Guidelines for Application of OTN TCM

OIF-OTN-TCM-01.0

June 2013

1 Introduction

Optical networking equipment based on the Optical Transport Network (OTN) standards defined by the ITU supports, as part of its functionality, an extensive set of connection monitoring functionality. Three distinct sets of monitoring overhead are provided: the section monitoring (SM) overhead which supports monitoring of OTU layer segments, analogous to SDH regenerator section monitoring functions; the path monitoring (PM) overhead which supports monitoring of ODU layer end-to-end trails (paths), analogous to SDH path monitoring functions; and tandem connection monitoring (TCM) overhead which supports monitoring of arbitrary sub-network connections. These monitoring functions may be used to monitor segments of an end-to-end OTN trail (path) and can be used to support unprotected or protected connections.

Six levels of TCM, each with various modes of operation, are provided to allow for simultaneous use for different monitoring applications along any each and every individual ODU trail. These applications include: segment protection, administrative domain monitoring, service monitoring, fault localization, verification of delivered quality of service, delay/latency measurements and adjacency discovery. It is important to note that for any given hierarchy of ODU trails (take for example a GbE service carried over an ODU0 trail tunneled over an ODU2 server trail which is in turn carried over an ODU4 trail traversing a DWDM system with 100G wavelength support), each independent ODU trail within that hierarchy is supported by an end-to-end path monitor and also by all six levels of tandem connection monitors. TCMs for one particular ODU layer trail within the hierarchy do not interfere with TCMs assigned for another ODU layer trail within the hierarchy.

TCM functions maybe cascaded or nested along any particular ODU layer trail, which may pass through multiple nodes and administrative domains (an administrative domain is any subnetwork that is operationally administered independently of other subnetworks across the network). The nested or cascaded structure is generally a direct result of the way the administrative domains are nested or cascaded. When cascaded, the same TCM level may be reused between different nodes along the same end-to-end connection, that is, along the same ODU trail. TCM functions nested within the same ODU trail must use different TCM levels and the more nesting that occurs, the more TCM levels are utilized. It is possible, though not highly likely for most ODU trails, that all TCM levels are utilized. It is important to utilize the OTU layer section monitor (SM) and ODU layer path monitor (PM) whenever possible to preserve TCM levels for other functions.

When TCM functions are nested within the same trail, if not assigned and configured correctly, the contents of a particular TCM may be overwritten, causing misinterpretation at the receiving end. There are no mechanisms in the current OTN standards that automatically ensure such misconfiguration does not occur. TCM levels are not automatically assigned and configured. This raises the following questions:

- “What TCM level and TCM mode should be used for a particular application?”

- "How is the TCM level and mode assigned?"
- "How are TCM assignment conflicts avoided?"

As a result it is critical for TCM to be carefully administered within a particular network and its use across different administrative domains (e.g., different carrier networks) must currently be negotiated. This document provides background information on the definitions, modes, and applications of TCM and defines guidelines for interworking of TCM in order to reduce the administration associated with TCM assignment and configuration. TCM assignment using a role-based approach is proposed with default assignment of TCM levels and modes. These defaults would be followed unless specific requirements within a particular network necessitate deviations from the default values. This document also considers the role of the control plane in configuring and administrating TCM levels.

2 Summary of ITU-T Recommendations Regarding TCM

A number of ITU-T Recommendations provide information regarding TCM definition and operations. The following sections summarize the information provided in these various ITU-T Recommendations regarding TCM functions, operations, and applications.

2.1 ITU-T Recommendation G.805 "Generic functional architecture of transport networks"

ITU-T Rec. G.805 deals with common architectural concepts of transport networks including tandem connection monitoring. It defines a tandem connection as an arbitrary series of contiguous "link connections" and/or "subnetwork connections" which represents the part of a trail that requires monitoring independently from the monitoring of the complete trail. It also defines the functions required for tandem connection monitoring. These functions include (but are not limited to):

- Monitoring functions for the tandem connection that are independent of defects and errors that occur upstream of the tandem connection (outside the tandem connection endpoints)
- Verification of tandem connection connectivity and continuity
- Fault management of the tandem connection including detection and reporting of near-end and far-end failure/alarm conditions
- Performance management of the tandem connection including detection and reporting of near-end and far-end error performance

Rec. G.805 also defines several applications for tandem connection monitoring based on the concept of a monitoring domain. Three general tandem connection domain applications are identified:

- *Protected domain* – A domain where tandem connection monitors are used to monitor the status (failure state and error performance) of working and protection connections for the purposes of controlling protection switching operations
- *Serving operator administrative domain* – A domain where a tandem connection monitor is used by a service provider (e.g., carrier or carrier's carrier) to monitor the status (failure state and

error performance) of a connection delivered to a customer (e.g., an end customer or another carrier)

- *Service requesting administrative domain* – A domain where a tandem connection monitor is used by a customer to monitor the status (failure state and error performance) of a connection received from a service provider

2.2 ITU-T Recommendation G.872 "Architecture of optical transport networks"

ITU-T Rec. G.872extends the architectural concepts provided by Rec. G.805 that are applicable to optical transport networks. It discusses architectural concepts of optical channel data unit (ODU) connection monitoring including tandem connection monitoring.

ITU-T Rec. G.872 discusses the concept of nested connections up to the maximum number of levels defined by the requirements of the specific technology (e.g., ITU-T Recommendation G.709). It notes that the number of connection monitoring levels that can be used by each operator/user involved in an optical channel data unit (ODU) connection must be negotiated by the parties involved. It also provides an example of a typical optical channel data unit (ODU) connection with five levels of nested connection monitoring (see Figure 1 below – each color represents a different level of nested monitoring).

