LCAS and GFP for Service Protection in Next Generation SONET/SDH

ANDRES SIERRA, NIJAS KOLOTHODY and STAMATIOS V. KARTALOPOULOS
TCom Graduate Program
The University of Oklahoma
4502 East 41st Street. Tulsa, OK, 74135.
USA
http://tcom.ou.edu

Abstract: - Automatic protection switching (APS) is a mechanism adopted by SONET/SDH to automatically relocate traffic from a high priority path to a path assigned for protection. Although this method is created to respond to failures and reestablish the service in less than 50ms, it does not address issues related to low priority traffic, which in case of a failure is simply lost. The generic framing procedure (GFP) and the link capacity adjustment scheme (LCAS) are new procedures included in the next generation SONET/SDH which along with automatic protection switching (APS) provides service protection solutions to both high and low priority traffic. This paper provides an overview of these technologies and explains the implementation of GFP and LCAS for alternative service protection on the next generation SONET/SDH.

Key words: - Concatenation, LCAS, GFP, APS, protection, NG-SONET/ SDH.

1 Introduction

The synchronous optical network/synchronous digital hierarchy (SONET/SDH) was developed in the 1980's to efficiently transport synchronous traffic over fiber optics [1, 2]. However, data networks require longer payload envelopes that may exceed several thousand bytes. For this reason, concatenation was created in order to accommodate traffic from higher-level client signals, such as ATM and HDLC, over SONET/SDH in order to transport payloads that exceed the capacity of the standard synchronous payload envelope (SPE in SONET) or virtual container-3 (VC-3 in SDH). Nevertheless, contiguous concatenation leads to bandwidth inefficiency because the envelope capacity grows in a stepwise manner as specified by the SONET/SDH protocol. Furthermore, every network element has to be provisioned in order to support contiguous concatenation.

Virtual concatenation (VCAT) was introduced to overcome these problems as well as making the network more cost effective, increasing the granularity and diminishing the bandwidth inefficiency. But virtual concatenation does not work alone; it is supported by the generic framing procedure (GFP) and the link capacity adjustment scheme (LCAS) [3, 4]. The GFP is an encapsulation protocol to map higher-level client signals to a SONET/SDH payload. LCAS is a method to dynamically change the capacity of a virtual container. In addition to wide granularity range and being able to adjust their capacity, today's networks need to be reliable and available in order to provide QoS to end customers. These requirements are accomplished by increasing the network's resilience and adaptability to failures. LCAS and GFP play another important role in this area, the provision of service protection in SDH/SONET by building robust networks [5].

The remainder of this paper is organized as follows: Section 2 will discuss concatenation techniques. Section 3 is an overview of automatic protection switching. In the remaining sections, the LCAS and GFP methods will be reviewed and an explanation of how these two methods enhance the protection strategy of the Next generation SONET/SDH network (NG-S) is given. Conclusions based on this work are presented in Section 7.

Table 1. Virtual tributary data rates

Virtual tributary(VT)	VT bandwidth	T-carrier supported	T-carrier Bandwidth
VT1.5	1.728Mbps	DS-1	1.544Mbps
VT2	2.304Mbps	E1	2.048Mbps
VT3	3.456Mbps	DS-1C	3.152Mbps
VT6	6.912Mbps	DS-2	6.312Mbps

In order to avoid terminology confusion and extended explanations, in the remainder of the paper SONET terms are used to address both SONET and SDH.

2 Concatenation

SONET/SDH has become today's most important transport technology due to the satisfactory utilization of thefiber optic transport capacity. SONET/SDH was initially conceived to efficiently transmit T/E-carrier based traffic which was embedded in virtual tributaries inside the SPE as shown in Table 1 [6].

A VT1.5 is able to transport 24 DS-0 channels. However, user requirements might sometimes be better addressed through the use of a single channel operating at a full capacity of 1.5Mbps, which is known as T-1 un-channelized. Basically STS-N frames contain N STS-1's, which means that SONET is channelized as the T-carrier. Applying the rule an STS-3 is able to transport 3 STS-1's, but analogous to the T1 example the requirements of a SONET user could be better addressed if instead of having 3 STS-1's each at 51.84Mbps, the user had a single channel at 155.52Mbps. SONET permits the creation of unchannelized STS-3, as well as other speeds, through the process of contiguous concatenation [7]. This is used for the transport of payloads that do not fit in the standardized set of virtual tributaries. Contiguous concatenation has been part of SONET standards to accommodate traffic from higher-level client signals such as ATM. In this method, the three STS-1's that are concatenated into a STS-3 must be located in physically adjacent columns. The concatenation is indicated by placing special values to the H1/H2 pointers. However, contiguous concatenation can cause an extreme wastage of bandwidth since the SONET speeds do not line within native application data rates [8]. Examples of bandwidth inefficiency in contiguous concatenation are shown in Table 2. The effective payload of an STS-1 is 49.346Mbps, with the remainder being the overhead. Therefore, if a fast Ethernet signal is to be transmitted across a concatenated SONET link, three STS1's are needed and not two, resulting in wastage of 33% of the bandwidth. It is also possible that the user needs a service to transport Gigabit Ethernet across SONET and to do so an STS-48c would be required; this represents a waste of 58% of the bandwidth. In addition to the poor bandwidth granularity

Table 2. Efficiency comparison of contiguous and virtual concatenation for various payloads.

