



SUNRISE TELECOM

... a step ahead



Application Series

Measuring APS in a SONET/SDH Network

302 Enzo Drive
San Jose CA 95138 USA
ph 1 408 363 8000
fax 1 408 363 8313
info@sunrisetelecom.com
www.sunrisetelecom.com

Publication Number APP-OPT-004 Rev. A

INTRODUCTION

Automatic Protection Switching (APS) is one of the most valuable features of SONET and SDH networks. Networks with APS quickly react to failures, minimizing lost traffic, which minimizes lost revenue to service providers. The network is said to be "self healing." This application note covers how to use Sunrise Telecom SONET and SDH analyzers to measure the amount of time it takes for a network to complete an automatic protection switchover. This is important since ANSI T1.105.1 and ITU-T G.841 require that a protection switchover occur within 50 ms. To understand the APS measurement, a brief review is first given. This is followed by an explanation of the basis behind the APS measurement. The final section covers how to operate your Sunrise Telecom SONET and SDH equipment to make an APS time measurement.

WHAT IS APS?

Automatic protection switching keeps the network working even if a network element or link fails. The Network Elements (NEs) in a SONET/SDH network constantly monitor the health of the network. When a failure is detected by one or more network elements, the network proceeds through a coordinated predefined sequence of steps to transfer (or switchover) live traffic to the backup facility (also called "protection" facility). This is done very quickly to minimize lost traffic. Traffic remains on the protection facility until the primary facility (working facility) fault is cleared, at which time the traffic may revert to the working facility.

In a SONET or SDH network, the transmission is protected on optical sections from the Headend (the point at which the Line/Multiplexer Section Overhead is inserted) to the Tailend (the point where the Line/Multiplexer Section Overhead is terminated).

The K1 and K2 Line/Multiplexer Section Overhead bytes carry an Automatic Protection Switching protocol used to coordinate protection switching between the headend and the tailend.

The protocol for the APS channel is summarized in Figure 1. The 16 bits within the APS channel contain information on the APS configuration, detection of network failure, APS commands, and revert commands. When a network failure is detected, the Line/Multiplexer Section Terminating Equipment communicates and coordinates the protection switchover by changing certain bits within the K1 & K2 bytes.

During the protection switchover, the network elements signal an APS by sending AIS throughout the network. AIS is also present at the ADM drop points. The AIS condition may come and go as the network elements progress

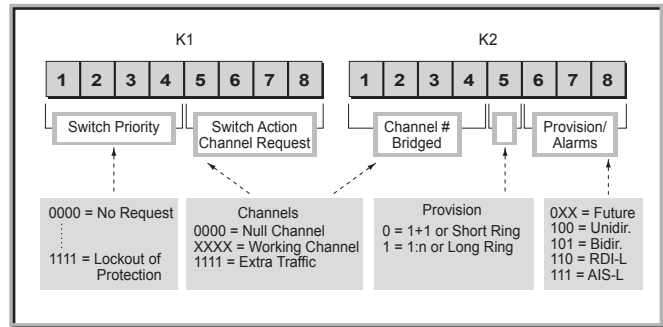


Figure 1 APS channel K1 and K2 bytes

through their algorithm to switch traffic to the protection circuit.

AIS signals an APS event. But what causes the network to initiate an automatic protection switchover? The three most common are:

- Detection of AIS (AIS is used to both initiate and signal an APS event)
- Detection of excessive B2 errors
- Initiation through a network management terminal

According to GR-253 and G.841, a network element is required to detect AIS and initiate an APS within 10 ms. B2 errors should be detected according to a defined algorithm, and more than 10 ms is allowed. This means that the entire time for both failure detection and traffic restoration may be 60 ms or more (10 ms or more detect time plus 50 ms switch time).

PROTECTION ARCHITECTURES

There are two types of protection for networks with APS:

- Linear Protection, based on ANSI T1.105.1 and ITU-T G.783 for point-to-point (end-to-end) connections.
- Ring Protection, based on ANSI T1.105.1 and ITU-T G.841 for ring structures (ring structures can also be found with two types of protection mechanisms - Unidirectional and Bidirectional rings).

Refer to Figures 2-4 for APS architectures and unidirectional vs. bidirectional rings.