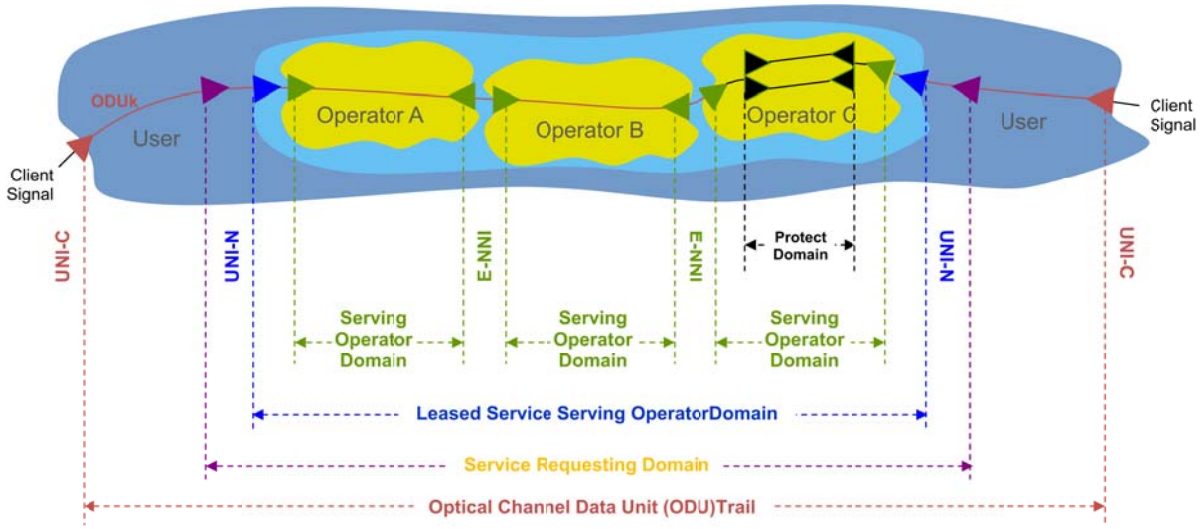

Figure 1: TCM application example [Note: This figure is based on ITU Rec. G.872 Figure 7]

This example illustrates an end to end trail that contains a service requesting administrative domain extending from a customer interface across a serving operator administrative domain providing the leased service to another customer interface. Within the leased service serving operator administrative domain are three separate cascaded service operator administrative domains, one of which contains a protected domain. The customer monitors the quality of the leased service while the leased service serving operator monitors the quality of service provided to the customer. In addition, each serving operator domain is monitored independently along with the protected domain within one of the serving operator domains. In this example, the same TCM level (green) is reused by Operators A, B and C for end-to-end monitoring of their specific domains.

2.3 ITU-T Recommendation G.709 "Interfaces for the Optical Transport Network (OTN)"

ITU-T Rec. G.709 defines the overhead required to support tandem connection monitoring for the OTN. This includes all TCM bit and byte assignments within the OTN frame structure and the definition of the functions of those bits and bytes. G.709 specifies that OTN provides six fields or levels of ODUk TCM (referred to as TCM1, TCM2, …TCM6) and the number of active TCM levels along an ODUk trail may vary between 0 and 6 (see Figure 2 below). At domain interfaces, G.709 specifies that the provisioning of the maximum number of levels which will be passed through the domain is possible (default of three levels). These tandem connections should use the lower levels (i.e. TCM1, TCM2 or TCM3). Levels beyond the maximum may/will be overwritten in the domain.

