put containers into the correct order.
- A similar frame and multi-frame indicator scheme is implemented in the K4 byte for low order VC groups.

Contiguous vs Virtual Concatenation

Contiguous

- Poor granularity of container size
- Container travels along same path
- Requires all elements in path to understand concatenation indication
- Independent of network management system
- No differential delay

Virtual

- Flexible granularity (high order and low order)
- Individual containers can take separate paths
- Only the end elements need understand the concatenation arrangement
- Requires control from the network management system
- Individual containers may experience differential delay

Link Capacity Adjustment Scheme

Requirement

- Allows containers to be added/removed from a group as the data bandwidth requirement changes
- Also provides ability to remove links that have failed
- Addition and removal of containers must be hitless

Operation

- A control packet is used to configure the path between source and destination
- The control packet is transmitted in the H4 byte for high order and K4 byte for low order virtual concatenation
- The control packet describes the link status during the next control packet
- Changes are sent in advance so the receiver can switch as soon as the new configuration arrives

DoS Technology Standards

GFP & LAPS Encapsulations

Existing (Fully Ratified)

• ITU-T G.7041/Y.1303	(Dec 2001)	GFP (Framed & Transparent)
• ITU-T X.85/Y.1321	(Mar 2001)	LAPS (IP over SDH)
• ITU-T X.86/	(Feb 2001)	LAPS (Ethernet over SDH)

Virtual Concatenation & LCAS

Existing (Fully Ratified)

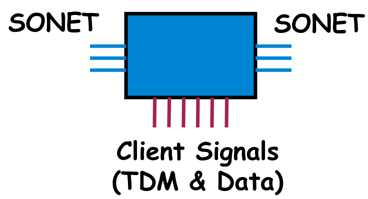
• ITU-T G.707/Y.1322	(Sep 2002)	SDH VC
• ITU-T G.7042/Y.1305	(Nov 2001)	LCAS
• ANSI T1.105a-2002	(2002)	SONET VC & LCAS

Seminar 2: DoS Equipment

Seminar Content

- DoS technology structures recap
  - GFP, Virtual Concatenation & LCAS
- DoS equipment architectures & network topologies
  - MSPP & MSSP equipment
  - Linear, ring & mesh topologies
- DoS equipment test challenges
  - SONET/SDH error/alarm handling & protection switching
  - Payload handling including encapsulation & concatenation
- Wrap Up + question & answer session

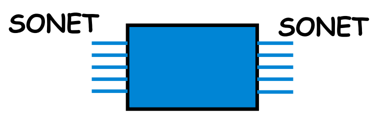
Key DoS Equipment



Next Gen SONET/SDH Multi-Service Provisioning Platform (MSPP)

Focus on add/drop multiplexing (aggregation) and grooming as well as providing switching (ie. X-connect) capability.

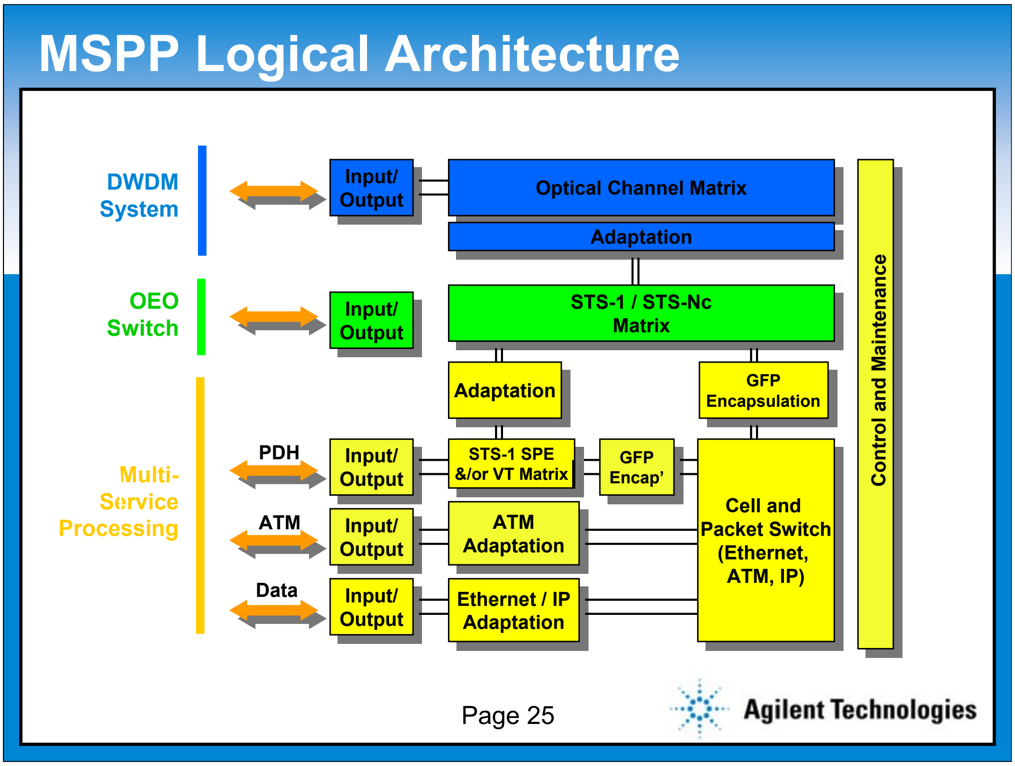
Examples: Cisco ONS 15454
Ciena Metro Director



Next Generation SONET/SDH Multi-Service Switching Platform (MSSP)

Focus on bandwidth management (ie. switching) via large, non-blocking, digital cross-connect.

Examples: Cisco ONS 15600
Ciena Core Director

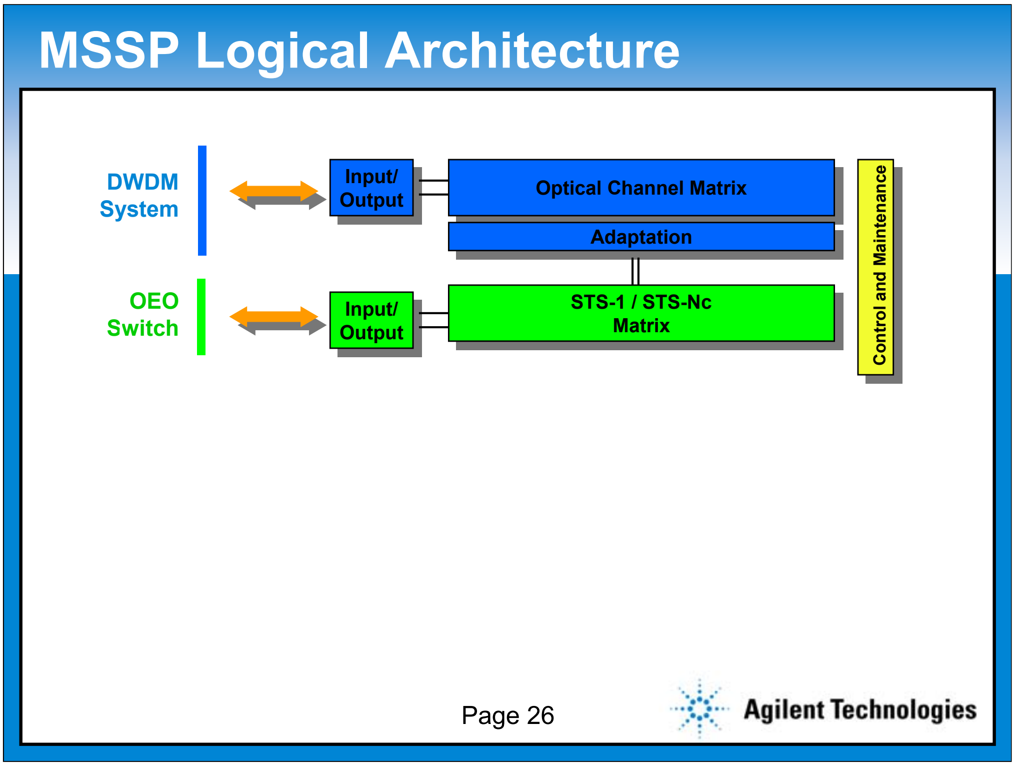


This diagram represents the same concept. This shows how multiple functions are merged into a single device in a NG SONET/SDH MSP. The yellow boxes provide the interfaces and infrastructure for receiving and transmitting a range of technologies including PDH, ATM, Ethernet and IP.

This connects through adaptation components to a SONET/SDH stratum. This contains optical interfaces to handle SONET/SDH from STS1 upwards. Finally the blue area shows the line side of the device, in this case a DWDM system.

Different NEMs devices will contain some or all of these sections and with differing degrees of priority to each. For example a Cisco 15454 will have all the yellow and a lot of green. A Ciena K2 will be similar, but Ciena's Core Director will major on the Blue and green areas with little capability in the yellow area.

The main thing to take from this diagram and the previous is the convergence of multiple technologies and a large number of interfaces and functions within a single device.