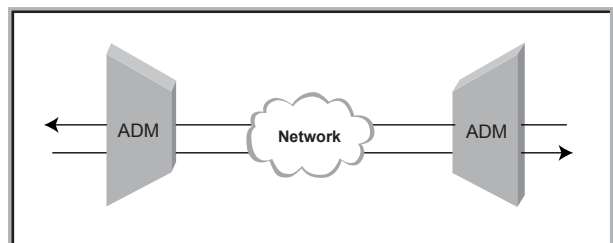


Figure 2 Linear Protection

PROTECTION SWITCHING SCHEMES

The two most common schemes are 1+1 protection switching and 1:n protection switching. In both structures, the K1 byte contains both the switching preemption priorities (in bits 1 to 4), and the channel number of the channel requesting action (in bits 5 to 8). The K2 byte contains the channel number of the channel that is bridged onto protection (in bits 1 to 4), and the mode type (in bit 5); bits 6 to 8 contain various conditions such as AIS-L, RDI-L, indication of unidirectional or bidirectional switching.

1+1

In 1+1 protection switching, there is a protection facility (backup line) for each working facility. At the headend, the optical signal is bridged permanently (split into two signals) and sent over both the working and the protection facilities simultaneously, producing a working signal and a protection signal that are identical. At the tailend, both signals are monitored independently for failures. The receiving equipment selects either the working or the protection signal. This selection is based on the switch initiation criteria which are either a signal fail (hard failure such as the loss of frame (LOF) within an optical signal), or a signal degrade (soft failure caused by a bit error ratio exceeding some predefined value). Refer to Figure 5.

Normally, 1+1 protection switching is unidirectional, although if the line terminating equipment at both ends supports bidirectional switching, the unidirectional default can be overridden. Switching can be either revertive (the flow reverts to the working facility as soon as the failure has been corrected) or nonrevertive (the protection facility is treated as the working facility)

In 1+1 protection architecture, all communications from the headend to the tailend are carried out over the APS channel via the K1 and K2 bytes. In 1+1 bidirectional switching, the K2 byte signaling indicates to the headend that a facility has been switched so that it can start to receive on the now active facility.

1:n

In 1:n protection switching, there is one protection facility for several working facilities (the range is from 1 to 14) and all communications from the headend to the tailend are carried out over the APS channel via the K1 and K2 bytes. All switching is revertive, that is, the traffic reverts back to the working facility as soon as the failure has been corrected. Refer to Figure 6.

Optical signals are normally sent only over the working facilities, with the protection facility being kept free until a working facility fails. Let us look at a failure in a bidirectional architecture. Suppose the tailend detects a failure on working facility 2. The tailend sends a message