Service / data rate	Contiguous Concatenation		Virtual Concatenation	
	Data rate	ineffici ency	Data rate	Ineffici ency
Ethernet/ 10Mbit/s	STS-1c / 51.84Mbit/s	80%	VT1.5-7v / 11.2Mbit/s	11%
FastEtherne/ 100Mbit/s	STS-3c / 155.52Mbit/s	33%	STS-1-2v / 100.22Mbit/s	0%
ESCON/ 200Mbit/s	STS-12c / 622.08Mbit/s	58%	STS-1-4v / 200.44Mbit/s	0%
GbEthernet/ 1000Mbit/s	STS-48c / 2488.3Mbit/s	67%	STS-3c-7v / 1052.3Mbit/s	5%

requirement contiguous concatenation also requires concatenation functionality at each network element (NE). This requirement results in higher costs to build and provision the network.

Given that contiguous concatenation is determined by the rule N x STS-1, where N can be 1, 3, 12, 48, its granularity is limited to predetermined data rates. On the other hand virtual concatenation offers an alternative method to contiguous concatenation which permits the creation of payloads at lower incremental rates [7]. This means that virtual concatenation can grow in smaller steps as shown in Tables 2 and 3, which results in a higher bandwidth granularity. In Table 2 and 3, X is the number of contiguous frames. Since the virtual concatenated groups do not have to be physically associated, each member can be routed and transported across separate links and recombined at the end point, requiring concatenation functionality only at the path termination equipment (PTE).

Since channels are not restricted to the same paths between PTEs a differential delay between frames will occur. This differential delay is compensated using a multiframing and sequencing approach with

Table 3. Virtually concatenated SONET payloads

VTn-Xv	STS-	X-values	Capacity (Mbit/s)	Steps (Mbps)
VT1.5-Xv	STS-1	1-28	1.6-44.8	1.6
VT2-Xv	STS-1	1-21	2.176-45969	2.176
VT3-Xv	STS-1	1-14	3.328-46.696	3.328
VT6-Xv	STS-1	1-7	6.784-47.448	6.784
VT1.5-Xv	STS-3c	1-64	1.6-102.4	1.6
VT2-Xv	STS-3c	1-63	2.176-137.088	2.176
VT3-Xv	STS-3c	1-42	3.328-139.776	3.328
VT6-Xv	STS-3c	1-21	6.784-142.464	6.784

Table 4. Virtual concatenation features

Virtual concatenation features	
Enables closer alignment of native data rates.	Optimizes the utilization of the physically available resources.
Provides flexible incremental bandwidth allocations.	Does not require that intermediate NE manage this procedure.
Efficiently supports and accommodates any data service.	Makes easier the migration from TDM based traffic to packet oriented traffic.

which the individual frames are realigned at the receiving PTE. This realignment process has to cover a differential delay of at least 125 μsec.

There are two different types of virtual concatenation: high order (HO) and low order (LO). For HO virtual concatenation the variable X indicates the number of payloads that have been logically associated and can not exceed 256 (i,e, STS-1-Xv:virtual concatenation of X STS-1 payloads). If LO is employed, the n on VTn-Xv denotes the type of virtual tributary (VT=1.5,2,3,6) applied, while the X denotes the number of VTn's and it can not exceed 64 (i,e, VT1.5-2v: virtual concatenation of 2 VT1.5) [9]. This nomenclature can be appreciated in more detail in Table 3.

HO virtual concatenation requires the use of a sequence indicator (SQ) in the H4 multiframe overhead to identify the order in which the individual payloads are combined to form the contiguous container. The bit 2 of the K4 (Z7) tributary overhead byte must be used when employing LO virtual concatenation. Table 4 explains in greater detail the advantages of virtual concatenations.

3 Automatic Protection Switching

In view of the fact that most of the voice and data traffic is carried over SONET, the network has to fulfill demanding rules on service protection and provide very high level of service quality. In addition it must make the network available to users for the maximum possible time and must react expeditiously to link failures or degradation. There are three types of protection strategies: 1+1, 1:1 and 1:N. In the 1+1 two paths on different routes are used to transmit data, therefore if one path fails the receiver automatically switches to the alternate path. 1:1 is used to transport data on only one of the links and other link is used to transport low priority traffic. If a failure occurs in the path used for high priority traffic, the link is redirected to the standby link. The 1:N case operates in a similar fashion to the 1:1 case, except that it has one protection channel for N active channels [10].