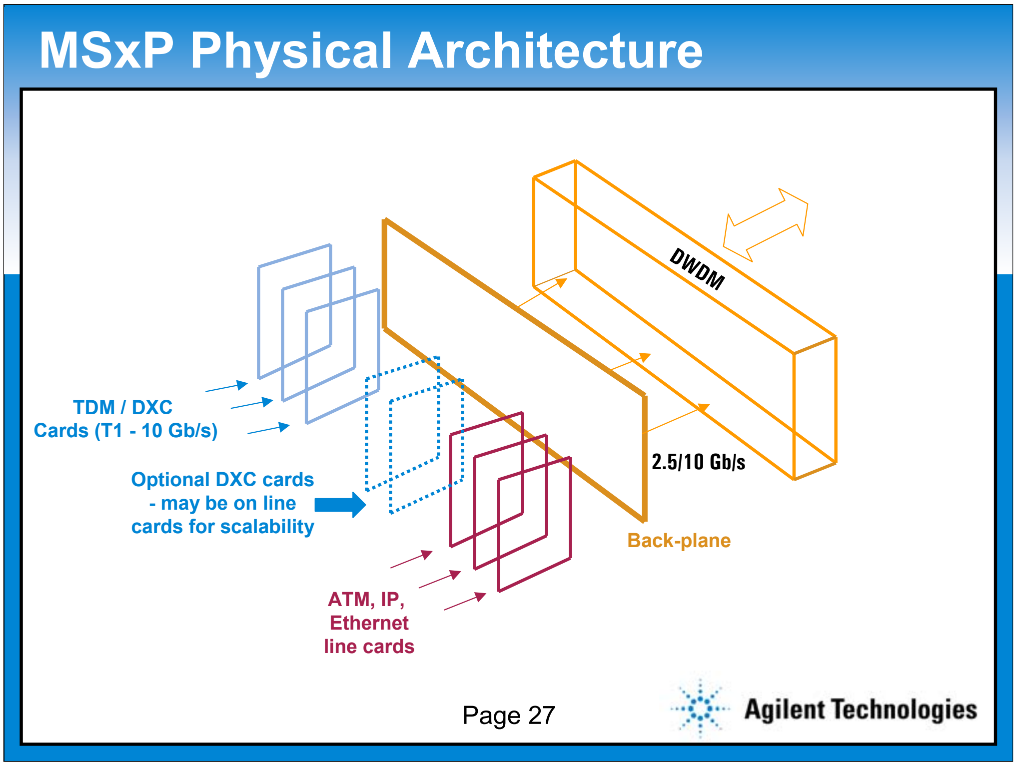


This diagram represents the same concept. This shows how multiple functions are merged into a single device in a NG SONET/SDH MSP. The yellow boxes provide the interfaces and infrastructure for receiving and transmitting a range of technologies including PDH, ATM, Ethernet and IP.

This connects through adaptation components to a SONET/SDH stratum. This contains optical interfaces to handle SONET/SDH from STS1 upwards. Finally the blue area shows the line side of the device, in this case a DWDM system.

Different NEMs devices will contain some or all of these sections and with differing degrees of priority to each. For example a Cisco 15454 will have all the yellow and a lot of green. A Ciena K2 will be similar, but Ciena’s Core Director will major on the Blue and green areas with little capability in the yellow area.

The main thing to take from this diagram and the previous is the convergence of multiple technologies and a large number of interfaces and functions within a single device.



This is a generic architecture of an MSP.

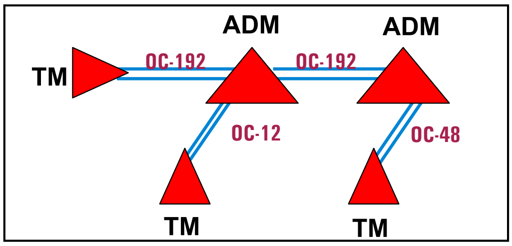
We have SONET cards, separate XC cards: some to go down to STS-1 level and others to go down to VT/TU level, and we have Ethernet cards. This shows the concept of multiple ports operating at a variety of different rates and employing a range of technologies

All this goes into a high bandwidth backplane.

In the future, they may connect to an Optical ADM but they're not there yet.

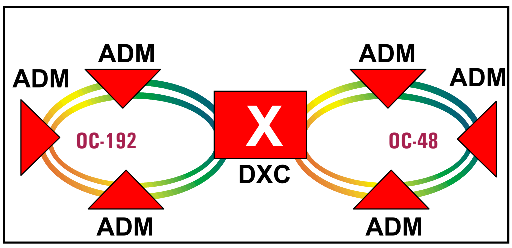
SONET/SDH Legacy Topologies

- **Linear Point to Point**



- Terminal (TM) & add/drop (ADM) nodes.
- Service may originate or terminate on any node (bi-directional).

- **Ring**



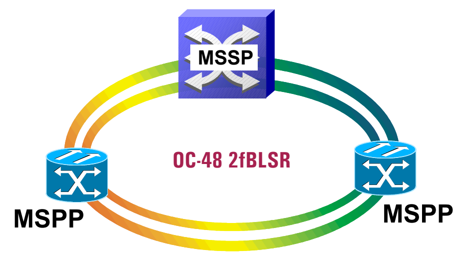
- Add/drop nodes.
- Uni- or bi-directional.
- Line- or path-switched protection schemes.
- 1+1 linear connection between rings.

Agilent Technologies

TO help explain the applications for OmniBER XM we need to study some common network topologies. We’ll look at Point-to-Point, Ring and mesh networks and a few variations on those themes.

Switching

- **2 Fiber Bi-directional Line Switched Ring (2fBLSR)**
  - 2fBLSR allocate half available bandwidth for protection, eg. in OC-48, STS 1-24 are for working traffic and STS 25-48 for protection
  - Fibers run in opposite directions, each carrying traffic in STS 1-24
  - If break in one fiber occurs, traffic switches to STS 25-48 on other fiber. Whole line (ie. all channels) is switched.
  - X-Connect makes switch driven by line card PM error thresholds or LOS, LOF, B2 & AIS-L



2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

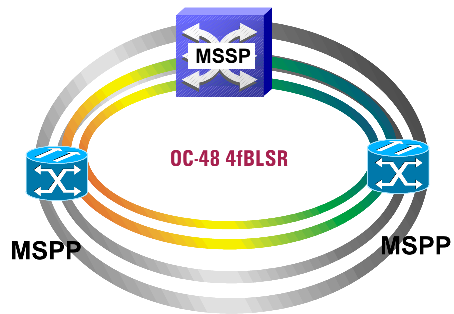
In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber

Switching

- **4 Fiber Bi-directional Line Switched Ring (4fBLSR)**
- 4fBLSR utilises span and ring protection schemes
- Span switching restores between adjacent nodes by using protection fiber bandwidth between the nodes
- Ring switching provides network protection by wrapping circuits on to protection bandwidth
- Very robust, can withstand 2 network failures
- X-Connect makes switch driven by line card PM error thresholds or LOS, LOF, B2 & AIS-L



Agilent Technologies

4fBLSR utilises both span and ring protection schemes

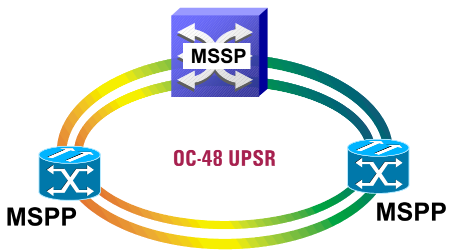
If a failure occurs between 2 adjacent nodes, Span switching restores by using protection fiber bandwidth (ie switching to a different fiber) between the 2 nodes

Ring switching provides network protection by wrapping circuits on to the protection bandwidth in a similar manner to 2F BLSR

4fBLSR is a very robust architecture that can withstand 2 simultaneous network failures

Switching

- **Uni-directional Path Switched Ring (UPSR)**



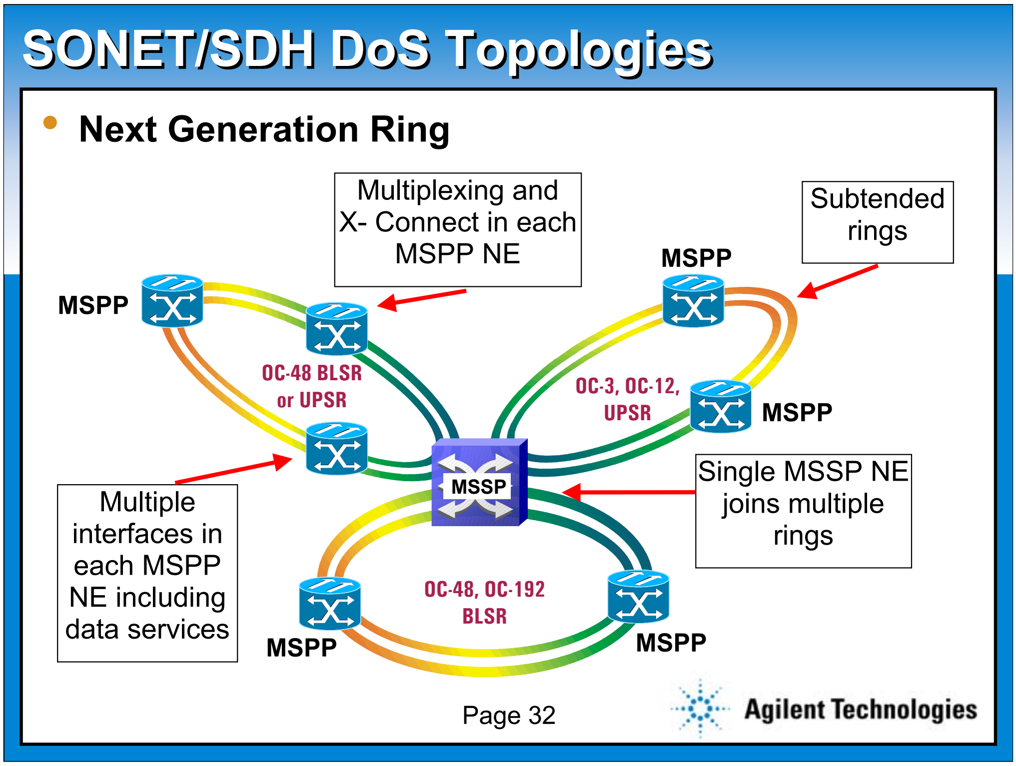
- UPSRs provide duplicate fibers around the ring
- Working traffic flows one way, protection traffic in the other
- If a problem occurs, receiving node switches to path coming in opposite direction
- Both fibers carry ALL traffic. Switching is at path level
- X-Connect makes switch driven by line card PM error thresholds or AIS-P, B3, UNEQ-P & TIM-P.