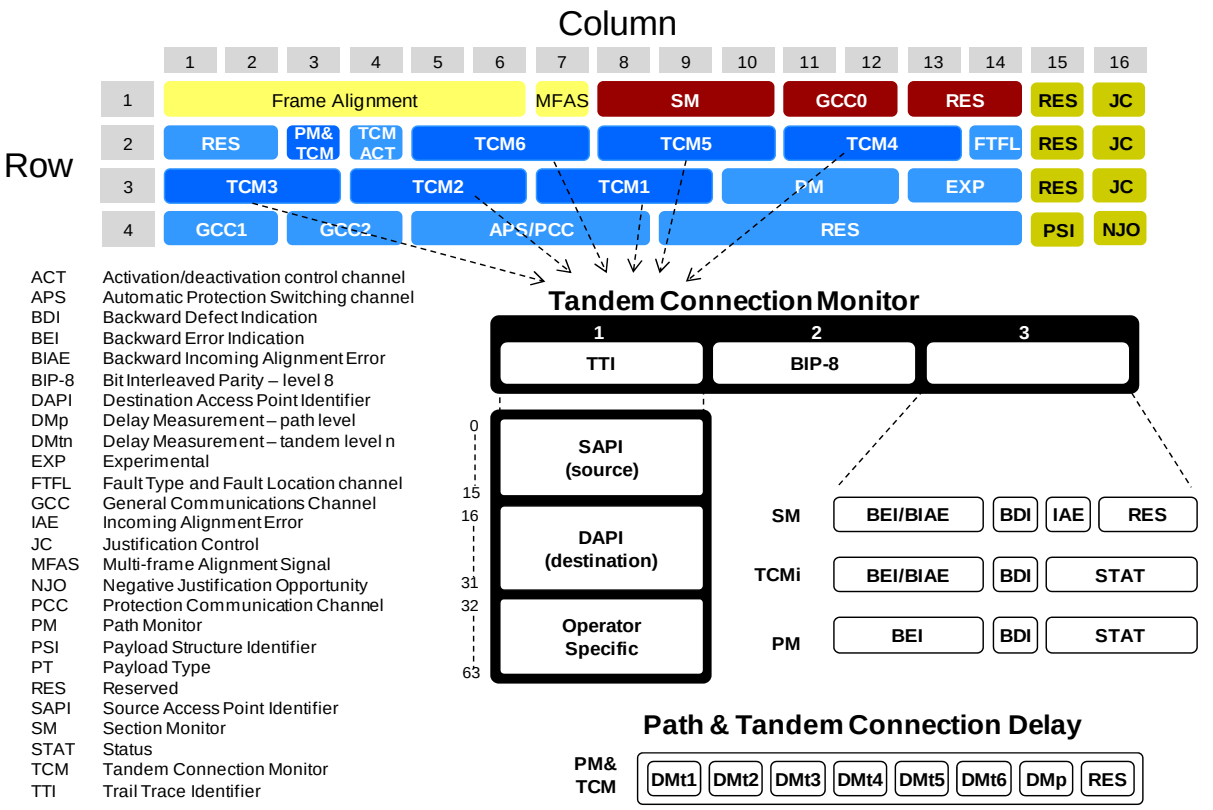

Figure 2: Location of the TCM overhead (shown as dark blue color) within the OTUk frame [Note: This figure is based on ITU Rec. G.709 Figure 15-3]

G.709 specifies that the TCM functions for monitored connections may be nested, cascaded or both. Overlapping of TCM functions is an additional configuration supported for testing purposes only but must be operated in a non-intrusive mode where maintenance signals are not generated.

G.709 also describes the network applications supported by the ODUk TCM functions and references [ITU-T G.805] and [ITU-T G.872]. The applications referenced are the service requesting administrative domain (called optical UNI-to-UNI tandem connection monitoring), service operator administrative domain (called optical NNI-to-NNI tandem connection monitoring), and protected domain (linear

protection, shared ring protection, and automatic restoration) applications. In addition, G.709 identifies the use of TCM functions to support fault localization and service maintenance functions.

2.4 ITU-T Recommendation G.798 "Characteristics of optical transport network hierarchy equipment functional blocks"

ITU-T Rec. G.798 provides the modelling of the OTN equipment functional blocks including the TCM functions. The definition of the TCM processing includes defect detection and generation, defect correlation, consequent actions (e.g., maintenance signal generation), and performance monitoring functions. G.798 also provides an appendix with examples of TCM applications.

G.798 models TCM functions through separate termination, adaptation, and control elements. The termination and adaptation elements are further sub-divided into separate unidirectional components dedicated to TCM source and sink operations. The termination elements deal mainly with the generation and insertion of TCM overhead bits/bytes at the source end of a tandem connection, and extraction and processing of the TCM overhead bits/bytes at the sink end of a tandem connection. The adaptation elements deal mainly with the layer-to-layer processing required at the source and sink ends of a tandem connection (e.g., detection of incoming alignment errors or insertion of maintenance signals).

2.5 ITU-T Recommendation G.798.1 "Types and characteristics of OTN Equipment"

ITU-T Rec. G.798.1 provides an example of assigned TCM levels within a network and describes the maintenance signal interactions (e.g., AIS propagation) between tandem connections that are concatenated in the same sublayer and between tandem connections that are at different sublayers. G.798.1 also provides examples of I-NNI, E-NNI and UNI-N ports in which the presence of TCM functionality is illustrated.

2.6 ITU-T Recommendation G.7710 "Common equipment management function requirements"

ITU-T Rec. G.7710 provides information related to management of TCM functions (configuration, fault, performance, etc.) including TCM activation. One of the aspects of activation that Rec. G.7710 covers is the activation of a TCM for different nesting scenarios. These include activating a TCM that is nested within one or more other TCM levels, activating a TCM that has one or more existing TCM levels nested within it, and activating a TCM that is a combination of the previous two cases. This document specifies that two activation behaviors are possible from an NE perspective:

- TCM levels can be allocated flexibly, that is, in any order
- TCM levels cannot be allocated flexibly, that is, they require a fixed ordering

The first case requires only that the TCM be activated at the correct location with respect to any existing TCM levels. The second case may require that existing TCM levels be rearranged in order to support a new TCM level.

2.7 ITU-T Recommendation G.7714.1 "Protocol for automatic discovery in SDH and OTN networks"

ITU-T Rec. G.7714.1 describes the methods, procedures and transport plane mechanisms for discovering layer adjacency for automatically switched optical networks (ASON).Section 6 of G.7714.1 points out the use of the TTI field of TCM level 6 as the default mechanism for carrying layer adjacency discovery messages.

2.8 ITU-T Recommendations G.873.1 "OTN Linear Protection" and G.873.2 "ODUk Shared Ring Protection "

ITU-T Recs. G.873.1 and G.873.2 define the automatic protection switching (APS) protocol and protection switching operation for OTN linear and ring protection schemes at the optical channel data unit (ODUk) level. One of the key schemes provided in G.873.1 and G.873.2 is ODUk subnetwork connection protection with sublayer monitoring (SNC/S).In this case protection switching is triggered by signal fail or signal degrade defects detected at the ODUkT sublayer trail (TCM). An ODUkT sublayer trail is established for each working and protection entity. Protection switching is triggered only on defects of the protected domain. The Recommendations point out that care has to be taken to make sure that there are no overlapping domains of use of a TCM level (i.e. TCM levels should only be used in nested or concatenated modes).