In order to support these strategies, protection schemes are incorporated in SONET through messages sent on the K1/K2 bytes of the line overhead [11]. These two bytes communicate automatic protection switching (APS) commands and errors which are used only on the first STS frame of an STS-n signal. Bits 1 - 4 on K1 byte are the switch request bits and have sixteen possible values to indicate if the link is under normal operation or if it has been locked-out for protection. Commands can automatically indicate if there has been a loss of frame or a loss of signal or even if the signal has been degraded. The final four bits of K1 and the first four bits of K2 are the destination ring node identifier and the source ring node identifier respectively. The fifth bit of K2 is the long/short path bit which indicates if a message is sent over the long or short path on a four fiber bidirectional line-switched ring. Bits 6 – 8 are status messages which indicate normal operation or if extra traffic exist on the protection channel among other four more defined stages.

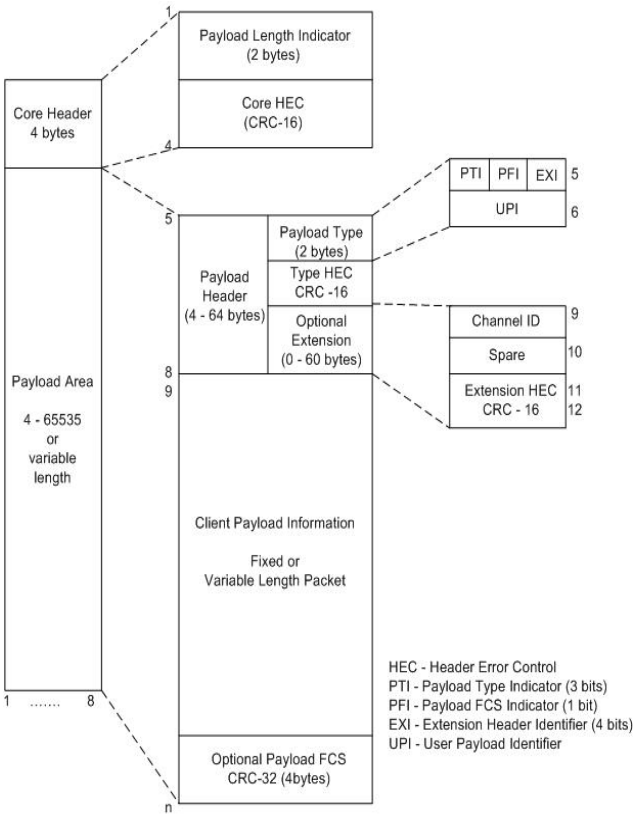


Fig. 1. GFP Frame

4 Generic Framing Procedure

GFP presents a procedure to map variable frame sizes of asynchronous and bursty traffic from higher level clients like ESCON, FICON, Fiber channel and Gigabit Ethernet onto a general purpose frame which is then mapped into the SONET synchronous payload envelopes (SPE). This results in the flexibility to efficiently transport these protocols over the existing SONET infrastructures [3]. GFP creates a simple multiplexing method by which the data originating from the different clients can be easily multiplexed and sent over the same link in a ring or point-to-point topology. Moreover, since GFP supports mapping and transport of variable length user payloads, it does not require process intensive segmentation and reassembly (SAR) which in turn simplifies its hardware and offers higher throughput efficiency appropriate for high-speed data transmission.

GFP has a flexible frame structure optimized for the detection and correction of errors. GFP frame structure is illustrated in Figure 1. The core header is intended to support non-client specific data link management functions like GFP frame delineation. The core header defines the size of the GFP frame in octets using a two-byte field and an error checking code over this payload length indicator. The CRC-16 provides robustness by correcting single-bit errors in the core header, which ensures reliable transmission of GFP without losing customer data. The payload area is of variable length from 4 to 65,535 bytes and is used to carry client data. It can be seen, Figure1, that the payload area consists of the payload header, the payload information field and an optional payload frame check sequence. The payload header in general is used to define the type of information transported, either user data frames or client management frames and also the content of the payload. The payload type identifier (PTI) distinguishes between the client management frames and the user data frames. The FCS is used to detect the errors in the payload field. The payload FCS indicator specifies the presence of the optional FCS field. The extension header identifier (EHI) indicates the type of network in the GFP frame which can be either null, ring or linear. The user payload identifier (UPI) defines the type of payload and encapsulation contained in the data frame such as frame mapped Ethernet, frame mapped FICON. UPI can also indicate management signals such as the loss of client signal or the loss of character synchronization. The client payload information describes the exact customer data service traffic.

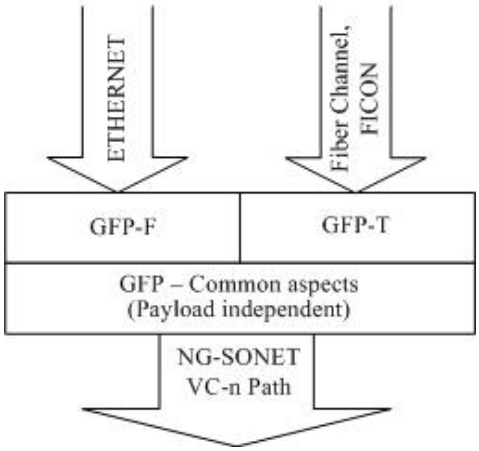


Fig. 2. Data over GFP over NG-S

4.1 Optimization of the GFP Model

In order to accommodate higher level client signals to the SONET payload, GFP supports two modes of signal adaptation, the frame mapped GFP (GFP-F) is relevant to most packet switching environments, and the transparent GFP (GFP-T) for transporting block coded delay sensitive signals.