Agilent Technologies

UPSRs provide duplicate fibers around the ring. The working traffic flows one way on one fibre, while the protection traffic flows in the other direction on the other fiber. Both fibers carry ALL traffic

If a problem occurs, the receiving node switches to the equivalent path coming in opposite direction

Switching decision is made by the NE processor based on PM data from the line card. The DXC activates the switch at path level.



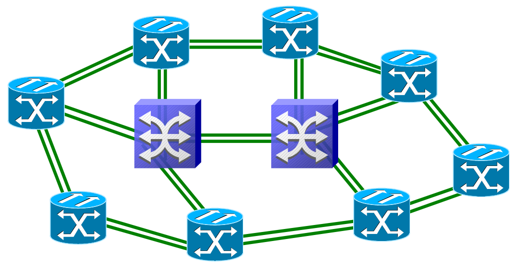
MSPs can deliver greater efficiency in several ways. Many next generation MSPs can subtend multiple rings. This provides the chance to use a central NE as a solution for attaching local loops to a regional backbone. Effectively one new MSP may replace two NE's that were previously used as the interfaces from one ring to the next. Subtending rings from single NE in this way reduces the number of nodes and cards required and reduces external shelf-to-shelf cabling.

Local loops can run at OC-3 or OC-12, while the backbone loop(s) can run at OC-48 or OC-192.

An example seen in a customer test lab is a 16 node ring with 16 subtended rings linked to each of the 16 nodes !

SONET/SDH DoS Topologies)

- **Path Protected Mesh Network (PPMN)**



- PPMN extends UPSR to cover the meshed architecture of several interconnected rings
- PPMN creates 2 alternative routes between source and destination nodes that do not lie on the same ring, but link through a network of meshed connections

MSPs can deliver greater efficiency in several ways. Many next generation MSPs can subtend multiple rings. This provides the chance to use a central NE as a solution for attaching local loops to a regional backbone. Effectively one new MSP may replace two NE's that were previously used as the interfaces from one ring to the next. Subtending rings from single NE in this way reduces the number of nodes and cards required and reduces external shelf-to-shelf cabling.

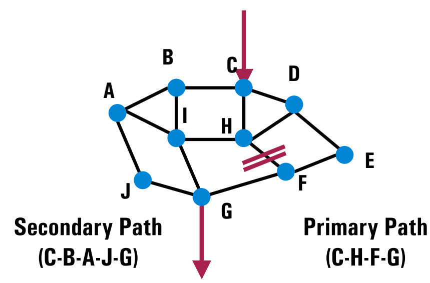
Local loops can run at OC-3 or OC-12, while the backbone loop(s) can run at OC-48 or OC-192.

An example seen in a customer test lab is a 16 node ring with 16 subtended rings linked to each of the 16 nodes !

SONET/SDH DoS Topologies

- **PPMN Protection Switching Operation**
  - Redundant circuit paths diversely routed upon initial connection request
  - Based on open shortest path algorithm
  - Paths switched individually. Switch on one channel must not affect any other channels
  - Switch over in less than 50ms

A-B-C-H-F-G-J form a "UPSR" ring for the circuit connection C-G.



Path Protected Mesh Networking (PPMN)

There are many benefits to implementing a PPMN. These include:

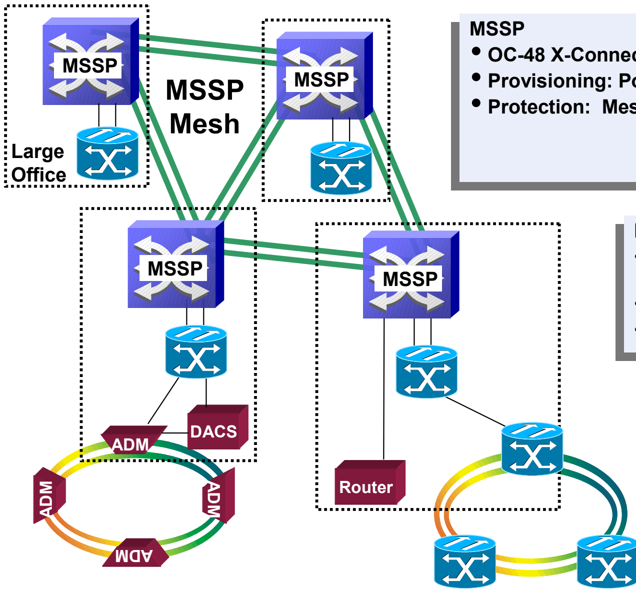
*** Optical path protection over meshed topology - Similar to UPSR protection**

*** Redundant circuit paths diversely routed upon initial connection request**

- Based on open shortest path algorithm

*** Less than 50ms switch over**

Example DoS Network



MSSP
- OC-48 X-Connect with STS-1 level grooming
- Provisioning: Point & Click
- Protection: Mesh, 1+1, 4F BLSR, 2F BLSR, UPSR

Ring (4F BLSR, 2F BLSR, UPSR)

MSPP
- Aggregate DS-3, Gig E, OC-3, OC-12 up to OC-48 or OC-192
- Provisioning: Point & Click
- Protection: Ring, 1+1, Mesh

MSPP/MSSP Control Plane
- Common Control Plane for automated end-to-end provisioning across MSPP and MSSP- future.

Seminar 2: DoS Equipment

Seminar Content

- DoS technology structures recap
  - GFP, Virtual Concatenation & LCAS
- DoS equipment architectures & network topologies
  - MSPP & MSSP equipment
  - Linear, ring & mesh topologies
- DoS equipment test challenges
  - SONET/SDH error/alarm handling & protection switching
  - Payload handling including encapsulation & concatenation
- Wrap Up + question & answer session