Rec. G.873.2 also suggests the use of TCM level 6 for monitoring an ODUk connection which is supported by two or more concatenated ODUk link connections (supported by back-to-back OTUk trails). G.873.2 specifies an ODU SRP-1 protection application which uses the TCM6 field to monitor the status/performance of the ODU connection between two adjacent ODU SRP-1 nodes.

3 Terminology and Definitions for OTN TCM

3.1 ITU-T Rec. G.798 TCM Modes

ITU-T Rec. G.798 defines three modes for TCM:

- Operational mode
    - In Operational mode, the TCM information is extracted from the TCM field and used to trigger actions such as alarm generation, switching action, etc.
- Transparent mode
    - In Transparent mode, the TCM information is passed through without change (i.e., transparently) and no processing is performed.
- Monitoring mode
    - In Monitoring mode, TCM information is processed to recover defects and status information, but is still passed through unchanged to succeeding nodes.

3.2 TCM Functional Blocks

The Rec. G.798 TCM functional blocks and their basic functionality are as follows:

- ODUkT/ODUk_A_So: ODUkT/ODUk Adaptation Source Function

    - Starts a selected TCM level and can initiate maintenance signals (LCK) if OPERATIONAL
    - Provides access to ODUk PM
    - Insert APS Overhead if OPERATIONAL
- ODUkT/ODUk_A_Sk: The ODUkT/ODUk Adaptation Sink Function
    - Ends a selected TCM level and can initiate maintenance signals (AIS, LCK) if OPERATIONAL
    - Provide access to ODUk PM
    - Access APS Overhead if OPERATIONAL
- ODUkT_TT_So: ODUkT Trail Termination Source Function
    - Computes the BIP8, adds tandem connection monitoring overhead (TCMOH) if OPERATIONAL
    - Inserts BDI/BEI if OPERATIONAL OR MONITOR
- ODUkT_TT_Sk: ODUkT Trail Termination Sink Function
    - Computes BIP8, collects defects for PM, and extracts TCMOH if OPERATIONAL or MONITOR
- ODUkT_TCMC: TCM Control Function
    - Responsible for activation and deactivation of a TCM trail, sets TCM level, and sets modes for termination and adaptation functional blocks

These functions are shown in the figure below:

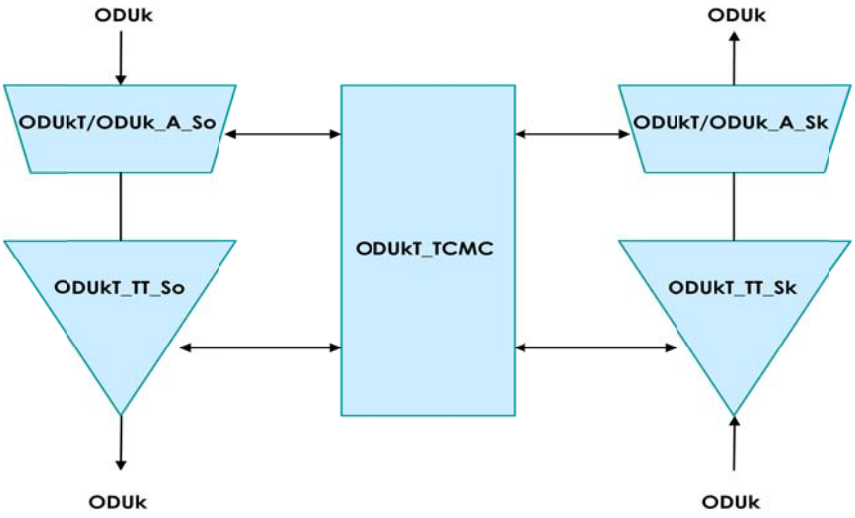

Figure 3: G.798 TCM Functional Blocks

The following table summarizes the different combinations of TCM mode and where they are used.

Table 1: Combinations of TCM modes from ITU-T G.798

Source/ Sink	Use	ODUkT_TT Mode	ODUkT/ODUk_A Mode	Functions

Source	TCM assigned	Operational	Operational	• Originate TCM Trail • Insert TTI, BIP8 • Insert BDI, BEI/BIAE, LCK • Insert IAE • Insert APS • Insert and Process DM
Source	TCM not assigned	Transparent	Transparent	• Transparent Pass Through of TCMOH
Sink	TCM assigned	Operational	Operational	• Terminate TCM Trail, Reset TCMOH • Process BIP8 • Extract TTI • Extract BDI, BEI/BIAE • Extract STAT • Return DM to Remote Point • Return BDI, BEI/BIAE to Remote Point • Extract APS • Insert ODUk LCK • Insert ODUk AIS/SSF Consequent Action
Sink	"Shadow" TCM assigned	Operational	Transparent	• Transparent Pass Through of TCMOH • Process BIP8 • Extract TTI • Extract BDI, BEI/BIAE • Extract STAT • Return DM to Remote Point • Return BDI, BEI/BIAE to Remote Point
Sink	Test Purposes	Monitor	Operational	• Terminate TCM Trail, Reset TCMOH • Process BIP8 • Extract TTI • Extract BDI, BEI/BIAE • Extract STAT • Return BDI, BEI/BIAE to Remote Point • Extract APS • Insert ODUk LCK • Insert ODUk AIS/SSF Consequent Action
Sink	Test Purposes	Monitor	Monitor (or Transparent)	• Transparent Pass Through of TCMOH • Process BIP8 • Extract TTI • Extract BDI, BEI/BIAE • Extract STAT • Return BDI, BEI/BIAE to Remote Point
Sink		Transparent	Operational	For further study

Sink	TCM not assigned	Transparent	Transparent	• Transparent Pass Through of TCMOH
Sink	SNC/Ns Protection	Non-Intrusive Monitor		• Process BIP8 • Extract TTI • Extract BDI, BEI/BIAE • Extract STAT • Extract APS

Note: Access to the APS bytes is required for bidirectional protection switching.