The two GFP modes, GFP-F and GFP-T, are supported by a payload independent common GFP part known as GFP-client specific aspects. Figure 2 shows the mapping of different payload types into the STS-n of the next generation SONET/SDH protocol.

4.2 Frame Mapped GFP

Frame mapped GFP (GFP-F) is optimized for packet switching and mapping variable length applications such as IP, Ethernet, Fast Ethernet and multi-protocol label switching (MPLS) traffic. The client signals or packets are mapped frame by frame into the client payload information field. Payload data units (PDU) from different clients can be packet level multiplexed onto the same time division multiplexed (TDM) channel prior to transmission through the SONET infrastructure. GFP-F has advantages of simplicity and use least amount of overhead which guarantees the best bandwidth efficiency. However, GFP-F requires buffering and MAC hardware. In summary, the GFP features are:

- Frames are variable
- It supports rate adaptation and multiplexing at packet level
- It aggregates frames at the STS and VT levels

- It supports most packet data types
- It requires buffering
- It requires MAC awareness
- It introduces latency
- It supports client data frames (CDF) for both client data and management
- It supports control frames for idle and OA&M

4.3 Transparent Mapped GFP

Transparent mapped GFP (GFP-T) is used for mapping frames of fixed length which are strict delay sensitive, and have strict loss and throughput requirements. GFP-T defines the mapping of 8B/10B block coded signals which have applications in storage area networks (SAN), in which the data along with the control information are transmitted to the sink. The 8B/10B code converts the 2^8 values to 2^{10} data values using a method that balances the number of ones and zeroes. Twelve of these codes are used for sending control information from the transmitter to the receiver.

In GFP-T, the 8B/10B codes are decoded and mapped onto the 8 payload bytes of a 64B/65B code. The fixed numbers of these characters are mapped byte by byte into a frame of static length. This octet mapping reduces the latency incurred due to buffering compared to GFP-F where the entire client data frame has to be buffered. The lower buffering latency makes GFP-T suitable for applications requiring a controlled transfer delay. Moreover, the GFP-T framing method is more bandwidth efficient than 8B/10B coding. An example of encapsulation using GFP is shown in Figure 3. In summary, the GFP-T features are:

- Fixed frame length
- N to 1 mapping of client packets
- It requires no buffering
- No latency is introduced
- No MAC is required, only 8B/10B coding

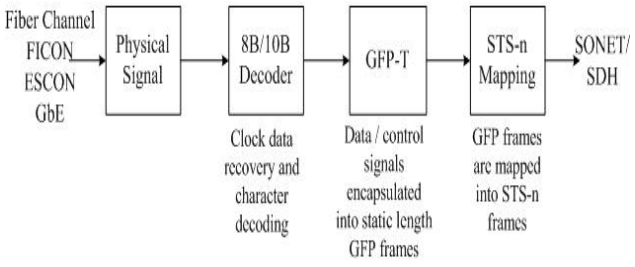


Fig. 3 GFP-T framing procedure

Table 5. VC and LCAS control packet

MultiFrame Indicator (MFI)	Mechanism to determine the differential delay between the source and the receiver and helps in realignment between members of the VCG
Sequence Indicator (SQ)	Unique number assigned to members within the same VCG
LCAS Control Commands (CTRL) *Fixed* LCAS not supported *Add* Request to add a member to the group *Norm* Normal transmission – This STS-1 in use *EOS* End of sequence and last STS-1 of this channel *Idle* Member is not part of this channel *DNU* Do not use – Broken Link reported	
Group Identifier (GID)	Informs the receiver which VCG a member belongs to
Re-Sequence Acknowledge (RS-Ack)	Informs the source that the receiver has received the initiated changes
Member Status Field (MST)	Status report of all the members of the VCG from the receiver to the source
CRC field	Error correction for the control packet. CRC-3 for LOVC and CRC-8 for HOVC

- The PHY layer is terminated
- Because there is no buffering, it retains no idle frames.

5 Link Capacity Adjustment Scheme

Even though granularity can be very flexible using virtual concatenation, it can be enhanced through the use of LCAS. LCAS specifies a methodology to dynamically increase or decrease the capacity of a container that is transported over SONET [4]. LCAS is a two-way handshake protocol between the end network elements that are connected at the customer side to the SONET infrastructure. It provides channels with the flexibility to dynamically adjust the capacity of the virtual concatenated group (VCG) without affecting the integrity of the SONET network. This means that the size of the data channel allotted to a customer can be changed at any time without losing the data transported on other channels in the network. This capacity adjustment is a one-way process, which means that the upstream link capacity can be different

to the downstream link capacity. This protocol gives service providers the flexibility to offer bandwidth-on-demand services. In legacy SONET networks this type of provisioning is a quite laborious and expensive procedure and takes days to be complete. LCAS mechanism also checks the links for connectivity and automatically removes and recovers the failed paths, without affecting the network performance.