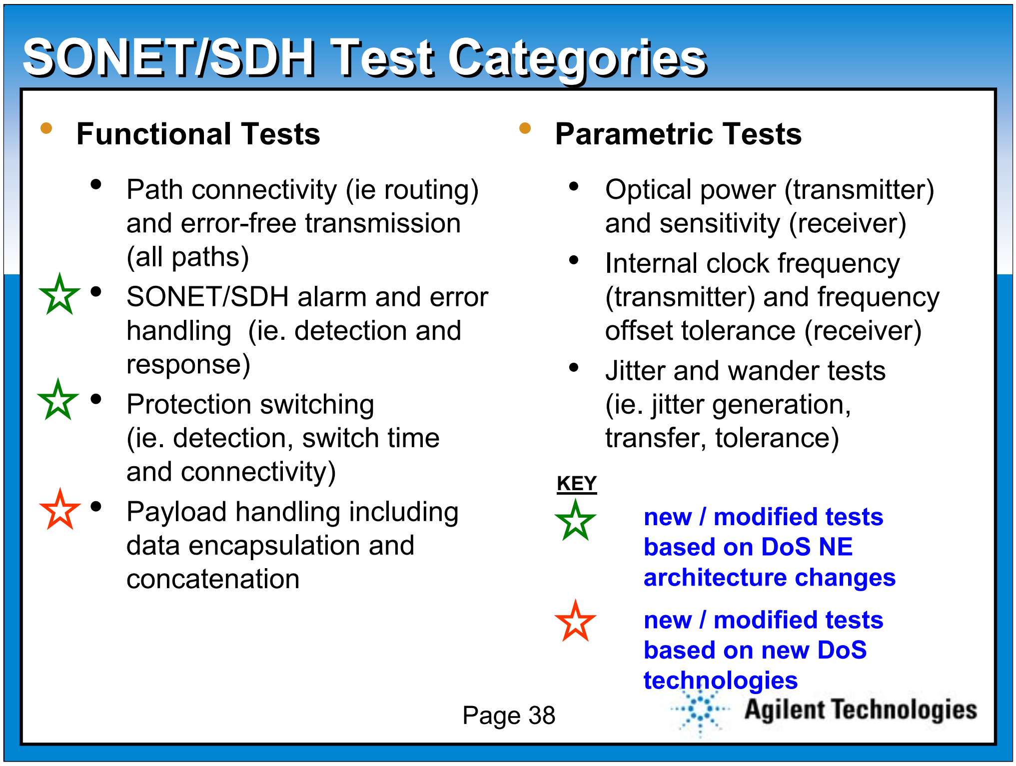
Agilent Technologies

DoS Equipment – New Test Challenges

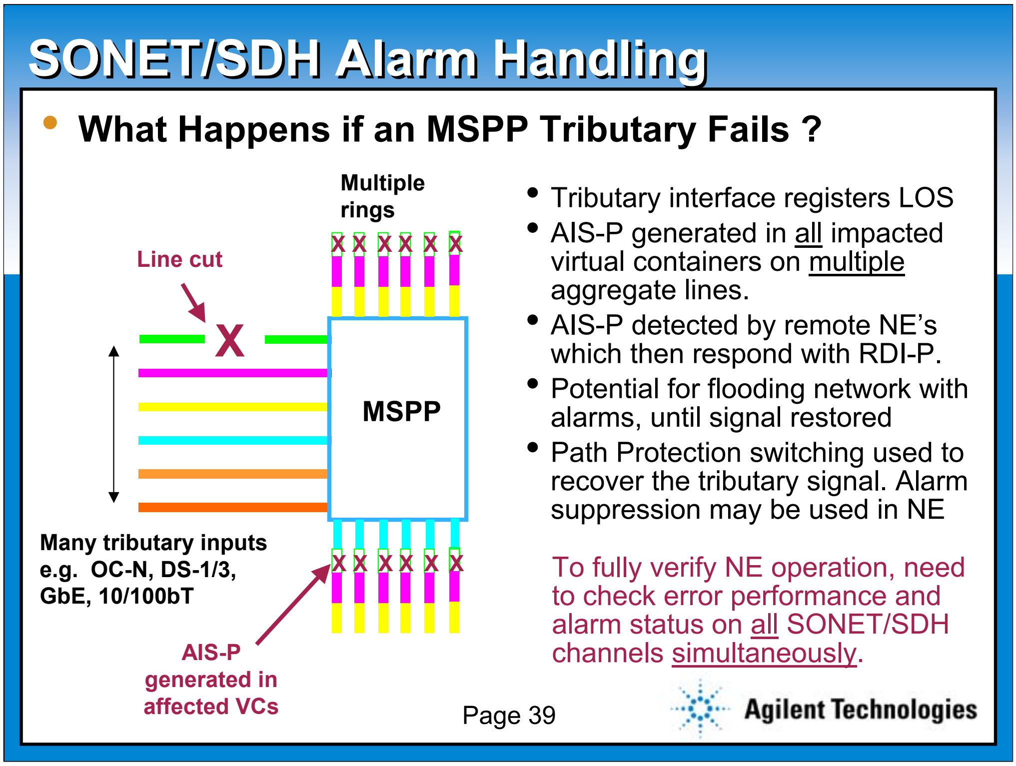
- **Legacy SONET/SDH**
  - Low port counts
  - TM, ADM & DXC separate NEs
  - Limited PDH/ SONET / SDH interfaces
  - Protection switching from card/card
  - Single rings & Point to Point topologies only
  - TDM /SONET / SDH payload mappings only
  - Contiguous concatenation only
- **Data over SONET/SDH**
  - High port counts - many ports per card
  - Single NE ADM + multi-service switch (eg. SONET / Ethernet)
  - Single NE covers PDH/ SONET/ SDH (DS-1 to OC-192/STM-64) plus data signal interfaces
  - Protection switching by card (line) or integral DXC (path/line)
  - Support for multiple rings and mesh network topologies
  - New technology - encapsulated data payload mappings
  - New technology - virtual concatenation procedures

Agilent Technologies

Deploying MSPs in the network brings significant benefits to network operators in terms of greater efficiency and flexibility coupled with lower running costs and easier provisioning. However for the NEM the MSPs present significant engineering challenges on all fronts – software, hardware and test. It’s testing we’re interested in of course, and here are some of the new challenges that have to be met.



Deploying MSPs in the network brings significant benefits to network operators in terms of greater efficiency and flexibility coupled with lower running costs and easier provisioning. However for the NEM the MSPs present significant engineering challenges on all fronts – software, hardware and test. It's testing we're interested in of course, and here are some of the new challenges that have to be met.



What happens if there's a cut in the tributary interface in an MSP:

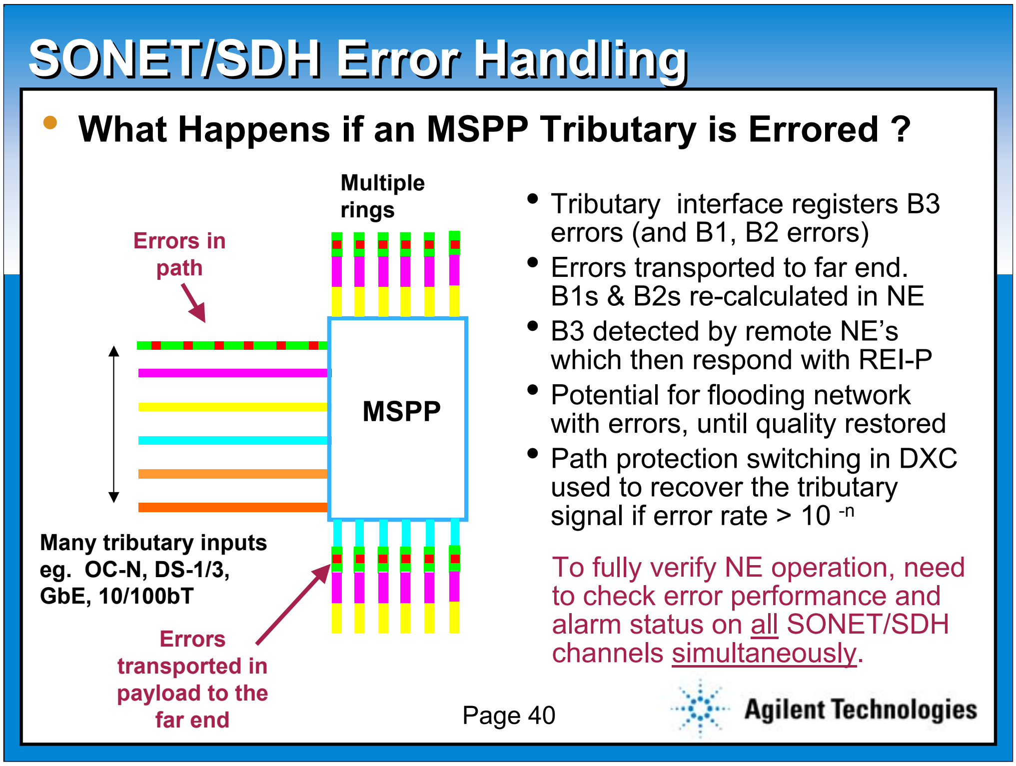
- First, the tributary interface registers a LOS

- Then, an AIS-P is generated in all impacted virtual containers on multiple aggregate lines. This is across all output rings, all at the one time.

- Then, an AIS-P is detected by all Network Elements that's associated with rings which then respond with an RDI-P

- Therefore, there's potential for flooding the network with alarms until the signal is restored. And that's significant. In the past, it was acceptable to test one channel at a time, but now you can error multiple rings on multiple paths at the same time. Errors traveling round the rings will invoke responses from the NEs around each ring and very quickly there will be literally a flood of errors. The only way that you can measure the behaviour of network elements in this type of environment is to use simultaneous multi-channel, multi-port testing. There is no other way – unless your prepared to make some very brave assumptions and take some huge risks.

- Finally, protection switching is used to recover the tributary signal



What happens if there's a cut in the tributary interface in an MSP:

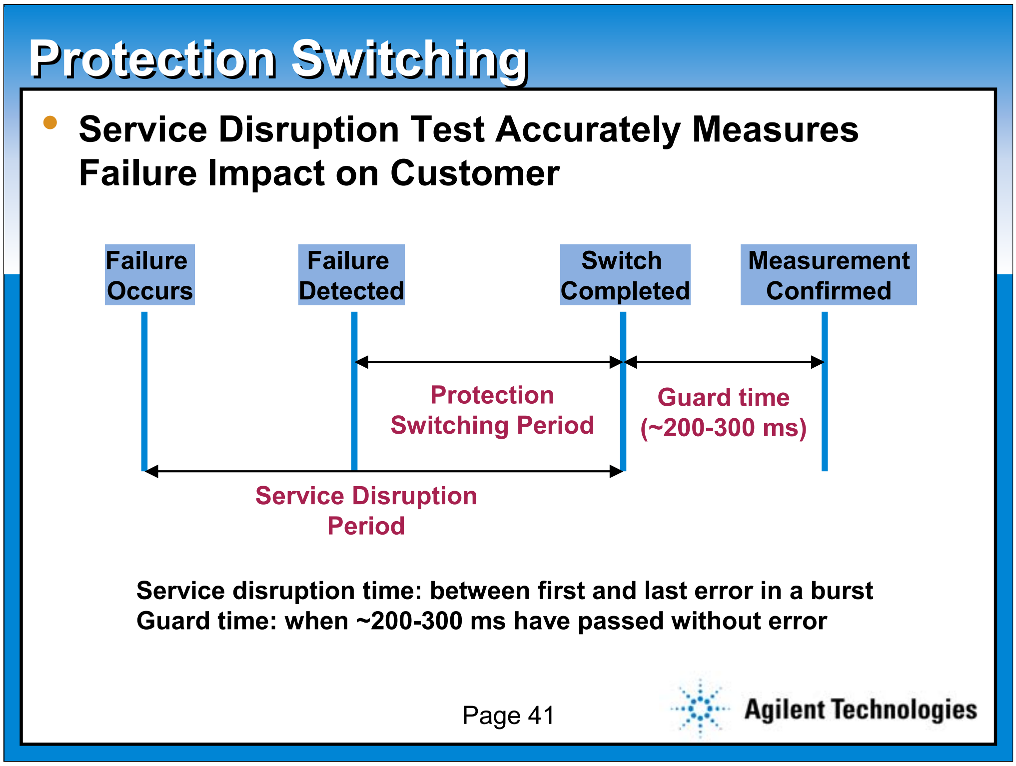
- First, the tributary interface registers a LOS

- Then, an AIS-P is generated in all impacted virtual containers on multiple aggregate lines. This is across all output rings, all at the one time.