4 TCM Roles

4.1 Introduction

Many of the ITU-T Recommendations address various TCM applications. Recs. G.805, G.872, and G.709 provide information related to three basic applications based on partitioning of the network into specific domains: protected domains (linear, ring, etc.); serving operator administrative domains (which can be nested or cascaded); and service requesting administrative domains (associated with the customer leasing the service from the service operators). The protection standards define the use of TCM for link monitoring for linear (Rec. G.873.1) and ring (Rec. G.873.2) applications. Rec. G.709 includes the use of TCM for fault sectionalization and isolation, i.e., maintenance functions. Rec. G.7714.1 includes the use of TCM for layer adjacency discovery operations.

In addition to roles-based applications, Rec. G.709 includes TCM allocation from a broad perspective by specifying which set of TCM levels should be assigned to pass through a domain (the lower TCM levels) and which TCMs should be assigned within the domain (the higher TCM levels). In fact, example multi-domain configurations suggest, but do not require, specific levels for specific applications. In general, TCM assignment must to be negotiated within the service provider community. Rec. G.873.2, recommends a specific TCM level (TCM6) for link monitoring in support of ring protection, and Rec. G.7714.1 recommends TCM6 for layer adjacency discovery functions. So some precedent has been set for the utilization of specific TCM levels for specific applications, although this has not been broadly applied and negotiation of TCM levels between service providers is still necessary in general.

The information provided by the ITU-T Recommendations can be extended to form the basis of roles-based TCM assignment. Figure 4 below illustrates a general network diagram with domain partitioning that includes various key topological elements.

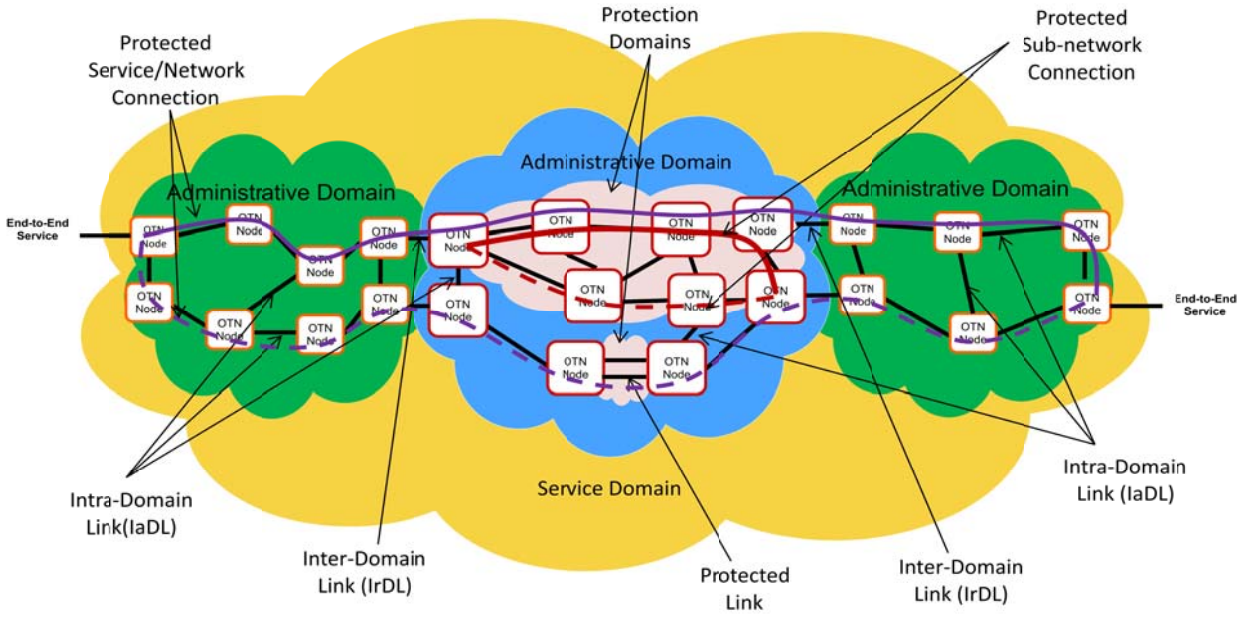

Figure 4: Generic Network Diagram with Domain Identification

This diagram is used to identify a set of roles each of which can be assigned a specific TCM level. By assigning a specific level to a specific role the possibility of automatic assignment and configuration of TCM without carrier negotiation of TCM level usage for the majority of end-to-end service connections may be supported. Only in special case situations would TCM negotiation be required.

Figure 4 shows a network made up of OTN nodes (network elements) interconnected by node-to-node links. This diagram is similar to Figure 1 which was based on information from Rec. G.872 less the customer network portion, since this paper is intended to mainly address service provider aspects. However, there are some key differences. A node in the context of this white paper represents an OTN network element that sources and terminates a tandem connection monitoring level, not necessarily any OTN network element, since this white paper is dealing with the application of TCM functions. Nodes in this context will typically provide ODU switching functionality, but may not in all cases. OTN network elements that are not capable of OTN switching functionality, such as OTUk regenerators or multiplexers, or OTN capable DWDM equipment, often exist between the switching nodes where in most cases the connections between those elements may be managed through the use of OTU section monitor or in some cases ODUk path monitoring functions thus preserving TCM levels for other uses. Such network elements would not be considered nodes in the context of this white paper. A link in this context generally represents an ODUk link connection between OTN nodes that utilizes a TCM for connection monitoring, not an OTUk layer link connection (note that the ODUk link connection may be either a higher order or lower order ODUk as defined by ITU standards).