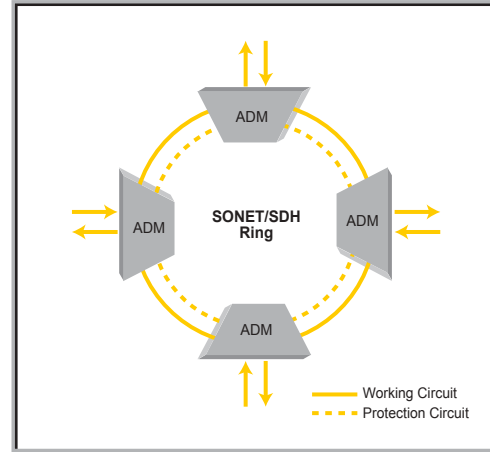


Figure 3 Ring Protection

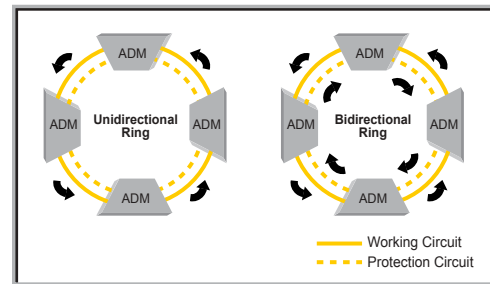


Figure 4 Unidirectional vs. Bidirectional Ring

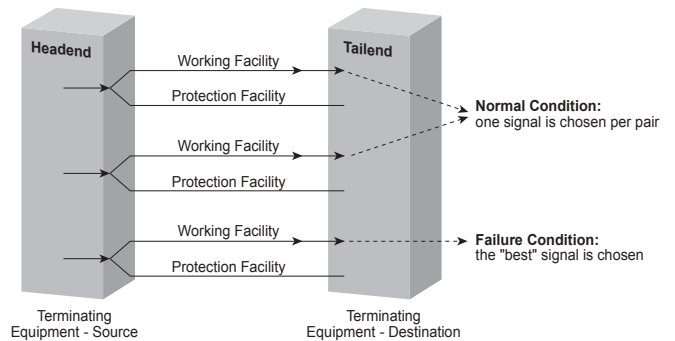


Figure 5 1+1 APS Architecture

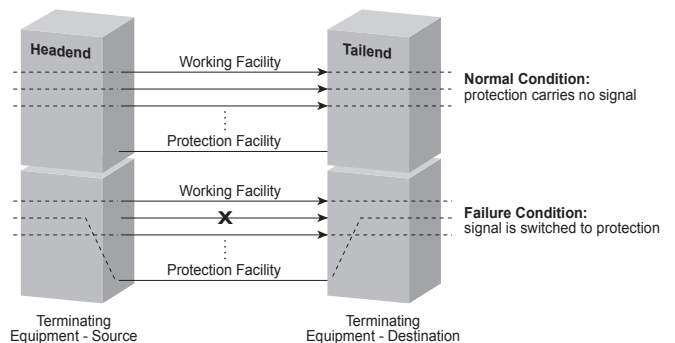


Figure 6 1:n APS Architecture

in bits 5-8 of the K1 byte to the headend over the protection facility requesting switch action. The headend can then act directly, or if there is more than one problem, the headend decides which is top priority. On a decision to act on the problem on working facility 2, the headend carries out the following steps:

1. Bridges working facility 2 at the headend to the protection facility
2. Returns a message on the K2 byte indicating the channel number of the traffic on the protection channel to the tailend
3. Sends a Reverse Request to the tailend via the K1 byte to initiate bidirectional switch

On receipt of this message, the tailend carries out the following steps:

1. Switches to the protection facility to receive
2. Bridges working facility 2 to the protection facility to transmit back

Now transmission is carried out over the new working facility.

Switch Action Comments

In unidirectional architecture, the tailend makes the decision on priorities. In bidirectional architecture, the headend makes the decision on priorities. If there is more than one failure at a time, a priority hierarchy determines which working facility will be backed up by the protection facility. The priorities that are indicated in bits 1-4 of the K1 byte are as follows:

1. Lockout
2. Forced switch (to protection channel regardless of its state) for span or ring; applies only to 1:n switching
3. Signal fails (high then low priority) for span or ring
4. Signal degrades (high then low priority) for span or ring; applies only to 1:n switching
5. Manual switch (to an unoccupied fault-free protection channel) for span or ring; applies only to 1+1 LTE
6. Wait-to-restore
7. Exerciser for span or ring (may not apply to some linear APS systems)
8. Reverse request (only for bidirectional)
9. Do not revert (only 1+1 LTE provisioned for nonrevertive switching transmits Do Not Revert)
10. No request

Depending on the protection architecture, K1 and K2 bytes can be decoded as shown in Tables 1-5.

Linear Protection (ITU-T G.783)

Bits 1234	Condition (state or external request)	Order
1111	Lockout of protection	Highest Lowest
1110	Forced switch	
1101	Signal fail high priority	
1100	Signal fail low priority	
1011	Signal degrade high priority	
1010	Signal degrade low priority	
1001	Unused	
1000	Manual switch	
0111	Unused	
0110	Wait to restore	
0101	Unused	
0100	Exercise	
0011	Unused	
0010	Reverse request	
0001	Do not revert	
0000	No request	

Table 1 K1 Byte, Bits 1-4 Types of Request

Bits 5678	Channel number	Requesting switch action
0000	0	<i>Null channel</i> (no working channel or extra traffic channel). Conditions and associated priority (fixed high) apply to the protection section.
0001 ⋮ 1110	1-14	<i>Working channel</i> Conditions and associated high priority (high or low) apply to the corresponding working sections. For 1+1, only working channel 1 is applicable, with fixed high priority.
1111	15	<i>Extra traffic channel</i> Conditions are not applicable. Exists only when provisioned in a 1:n architecture.

Table 2 K1 Byte, Bits 5-8, Channel No. for Action Switch Req.

Bits 1234	Channel number	Indication
0000	0	<i>Null channel</i>
0001 ⋮ 1110	1-14	<i>Working channel</i> For 1+1, only working channel 1 is applicable.
1111	15	<i>Extra traffic channel</i> Exists only when provisioned in a 1:n architecture.