- Then, an AIS-P is detected by all Network Elements that's associated with rings which then respond with an RDI-P

- Therefore, there's potential for flooding the network with alarms until the signal is restored. And that's significant. In the past, it was acceptable to test one channel at a time, but now you can error multiple rings on multiple paths at the same time. Errors traveling round the rings will invoke responses from the NEs around each ring and very quickly there will be literally a flood of errors. The only way that you can measure the behaviour of network elements in this type of environment is to use simultaneous multi-channel, multi-port testing. There is no other way – unless your prepared to make some very brave assumptions and take some huge risks.

- Finally, protection switching is used to recover the tributary signal



What happens if there's a cut in the tributary interface in an MSP:

- First, the tributary interface registers a LOS

- Then, an AIS-P is generated in all impacted virtual containers on multiple aggregate lines. This is across all output rings, all at the one time.

- Then, an AIS-P is detected by all Network Elements that's associated with rings which then respond with an RDI-P

- Therefore, there's potential for flooding the network with alarms until the signal is restored. And that's significant. In the past, it was acceptable to test one channel at a time, but now you can error multiple rings on multiple paths at the same time. Errors traveling round the rings will invoke responses from the NEs around each ring and very quickly there will be literally a flood of errors. The only way that you can measure the behaviour of network elements in this type of environment is to use simultaneous multi-channel, multi-port testing. There is no other way – unless your prepared to make some very brave assumptions and take some huge risks.

- Finally, protection switching is used to recover the tributary signal

Protection Switching

- **Why MSPP Protection Switching is More Complex**
  - With legacy ADMs, where the switch is to another port or card, it is possible to estimate the worst case position of a line card within the NE, and test the worst case scenario to the ITU-T/GR-253 50ms limit.
  - In MSPPs, Path Protection Switching involves the use of the integral X-connect and means that it is no longer possible to know which path will be used, and which path is the worst case. Hence all possible paths must be tested for correct connectivity and compliance to the ITU-T/GR-253 50ms limit.
  - Out of 1000s of channels, 100s could switch at the same time - how to verify that the correct connectivity of all channels was maintained.
  - Path protection switching is primarily implemented in software, not hardware, bringing a requirement for test at each software release

To fully verify NE operation, need to check switching times and correct connectivity on all SONET/SDH channels simultaneously.

What happens if there's a cut in the tributary interface in an MSP:

- First, the tributary interface registers a LOS

- Then, an AIS-P is generated in all impacted virtual containers on multiple aggregate lines. This is across all output rings, all at the one time.

- Then, an AIS-P is detected by all Network Elements that's associated with rings which then respond with an RDI-P

- Therefore, there's potential for flooding the network with alarms until the signal is restored. And that's significant. In the past, it was acceptable to test one channel at a time, but now you can error multiple rings on multiple paths at the same time. Errors traveling round the rings will invoke responses from the NEs around each ring and very quickly there will be literally a flood of errors. The only way that you can measure the behaviour of network elements in this type of environment is to use simultaneous multi-channel, multi-port testing. There is no other way – unless your prepared to make some very brave assumptions and take some huge risks.

- Finally, protection switching is used to recover the tributary signal

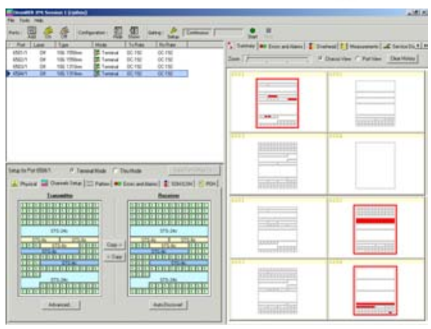
Protection Switching

- **A Typical MSPP Protection Switching Test**
  - Check switching thresholds by injecting errors and alarms in all or selected channels simultaneously.
    - Inject error ratio up to just below thresholds. Then increase to just above thresholds. Did DUT switch?
    - Inject LOS, LOF. RDI-L, RDI-P, AIS-L, AIS-P. Did switch occur?
  - Check switching time on all channels simultaneously.
    - Did all channels actually switch? And did they switch in < 50ms?
    - Were the un-switched channels affected in any way by the switch? (Check for errors across all channels)
  - Check correct connectivity on all channels simultaneously.
    - Compare expected J1 bytes against actual J1 bytes.

So to round up on switching. This is the procedure you'd follow to test protection switching on an MSP. This has been validated with a customer and seen in operation in there test lab. (although there existing equipment couldn't provide the final connectivity check).

Agilent OmniBER XM

- **An Example Multi-Channel / Multi-Port Analyzer**



- Measure BER, and inject error / alarm bursts, on all channels, on all ports, simultaneously.
- Stimulate & measure protection switch times on all channels, on all ports, simultaneously.
- Verify (post protection switched) correct path connectivity on all channels, on all ports, simultaneously (by comparing received vs expected J1 bytes).

Agilent Technologies

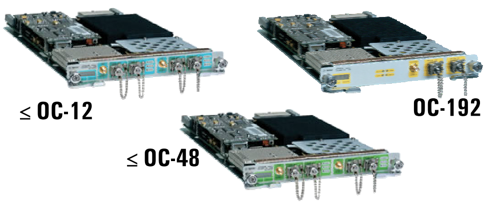
So to round up on switching. This is the procedure you'd follow to test protection switching on an MSP. This has been validated with a customer and seen in operation in there test lab. (although there existing equipment couldn't provide the final connectivity check).