Links between nodes contained within a particular administrative domain (e.g., service provider network), or serving operator administrative domain from Rec. G.805, are referred to as intra-domain

links (IaDL), while links that interconnect nodes in different administrative domains are termed inter-domain links (IrDL). Links between nodes, either IaDL or IrDL links, may be unprotected or protected. Protected links exist within a protection domain.

An end-to-end network that provides service to an end customer is made up of one or more administrative domains[1]. Each administrative domain can provide connectivity across its nodes and links to allow services to be established across its domain. These administrative domain connections may be protected on a segment by segment basis where a segment could traverse one or more links, or they could be protected on an end-to-end basis. A protection domain would exist for each protected segment or for the entire connection across the administrative domain.

An end-to-end customer service is supported across the network of one or more administrative domains. This is referred to as the service domain in Figure 3 and is equivalent to the leased service serving operator administrative domain from G.872. That connection may also be unprotected or protected, and if protected has an associated protection domain.

There are several components of this network that require monitoring. These include the links, either intra- or inter-domain links, the domain connections that traverse an administrative domain, and the service connections that traverse the service domain. Also any links or connections that are protected must be monitored to control protection switching operations. All of these components within an OTN network could utilize TCM functions and are candidates for automatic TCM assignment and configuration.

With respect to OTN protection mechanisms, many forms of OTN protection currently exist. These include

- SNC/I – where an OTUk SM that inherently terminates an OTUk trail is used to control protection operations for the underlying ODUk connection
- CL-SNCG/I – where an ODUk PM that inherently terminates a higher order ODUk trail is used to control protection operations for the underlying group of multiplexed ODUj connections
- SNC/S – where a ODUk TCM that terminates an ODUk tandem connection is used to control protection of all underlying ODU connections
- SNC/Ns - where a TCM is used to non-intrusively monitored an associated ODU connection and control protection operations
- SNC/Ne - where a PM is used to non-intrusively monitored an associated ODU connection and control protection operations

This white paper will address only the SNC/S and SNC/Ns protection mechanisms as they are the only ones applicable to TCM assignment. The other mechanisms, SNC/I, CL-SNCG/I, and SNC/Ne can be utilized where applicable and may preserve TCM levels for other applications.

[1] A particular service provider network may itself consist of multiple administrative domains.

It is important to note that this white paper attempts to presents guidelines for the automatic assignment of TCM levels to specific roles. This is intended to cover the majority of applications commonly found in OTN transport and switching network. It is not intended to be all-inclusive, that is, to cover all possible configurations. Network topologies that cannot be supported by the recommended assignments may always have TCMs assigned in a manner supporting the particular application. It is also important to recognize that in the context of this white paper links may run at any applicable rate, depending on the underlying physical transport mechanism supporting the link, while the domain and service connections are generally intended to represent connections at the required rate to support the end-to-end service, for example, a GbE service carried on an ODU0 end-to-end through multiple domains. It is not required, however, that all domains operate at the service rate. For example, a carrier may lease a high capacity connection ODU2 connection across another carrier domain for the purpose of transporting many ODU0 service containers. In the context of this white paper the high capacity ODU2 connection would represent and end-to-end service from the carrier's carrier perspective and would be subject to the TCM assignments described but for the ODU2 connection. Whereas the ODU0 connection would be treated as an end-to-end connection from the perspective of the carrier providing the GbE service transport and also be subject to the TCM assignment defined in this white paper but now for the ODU0 connection.

4.2 Application of TCMs to Links

4.2.1 Link Monitoring

In this role, TCM supports the following functions:

- Link failure/degrade detection (with or without OTUk regenerators)
- Fault sectionalization
- Link level APS (line switching equivalent)
- Link layer adjacency discovery

Recommended TCM mode and level assignment: Operational mode TCM6

This TCM level could be automatically assigned and configured at link interface provisioning time. Both unprotected and protected configurations can be supported. Note that it is possible for an OTUk regenerator to be present within the monitored link shown in Figure 5.

Unprotected Link Monitoring Points:

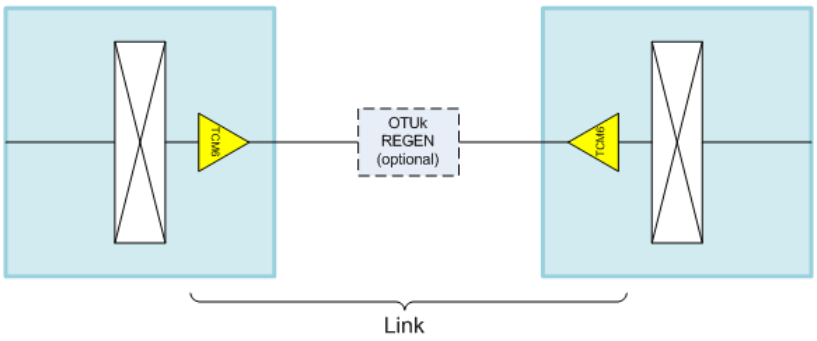

Figure 5: Generic Diagram of an Unprotected Link Monitored using TCM6.

4.2.2 Link Level APS

For link monitoring only SNC/S protection should be implemented. Though SNC/Ns link protection could be implemented, it is not recommended. SNC/Ns configurations cannot support layer adjacency discovery of working and protect links since only a non-intrusive monitor is present on the link side of the switch (the non-intrusive monitor has no ability to insert discovery information).