Table 3 K2 Byte, Bits 1-4 Bridged Channel

Bit (5)	Architecture	Bits (678)	
0	1+1	111	MS-AIS
1	1:n	110	MS-RDI
		101	Reserved for future use
		⋮	
		000	

Table 4 K2 Byte, Bits 5-8

Ring Protection (ITU-T G.841)

Bits 1234	Bridge Request code (1-4)	Destination Node Identification (5-8)
1111	Lockout of Protection (Span) or Signal Fail (Protection) LP-S	<i>The destination node ID is set to the value of the ID of the node for which that K1 byte is destined. The destination node ID is always that of an adjacent node (except for default APS bytes).</i>
1110	Forced Switch (Span) FS-S	
1101	Forced Switch (Ring) FS-R	
1100	Signal Fail (Span) SF-S	
1011	Signal Fail (Ring) SF-R	
1010	Signal Degrade (Protection) SD-P	
1001	Signal Degrade (Span) SD-S	
1000	Signal Degrade (Ring) SD-R	
0111	Manual Switch (Span) MS-S	
0110	Manual Switch (Ring) MS-R	
0101	Wait-To-Restore WTR	
0100	Exerciser (Span) EXER-S	
0011	Exerciser (Ring) EXER-R	
0010	*Reverse Request (Span) RR-S	
0001	*Reverse Request (Ring) RR-R	
0000	No Request NR	

*Note: Reverse Request assumes the priority of the bridge request to which it is responding.

Table 5 K1 Byte, Bits 1-4 Types of Req.; Bits 5-8 Destination Node

Source Node ID (Bits 1-4)	Bit (5)	Long/Short	Bits (678)	Long/Short
Source node ID is set to the node's own ID.	0	Short path code (S)	111	MS-AIS
	1	Long path code (L)	110	MS-RDI
			101	Reserved for future use
			100	Reserved for future use
			011	Extra traffic on protect. channels
			010	Bridged and Switched
			001	Bridged
			000	Idle

Table 6 K2 Byte, Bits 5-8 Destination Node

When measuring APS timing, the triggering event or sensor, such as an AIS-L/MS-AIS, AIS-P/AU-AIS, DS1 AIS, B1, B2, B3, BIP-V/LP-BIP, etc. must be specified. The test set starts measuring time from the moment it senses the event. After the event disappears, the test set stops the measurement and reports whether it falls within the specified switch time. The switch time is how long it takes the network element to switch to the protected line. The industry specified value is 50 ms. If the switch to the protection circuit takes longer than the required switch time, the test set will indicate the test failed. Even after the switch is made, some transient AIS alarms may appear temporarily. After the switch time has passed, the test set will wait until the gate time (measured from the start of the test) expires before timing out the test.

Detail

Connect the test set to the location in the network that you are concerned about. For many applications, this will be a drop point of an ADM. For other applications, it will be a monitoring point within the ring. Examples of both are shown in Figure 7. You will also need to decide

MEASURING APS WITH THE SUNSET 10G, SUNSET OCX, SUNSET SDH, OR STT NETWORK ANALYSIS MODULE

APS testing can be single-ended or dual-ended. In a single-ended test, the test set looks for the triggering event and measures the time it takes the circuit to switch to the backup and remove the AIS. Single-ended tests are most appropriate for in-service monitoring or events triggered by a network element. In a dual-ended test, one test set initiates the alarm or parity errors while the other measures the time it takes to correct.

APS should be tested during installation and can be done for individual network elements or entire linear and ring systems. APS can be tested and measured from PDH/T-Carrier tributaries' drop of the SONET/SDH circuit.

AIS will be present throughout the network during an APS switchover, so measuring the duration of AIS is a valid means of deriving the time that a network requires to complete a protection switchover. The type of AIS will vary depending on the location of the fault relative to the test equipment, as shown in Figure 7.