LCAS overhead is encoded in the H4 byte of the path overhead of the SPE for the high order virtual concatenation (HOVC) and of the K4 byte for the low-order virtual concatenation (LOVC). This protocol uses 32 HOVC multiframes and 8 LOVC multiframes to transport the status of all members. A member is defined as a single container that pertains to a virtual concatenated group (VCG). Some of the bytes of this H4/K4 multiframe are used by virtual concatenation for sending the multiframe indicator and sequence indicator (SQ) messages. The remainder of the H4/K4 bytes is used by LCAS protocol for sending control messages.

The LCAS protocol uses one of the six command control messages, as shown in Table 5, in each STS-1 to adjust the bandwidth. The state of the link is explained by the control message which was transmitted prior to the control message. The parameters used in virtual concatenation and LCAS control signaling are explained in Table 5.

The following steps illustrate the procedure for upsizing a link using LCAS protocol:

1. The network management system at the source locates a new path between the source and the receiver.
2. The source sends an ADD control command to add this link to the channel. The receiver then responds with MST values of either OK or FAIL.
3. Upon receipt of an OK signal, the source assigns this member an SQ number which will be one greater than the number currently used.
4. The control command for the last member of the VCG, which is already in use, is sent to EOS indicating the end of the sequence. This member has the highest SQ number.
5. Upon adding a member the status of the previous member is changed from EOS to NORM and the status of the lately added member is changed to EOS.

Figure 4 shows an example of the state of a network in which a request has been sent by the source to increase the capacity. Figure 5 illustrates the state after adding a new member to the network. In this case the sink responds back to the source by sending a RS-Ack signal after the changes have been initiated.