SNC/S Protected Link Monitoring Points:

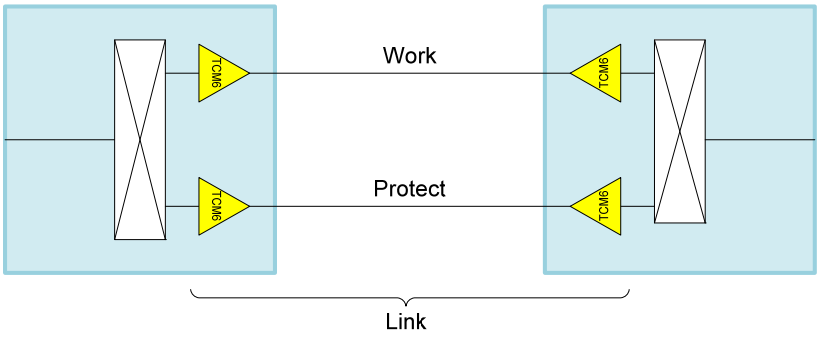

Figure 6: Generic Diagram of an SNC/S Protected Link using TCM6.

4.2.3 Layer Adjacency Discovery

ITU-T Rec. G.7714.1 specifies a specific discovery message format utilizing the SAPI field of the TTI byte of TCM6 for this function.

4.3 Application of TCMs to Administrative Domain Connections

4.3.1 End-to-End Domain Connection Monitoring

In this role, TCM supports the following functions:

- Domain failure/degrade detection

- Fault sectionalization
- Domain signal quality monitoring

Recommended TCM mode and level assignment: Operational mode TCM4

Unprotected End-to-End Domain Connection Monitoring Points:

In this configuration, the TCM is terminated at the domain boundary. This termination is always required regardless of how protection is configured within or across the domain in order to provide the proper end-to-end domain monitoring. Note that protection domains using TCM5 and link monitoring using TCM6 may be nested within the domain boundaries.

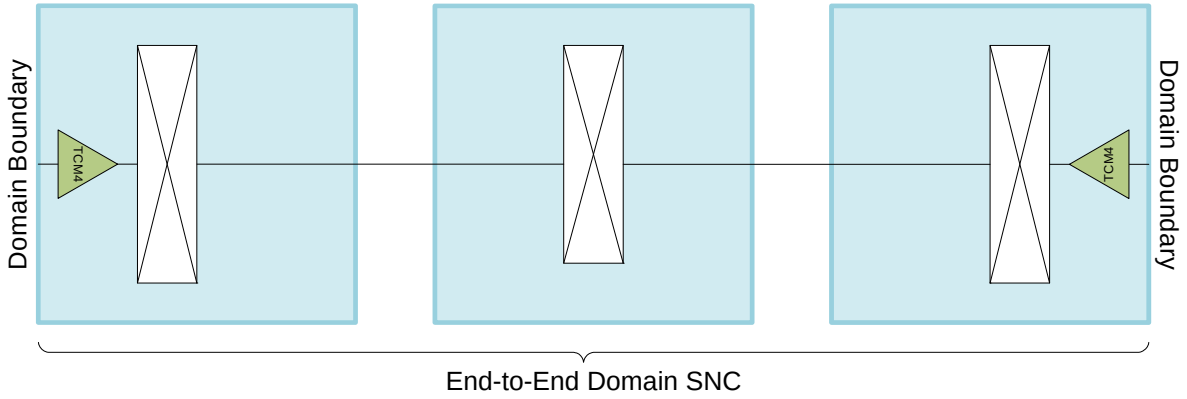

Figure 7: Generic Diagram of End-to-End Domain Connection Monitoring using TCM4.

4.3.2 SNC Protection for Administrative Domain Connections

Protection may be required on subnetwork connections within an administrative domain. These subnetwork connections may traverse a portion of the domain or traverse the domain end-to-end. Protected subnetwork connections that traverse only a portion of the domain may be cascaded. Each subnetwork connection may be independently protected.

In this role, TCM supports the following protection configurations:

- SNC/S protection: supports bounded protection domains without sympathetic[2] switching (protection domain is bounded by the TCM)

[2] Sympathetic switching is the term used here to identify protection switching activity caused by failure propagation into the intended protection domain from outside the intended protection domain. This may occur for protection configurations utilizing non-intrusive monitoring when the monitoring termination is located in a network element other than the one supporting the non-intrusive monitoring and the protection switching functions. This configuration is illustrated in Figure 11-10 of ITU Recommendation G.808.1.

- SNC/Ns protection: supports unbounded protection domains that may exhibit sympathetic switching (protection domain boundaries are not bounded by the TCM but by non-intrusive monitors)

Recommended TCM mode and level assignment: Operational mode TCM5 and TCM4 non-intrusive monitor for end-to-end domain connection protection using SNC/Ns

SNC/S Protected Domain Connection Monitoring Points:

In this configuration the TCMs are terminated on the network side of the switch function. Note that nested link monitors may exist on any node-to-node links (as defined in the Link Monitoring section). The protection switching domain is bounded by the TCM terminations so failures outside the protection domain have no effect on protection switching operation.