OmniBER XM – Solution Components

4 Slot Chassis

- Width 19”
- Height 2U (3.5”)
- Multiple chassis may be daisy chained

Smart instrument modules

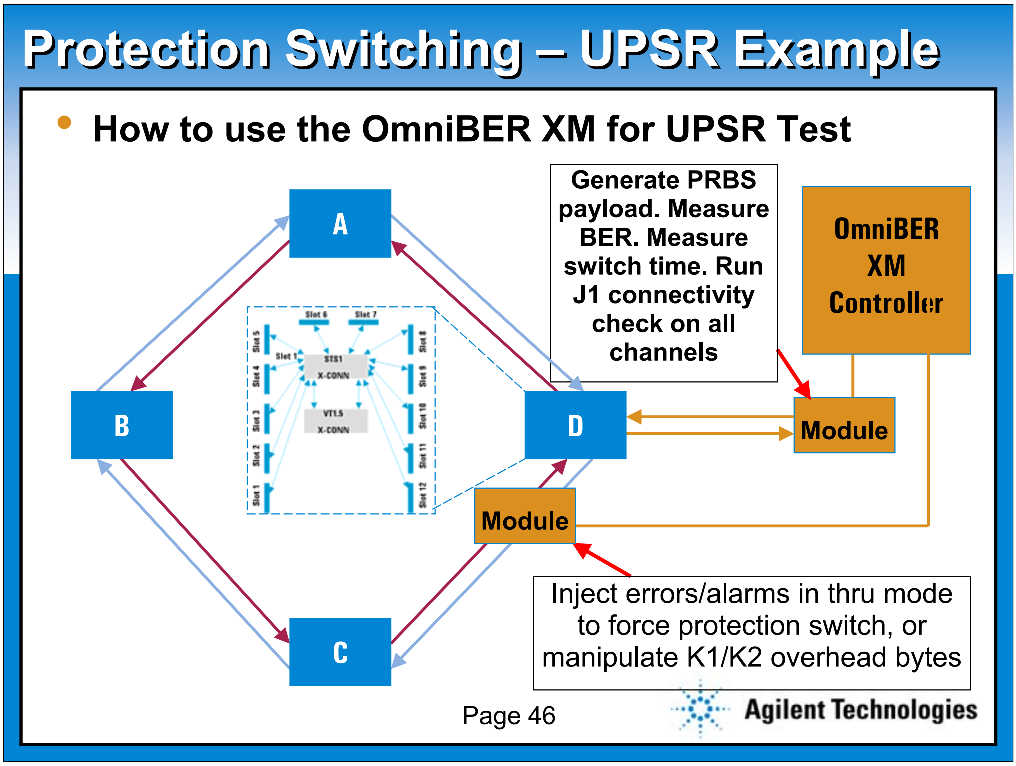


- Flexible / upgradable FPGA based instrument
- SCPI and TCL control

- System Controller (Pentium III)
- 2 Integrated LAN Ports

System controller

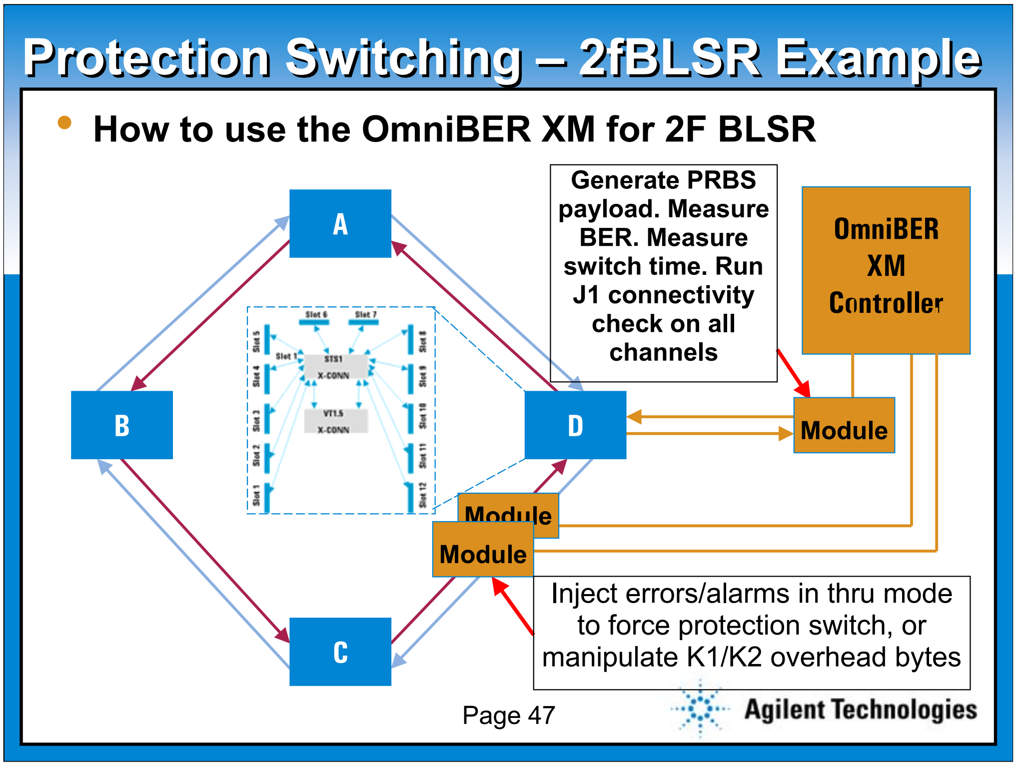
- Flexible, scaleable
- Multi-module, multi-port, multi-rate, multi-channel, multi-user, multi-tech



So how do we actually measure switch performance with the OmniBER XM?

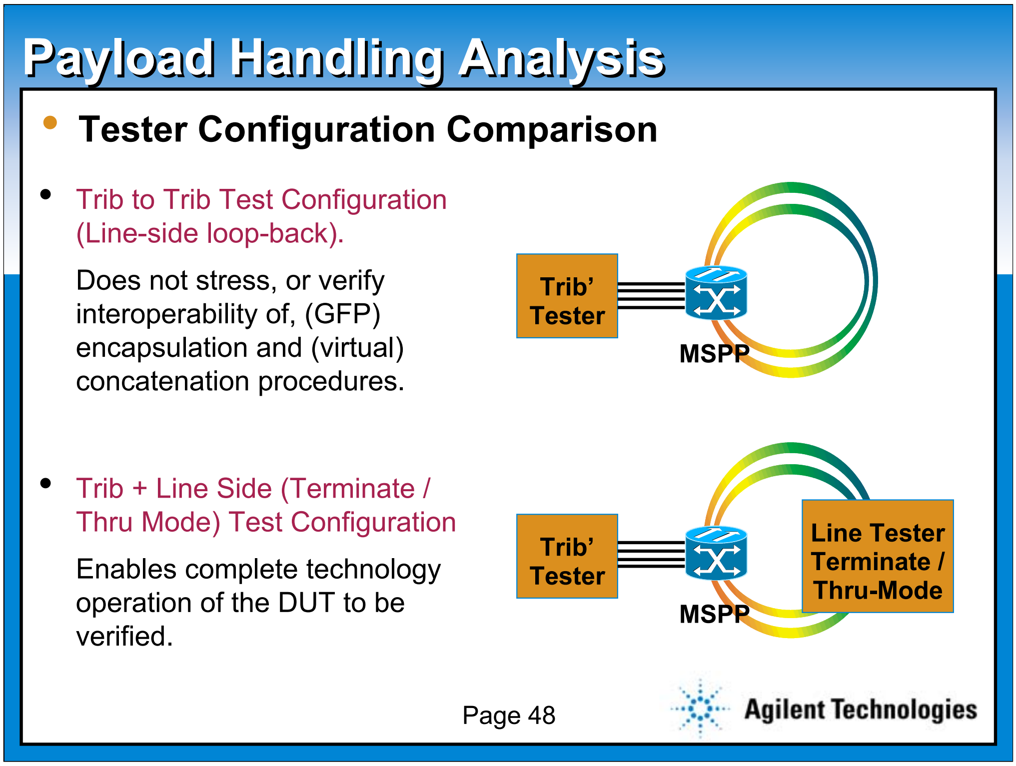
When using an XM to test switching times and connectivity in a BLSR network, this is the likely set-up. One port (or module) in through mode is used to inject errors and alarms or to manipulate K1/K2 overhead bytes in order to force protection switches to occur. A second module is connected to the NE of interest. This is used to generate a PRBS payload for transport through the test network and also is at the point in the test network where the protection switch time is measured. Finally this module is used to run the J1 connectivity check. Note that both of these modules may be in a single XM chassis. And remember that in one hit you're testing all channels on all ports.

Within the DUT, in this case "D" we've indicated the mechanism used for switching, The switch operation is carried out by the cross connect and involves switching at the path level. Any path can be connected from any slot to any other slot via the cross connect.



When using an XM to test switching times and connectivity in a BLSR network, this is the likely set-up. Two ports or modules (depending on line rate) in through mode are used to inject errors and alarms or to manipulate K1/K2 overhead bytes in order to force protection switches to occur. A third module is connected to the NE of interest. This is used to generate a PRBS payload for transport through the test network and also is at the point in the test network where the protection switch time is measured. Finally this module is used to run the J1 connectivity check.

Within the DUT, in this case “D” we’ve indicated the mechanism used for switching, as we did a few slides previously. The switch operation is carried out by the cross connect and involves switching at the path level, even though this is a line switched architecture. Think of a line switch as a bulk path switch. Any path can be connected from any slot to any other slot via the cross connect – in a line switch a whole slot’s worth (or at least a whole port’s worth within the slot) may be re-connected in one go.