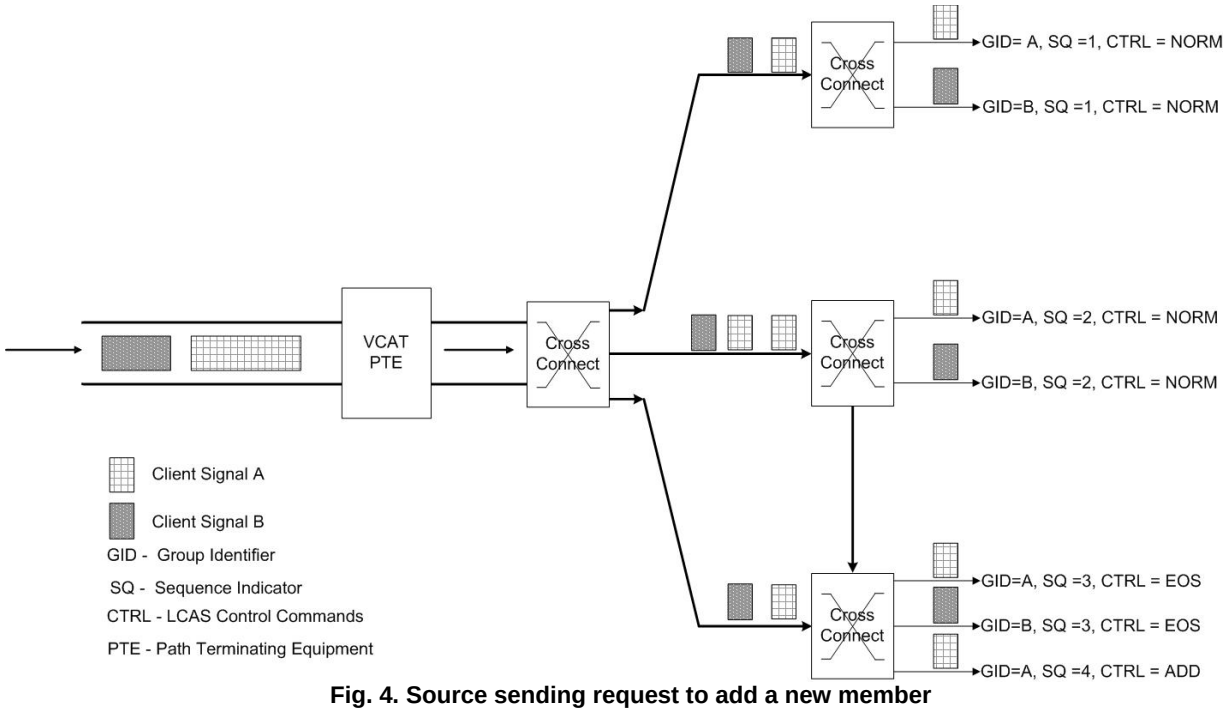


Fig. 4. Source sending request to add a new member

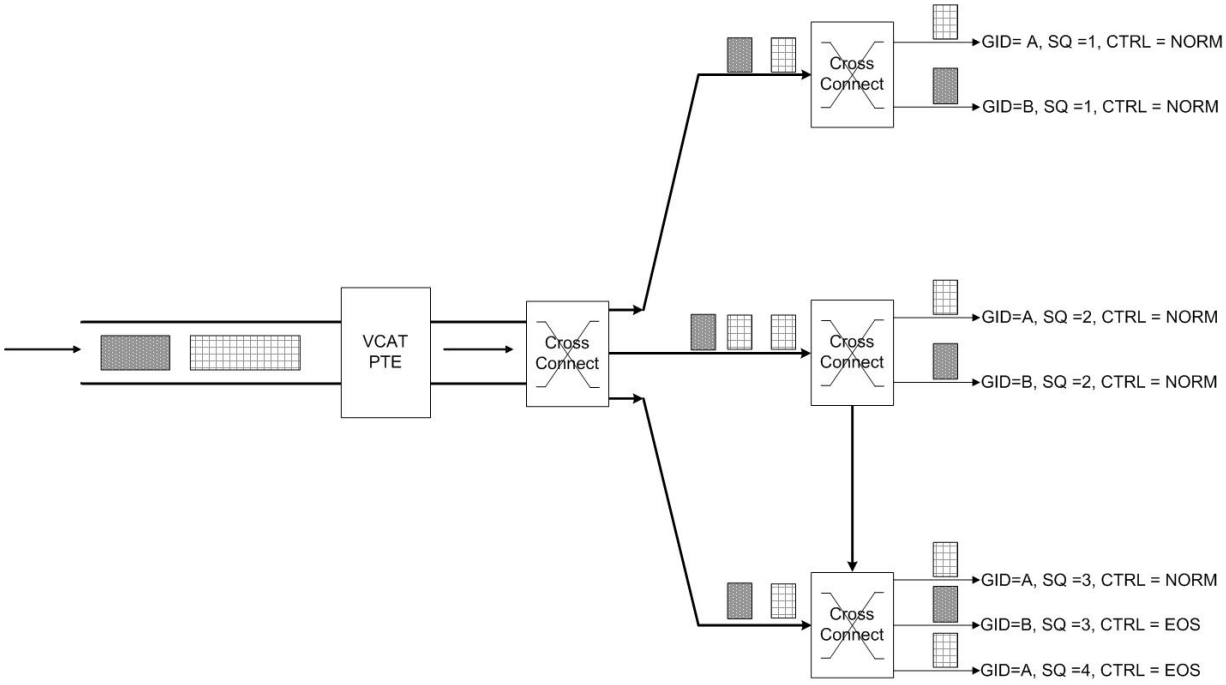


Fig. 5. Member added to the group

LCAS protocol helps in providing QoS, load balancing and fault recovery mechanism for the network. This is discussed in more detail in Section 6.

6 Service Protection

Automatic protection switching (APS) is a key service restoration functionality built into the SONET and SDH standards to protect against failures. In addition to this feature encoded in the overhead of a SONET frame, next generation SONET has increased its robustness and protection for packet networks using GFP and LCAS. According to SONET/SDH when a tributary fails then the edge node detects the failed signal, it declares loss of signal (LOS) and it generates an indication (AIS-L, AIS-P), which is then transmitted to all affected virtual containers (VC). The nodes that receive the AIS respond with a received defect indication (RDI-L for line or RDI-P for path). Similarly, the performance of a tributary is monitored by the BIP-8 byte in the overhead and recorded in the error control byte B3 (or B1, B2) when the performance degrades below an acceptable threshold, a received error indication (REI-L, REI-P) is sent. In this section the advanced service protection features achieved in the next generation SONET through implementation of GFP and LCAS is explained.

Section 4 explained that there are two types of GFP client frames in the PTI:

1. Client data frame, which is used to indicate that the frame payload area is transporting client signals as Ethernet, FICON, or Gigabit Ethernet.
2. Client management frame, which is used to indicate failures on the incoming client signal.

As previously explained, GFP supports client signal failure notifications, providing a method for a source process to transmit a client signal fail (CSF) indication to the sink process, upon detection of a failure in the incoming client signal. When a failure is detected, the GFP source adaptation process creates a client management frame which is transmitted immediately after the current frame. This client management frames has the PTI set to 100, the PFI to 0, a suitable EXI and the UPI can have either of the following values:

1. 0000 0001 indicates loss of client signal.
2. 0000 0010 indicates loss of client character synchronization.

If a CSF occurs in the middle of a GFP client data frame, the remainder of the frame is filled with 10B_Err codes, which is a special code used to convey client signal defects. In order to prevent excessive flooding a client management frame indicating is sent once every 100ms≤T≤1000ms.

When the GFP client sink receives a CSF message, it declares a client signal failure and the transmitter at the client output may be turned off for protection. The defect condition at the receiver should be cleared after receiving a valid client data frame or after failing to receive N CSF indications in N x 1000ms, where 3 is a suggested value for N.