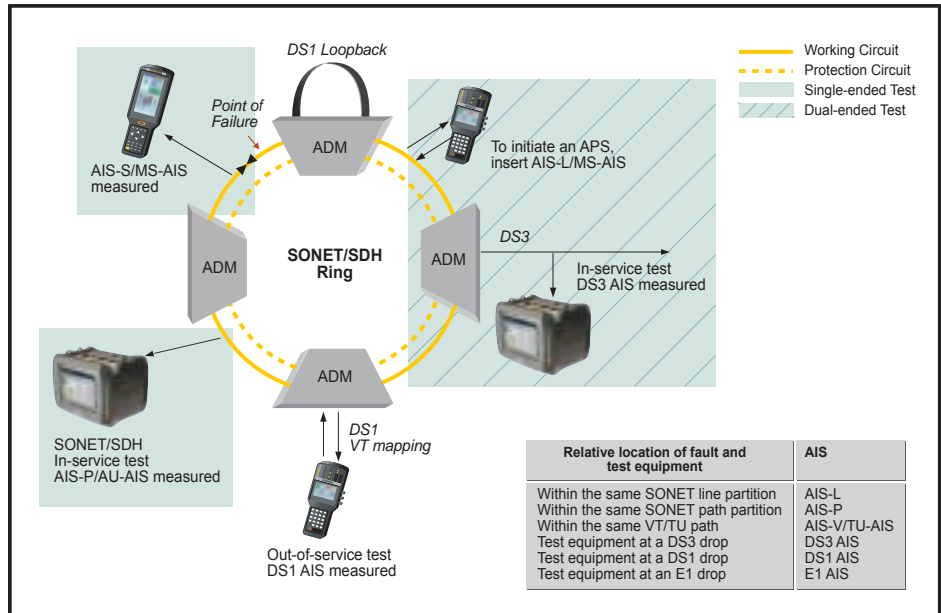


Figure 7 Single-ended vs. Dual-ended APS testing/APS time measurement locations

whether to connect the test set in-service or out-of-service. For most applications, traffic cannot be interrupted, so the testing will be done in-service. If a network is being installed or a new service provisioned, then testing can be done out-of-service. The test set will then generate a test pattern to simulate traffic.

For the test set, APS time can be measured in one direction inside a SONET/SDH ring. Operators then select three parameters to measure the APS time: Sensor, Switch Time Limit and Gate Time Limit. Refer to Figure 8.

Sensor

The Sensor is set to AIS. For an out-of-service test, make sure that pattern synchronization is established before beginning the test.

Switch Time Limit

After the APS time is measured, a "PASS" or "FAIL" will be displayed along with the measured time. The Switch Time Limit allows you to set criteria for the maximum APS time allowed for the network to pass APS testing. In general, this value should be set to 50 ms.

Gate Time Limit

During an automatic protection switchover, AIS may come and go as the NEs progress through their algorithm to switch traffic to the protection circuit. The Gate Time Limit allows you to set a time limit on how long to wait for AIS to come and go. Gate Time Limit must be longer than the Switch Time Limit, but should not be so long that other network events are mistakenly combined with the APS time measurement. Here is another way to think of Gate Time Limit and Switch Time Limit: $(\text{Gate Time Limit}) - (\text{Switch Time Limit}) = \text{the minimum interval required for the circuit to be AIS free}$. A good value for Gate Time Limit is 100 ms.

Starting the measurement

Once the three parameters are set, start the measurement. The SunSet test set is now armed and waiting for an APS event to be detected. Initiate the APS by (1) using a network management terminal, (2) inserting AIS-L with Sunrise Telecom equipment or other means, or by (3) breaking the working circuit. The APS time is measured & displayed.

CONCLUSION

Measuring APS is important to ensure that the SONET/SDH protection mechanism built into your network is working properly. When a failure occurs, minimizing lost traffic through the network will ensure happy end users. Use the APS measurement feature of your Sunrise Telecom SONET and SDH analyzers to ensure that your network APS is configured and operating properly.

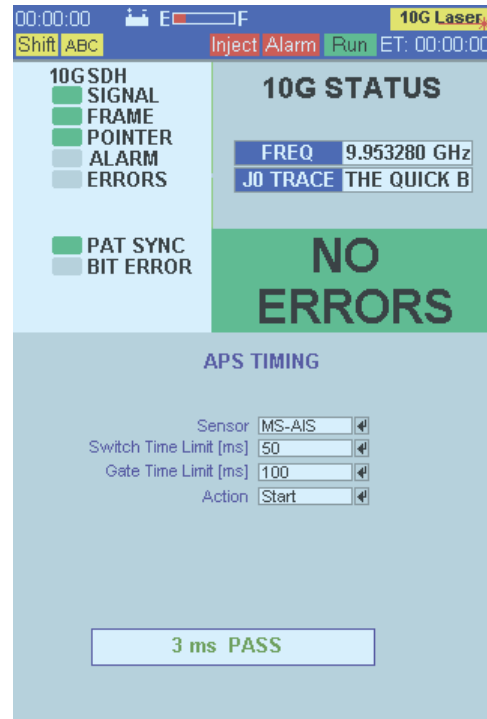


Figure 8 SunSet 10G APS Timing screen