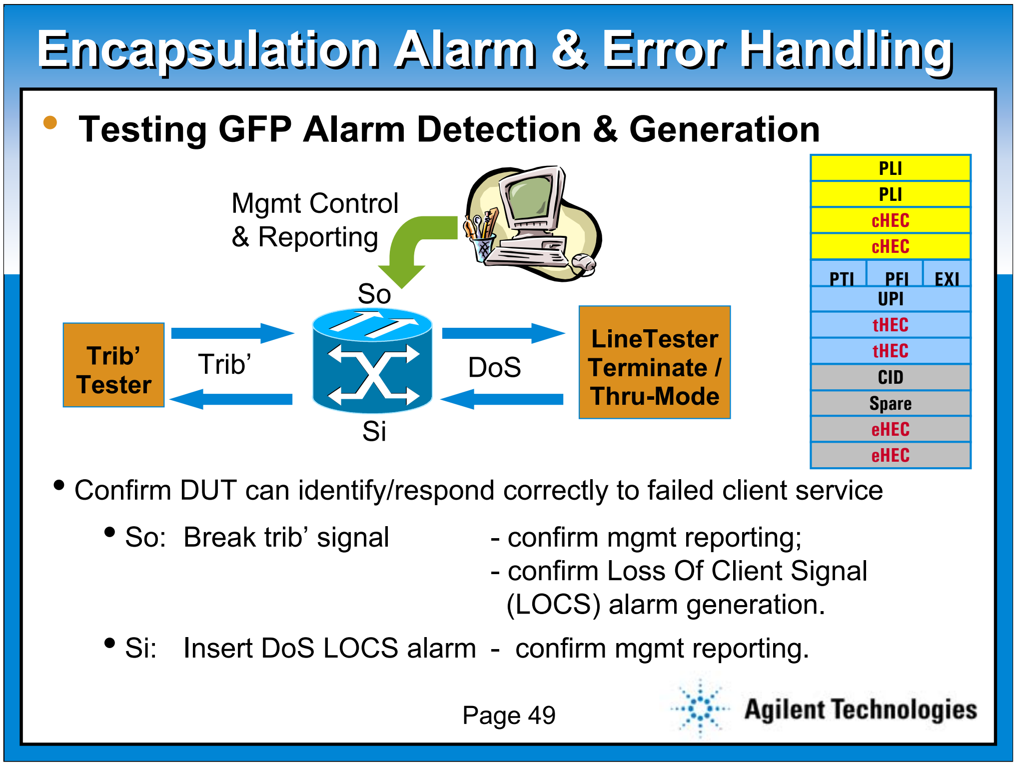


2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber

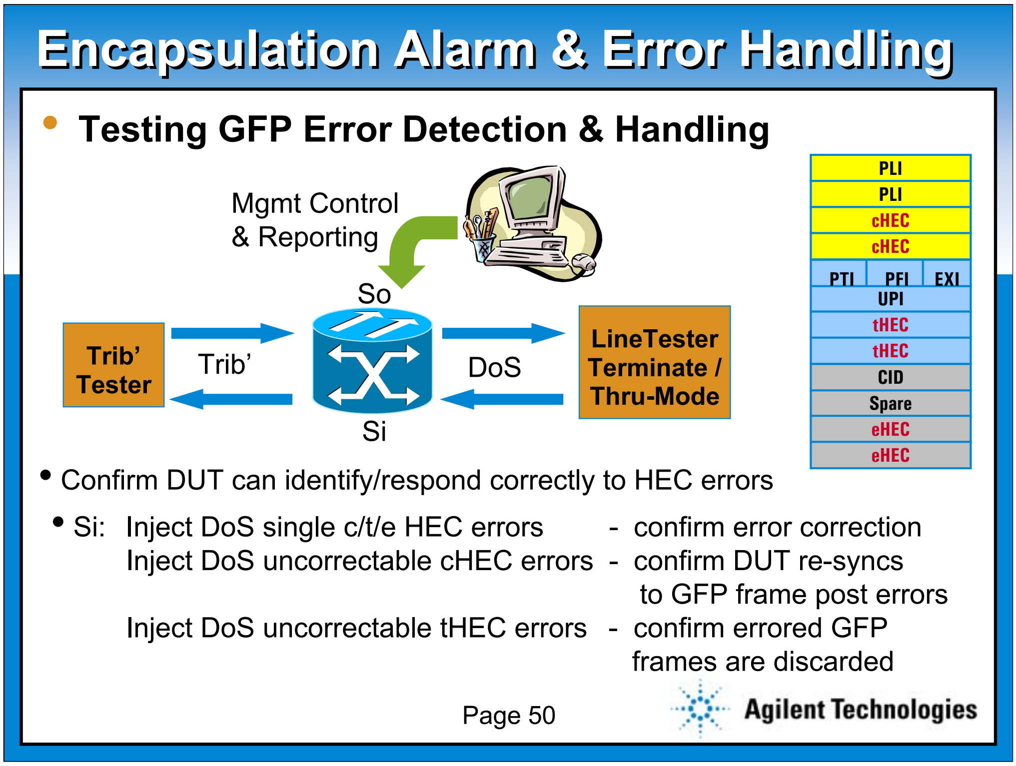


2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber

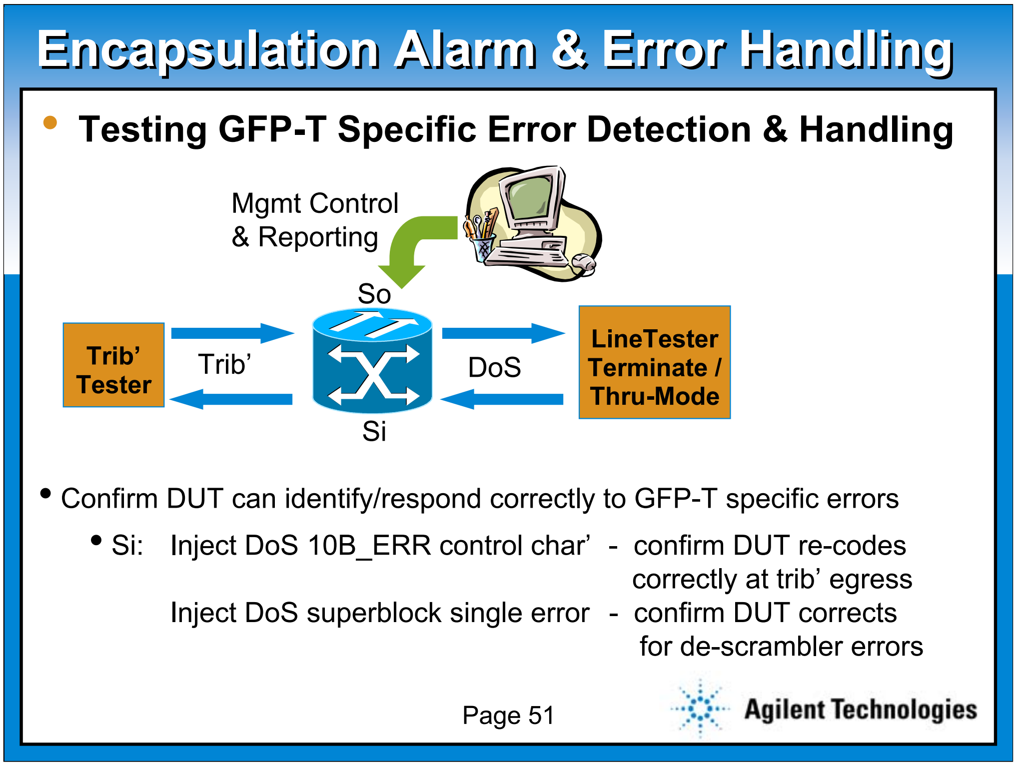


2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber

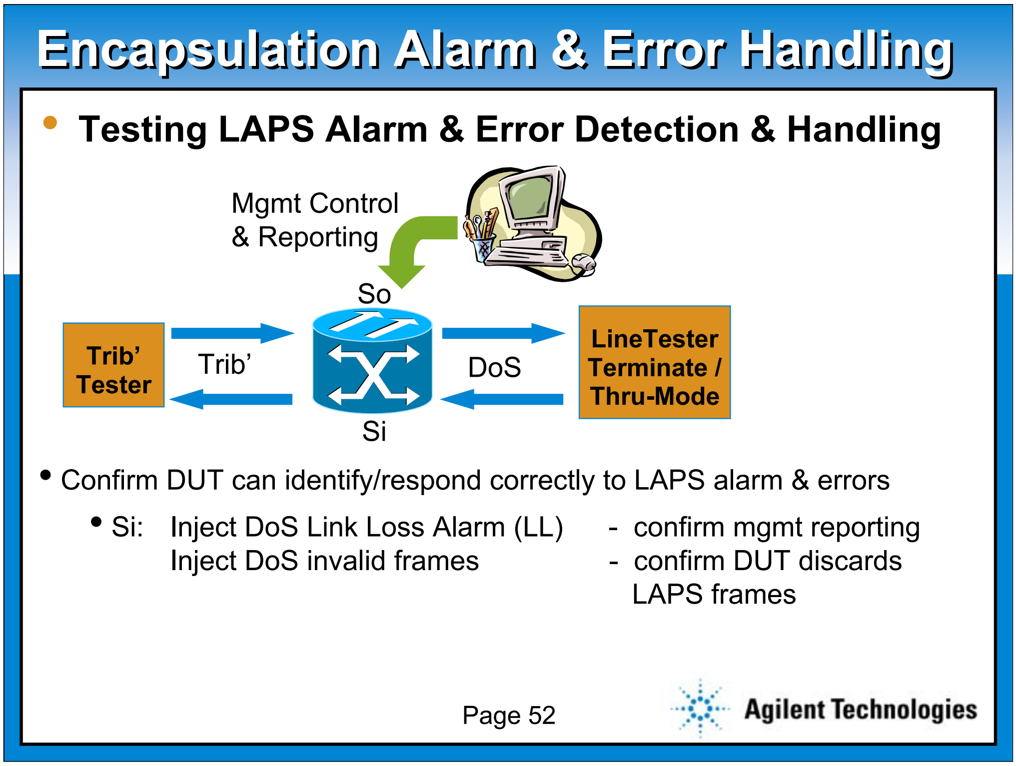


2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber



2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

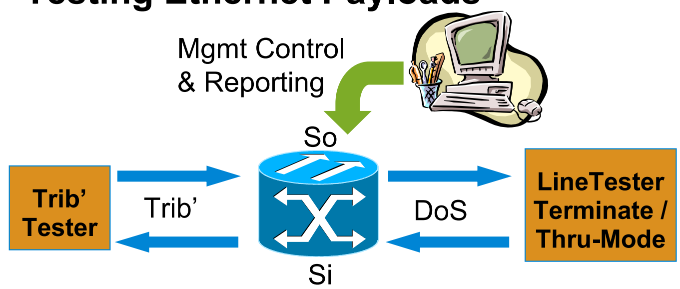
In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber

Payload Integrity Testing

- **Testing Ethernet Payloads**



- Confirm DUT can transmit Ethernet client service correctly
  - So: Insert trib' test cell - confirm correct transmit sequence.
    - confirm payload integrity via FCS.
    - stress DUT with Ethernet bandwidth.

    Insert trib' runt frames - confirm frames discarded.
    Insert trib' jumbo frames - confirm frames over limit discarded.
    Insert trib' VLAN tag - confirm correct routing.