LCAS permits the dynamic addition or removal of members of a VCG. It responds rapidly to failures of any member and rapidly adapts to specific bandwidth requirements that any user may request. A virtual concatenated channel combines numerous paths to form larger virtual channels, allowing each member of the VCG to take a different route. The members of a VCG are then reordered at the sink node, and the data stream that was initially broken up is recombined. In the event of a failure of any of the VCG members, the sink nodes send a message to the source node indicating which of the members has failed. The source node then stops using the non-working member and continues to employ only operational members and finally restores the service at a lower bandwidth. This failure and recovery process is depicted in Figure 6 and Figure 7. In the normal operating state, the service offered between end nodes corresponds to an STS-6v and the six SQs represent each of the six members in the concatenated group. The preferential routes will be those with least number of hops. However, multiple undependable routes can be used in order to enhance the bandwidth efficiency, as is the case of SQ 5 that may take an alternative route if there is a bandwidth restriction on the original path. A failure that occurs in a link that is common to all the members of the VCG is shown in Figure 7. When a failure occurs, one of two approaches may occur. In the first approach, the VCG will eliminate the members that transverse the failed path and continue operation at a lower data rate using healthy members until the failed link is recovered. The second scheme uses the available bandwidth to transport all the members without disrupting the traffic flow and thus avoids the failed path. In this case when the fault is cleared the sink sends an MST = OK signal to the source. The source then re-aligns the members to create a balanced traffic flow through the available paths. Both of these methods are possible using the LCAS protocol.

LCAS has the advantage of allowing the use of unprotected paths which reduces the bandwidth of a VCG in case of failure instead of experiencing a connection loss or having to pay for full protection. Therefore, LCAS presents a procedure that allows a signal to be transported at a lower bit rate rather than allowing a breakdown to occur due to the failure of unprotected link. It should be noted that prior to LCAS low priority traffic was not included service protection strategies and for higher priority traffic SONET used n+1 or 1:1 strategies which results in a

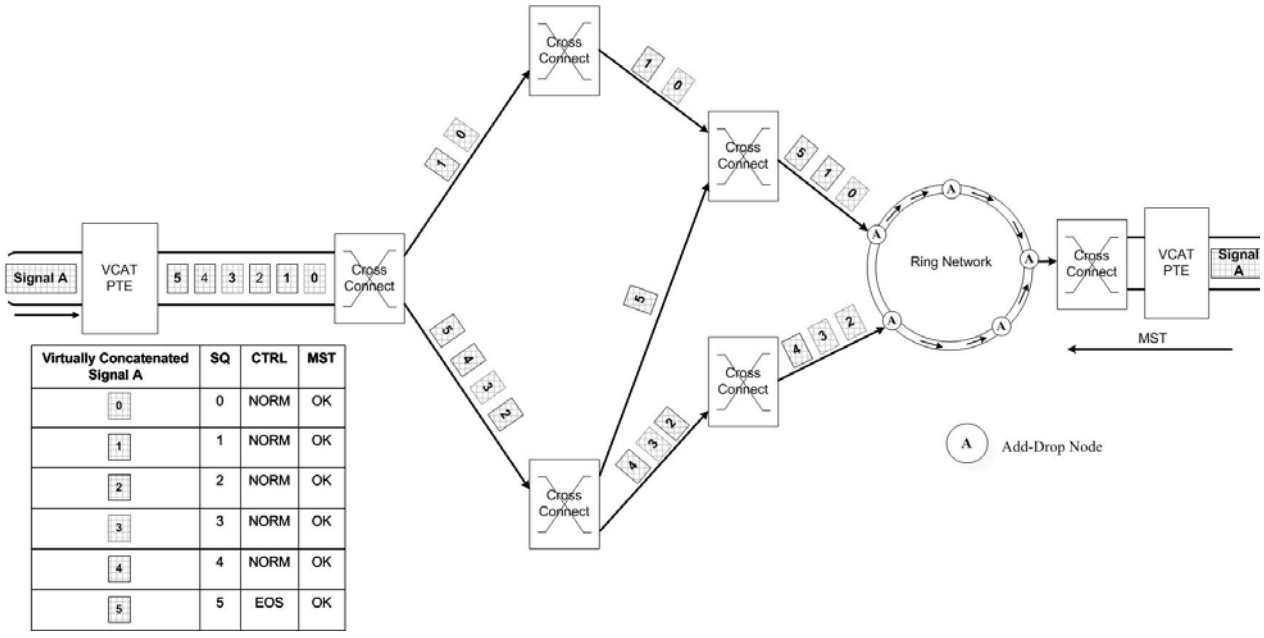
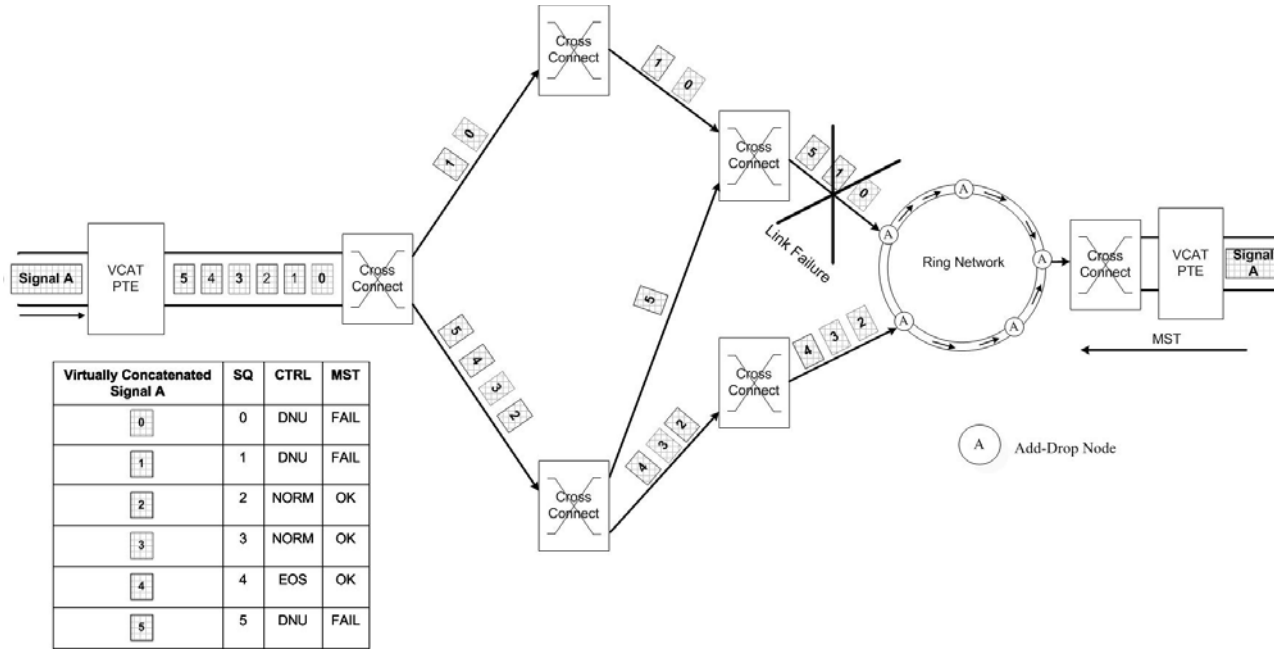


Fig. 6. An example of diverse routing performed with the help of LCAS protocol



Virtually Concatenated Signal A	SQ	CTRL	MST
0	0	DNU	FAIL
1	1	DNU	FAIL
2	2	NORM	OK
3	3	NORM	OK
4	4	EOS	OK
5	5	DNU	FAIL

Fig. 7. Network response to single link failures using LCAS protocol

higher cost per bandwidth. Following the advent of LCAS different levels of protection were available and in the event of a failure of an unprotected member, a signal with lower bit rate is still transmitted instead of experiencing an outage.

7 Conclusion

GFP and LCAS present an alternative method to the conventional service protection offered by APS. The implementation of GFP and LCAS on SONET/SDH networks, allows for the efficient utilization of unused bandwidth which was reserved for protection in bidirectional line switched rings (BLSR) and unidirectional path switched rings (UPSR). With the assistance of GFP and LCAS, data from a single client can be split and dynamically allocated on different routes to balance the traffic transported on the network. In the event of a failure in one of the routes, this feature in next generation SONET/SDH permits data to be transmitted over healthy paths at a lower bandwidth. This avoids the complete outage of unprotected client signals, which was an issue in legacy SONET/SDH where traffic from a single client was transmitted contiguously on a single route. Moreover, the next generation SONET/SDH over wavelength division multiplexing (WDM) technology is defined with the inclusion of the generalized MPLS (GMPLS). In this case, service protection is also achieved.

We conclude that GFP and LCAS enhance the service protection capabilities of SONET/SDH making it a more resilient and cost-effective architecture.

References

[1] ANSI T1.105, Synchronous Optical Network (SONET) – Basic Description Including Multiplex Structures, Rates and Formats, 2001.

[2] ITU-T Rec G.803, Architecture of Transport Networks Based on the Synchronous Digital Hierarchy (SDH), 1997.

[3] ITU-T Rec G.7041/Y.1303, Generic Framing Procedure (GFP), Dec. 2003.

[4] ITU-T Rec G.7042/Y.1305, Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated Signals, Feb. 2004.

[5] S.V. Kartalopoulos, *Next generation SONET/SDH: Voice and Data*, IEEE Press, 2004.

[6] W. Goralski, *SONET/SDH*, 3rd ed , McGraw-Hill, 2002.

[7] ITU-T Rec G.707/Y.1322, Network Node Interface for the Synchronous Digital Hierarchy, Dec. 2003.

[8] S.V. Kartalopoulos, *Understanding SONET/SDH and ATM: Communications Networks for the Next Millenium*, IEEE Press, 1999.
[9] L. Choy, Virtual Concatenation Tutorial: enhancing SONET/SDH Networks for Data Transport, *J. Opt. Netw*. Vol. 1, pp. 18-29., Dec. 2001.
[10] S.V. Kartalopoulos, *DWDM: Networks, Devices and Technology*. IEEE Press/ Wiley 2003.
[11] ITU-T Rec G.841, Types and Characteristics of SDH Network Protection Architectures, Oct. 1998.