2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

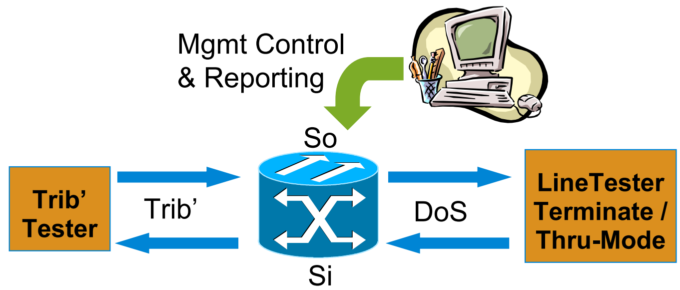
In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber

Concatenation Testing

- **Testing Virtual Concatenation**



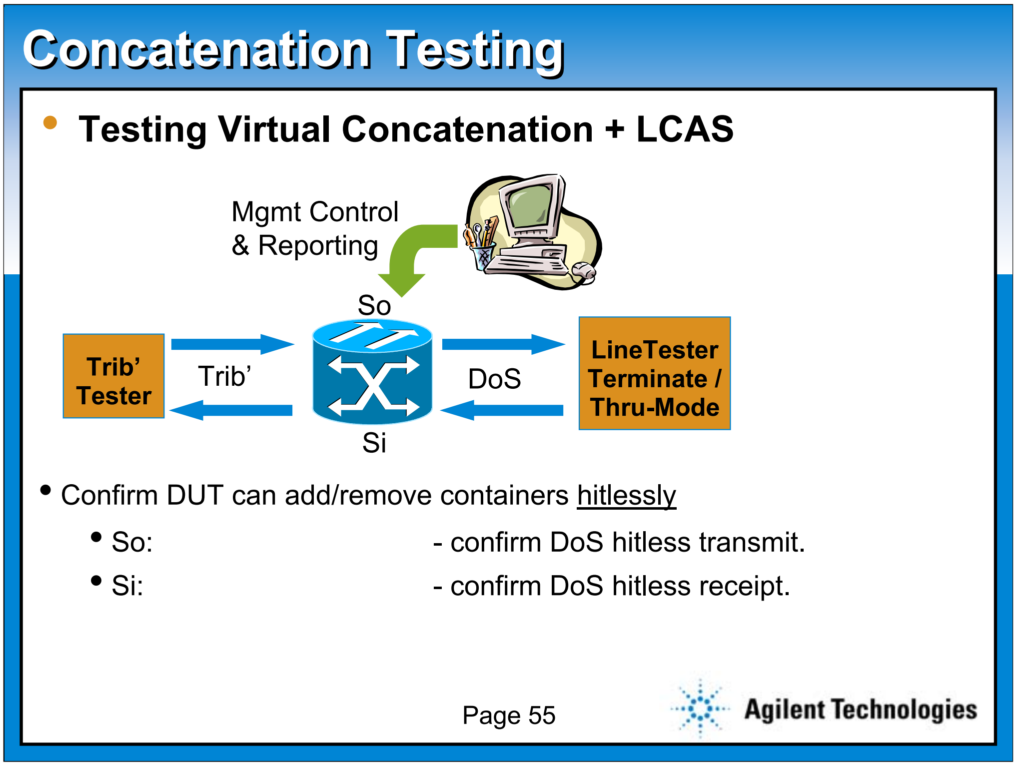
- Confirm DUT can transmit Ethernet client service correctly
  - So: - confirm zero delay on DoS output.
  - Si: Insert DoS differ' delay - check max delay tolerated by DUT
    Insert DoS OOM/LOM - confirm DUT detection & reporting
    Insert DoS sequence errors - confirm detection & mgmt reporting

2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber



2fBLSRs consist of 2 fibers each running in opposite directions . On each fiber, half the available bandwidth is reserved for protection

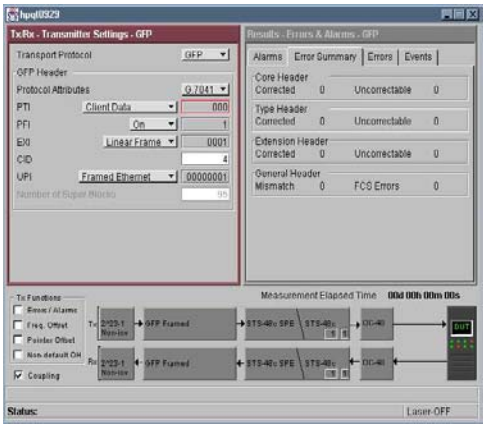
In OC-48, for example STS 1-24 are for working traffic and STS 25-48 for protection traffic. In reality, STS 25-48 may in fact be either utilised for additional unprotected traffic or set as unequipped.

Fibers run in opposite directions, each carrying traffic in STS 1-24

If break in one fiber occurs, traffic switches from STS 1-24 on the broken fibre to STS 25-48 on other fiber

Agilent OmniBER OTN J7232A

- **An Example DoS Line Side Analyzer**



- Simulate / analyze encapsulated Ethernet client signal payloads.
- Simulate / analyze GFP-F, GFP-T, LAPS and custom (eg. PoS, Cisco HDLC) encapsulation procedures.
- Simulate / analyze SONET/SDH virtual concatenation procedures, including differential delays.

Agilent Technologies

So to round up on switching. This is the procedure you'd follow to test protection switching on an MSP. This has been validated with a customer and seen in operation in there test lab. (although there existing equipment couldn't provide the final connectivity check).

SONET/SDH Jitter Measurements

Data over SONET/SDH Seminar 3, 19th February '03.

All you need to know about jitter measurements.

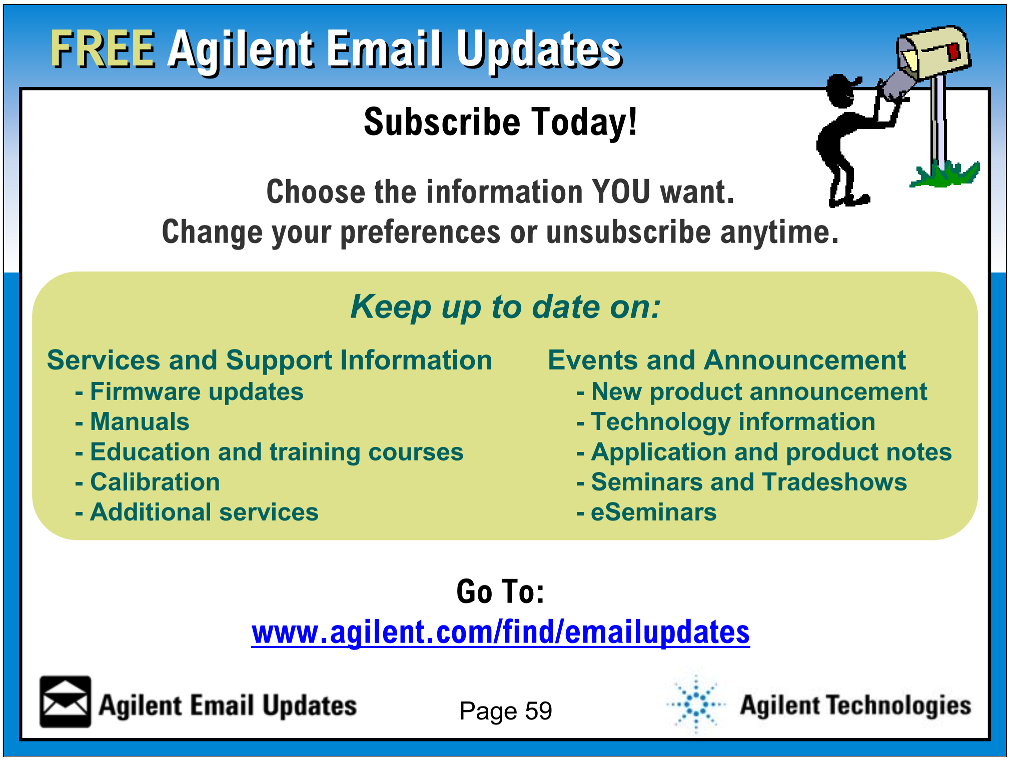
Jitter measurements and standards are equally as important to new DoS equipment and networks, as they were to legacy SONET/SDH. Despite many years of study and debate, much confusion still surrounds the topic of jitter measurements.

This seminar, focussed on jitter in its entirety, will address most of the key questions and issues associated with the topic, including tester versus operational equipment standards, intrinsic jitter measurement correction factors and much more.

Seminar 2: DoS Equipment

Seminar Content

- DoS technology structures recap
  - GFP, Virtual Concatenation & LCAS
- DoS equipment architectures & network topologies
  - MSPP & MSSP equipment
  - Linear, ring & mesh topologies
- DoS equipment test challenges
  - SONET/SDH error/alarm handling & protection switching
  - Payload handling including encapsulation & concatenation
- Wrap Up + question & answer session



In a moment we will begin with the Q&A but 1st, for those of you who have enjoyed today's broadcast, Agilent Technologies is offering a new service that allows you to receive customized Email Updates. Each month you'll receive information on:

•Upcoming events such as eSeminars, seminars and tradeshows

•the latest technologies and testing methods

•new products and services

•tips for using your Agilent products

•updated support information (including drivers and patches) for your Agilent products

It's easy to subscribe and you can change your preferences or unsubscribe at anytime. Once you've completed the NetSeminar feedback form you will be directed to Agilent's resource page located on slide # XX, at that point simply click on the Agilent Email Updates link and you will be directed to the subscription site.

Now on to the feedback form then to Q&A……..