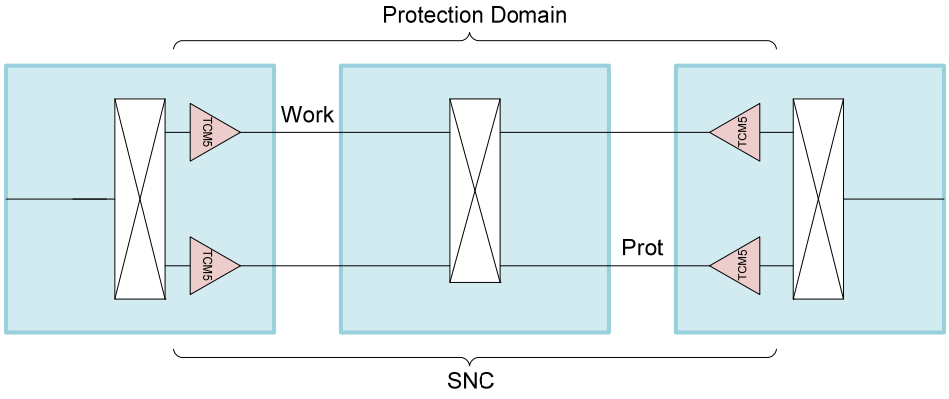

Figure 8: Generic Diagram of an SNC/S Protected Domain Connection using TCM5.

This is the preferred scheme for all intra-domain SNCP configurations (subnetwork connections within a domain that do not traverse the domain end-to-end) and may also be used for end-to-end domain connections.

SNC/Ns Protected Domain Connection Monitoring Points for Domain Connections:

In this configuration the TCMs are terminated outside the protection domain and non-intrusive monitors are provided to control the switch function. Note that nested link monitors may exist on any node-to-node links (as defined in the Link Monitoring section). The protection switching domain is not bounded by the terminated TCM but by the non-intrusive monitors, therefore it is possible for upstream defects to cause fault propagation into both working and protect subnetwork connections, which may result in sympathetic switching operation (switching due to faults outside the protection domain). For

this reasons, use of the SNC/Ns protection mechanism is only recommended when the TCM termination occurs within the same equipment as the non-intrusive monitoring function[3]. This limits the possibility of upstream fault propagation into the protection domain.

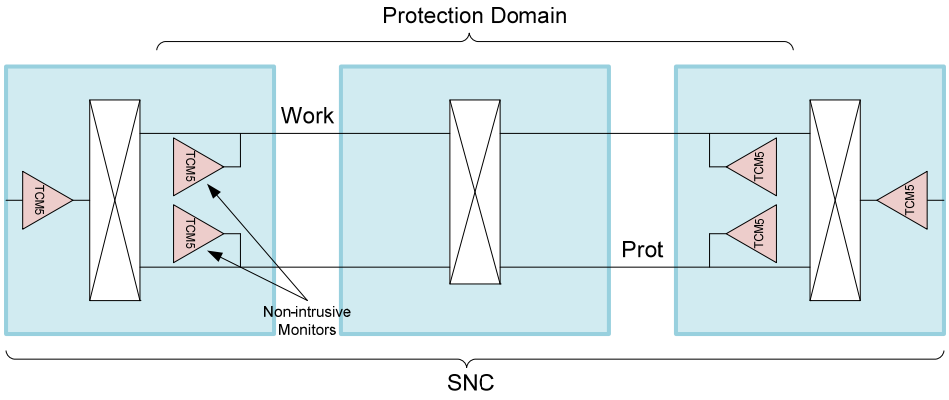

Figure 9: Generic Diagram of an SNC/Ns Protected Domain Connection using TCM5.

When SNC/Ns protected intra-domain SNCs are cascaded, it may be possible for TCMs to overlap as illustrated in Figure 10. The presence of overlap is dependent on the protection and TCM implementation. Because G.709 defines overlapping TCM operation for test purposes only, it is not recommended to use cascaded SNC/Ns in operational networks when this results in overlapped TCMs.

[3] In the case the non-intrusive monitor is not located in the same NE as the Termination (giving a similar architecture as in SDH implementations) the sympathetic switching can be avoided by an appropriate hold off timer.

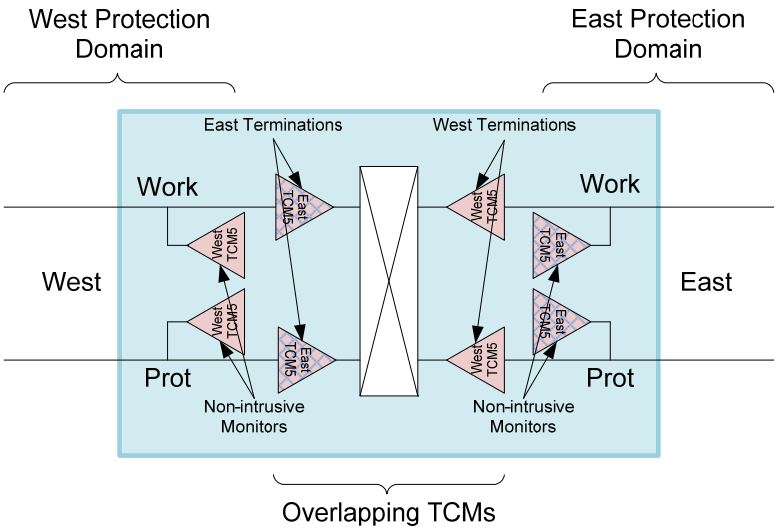

Figure 10: Overlapping TCMs with Back-to-Back SNC/Ns Protection

SNC/Ns Protected Domain Connection Monitoring Points using TCM 4 for End-to-End Domain Connections:

In this configuration, TCM4may be used to support end-to-end domain connection protection as well as the end-to-end domain connection monitoring. SNC/Ns protection is appropriate in this application since the domain termination and the non-intrusive monitors would be located within the same node. -

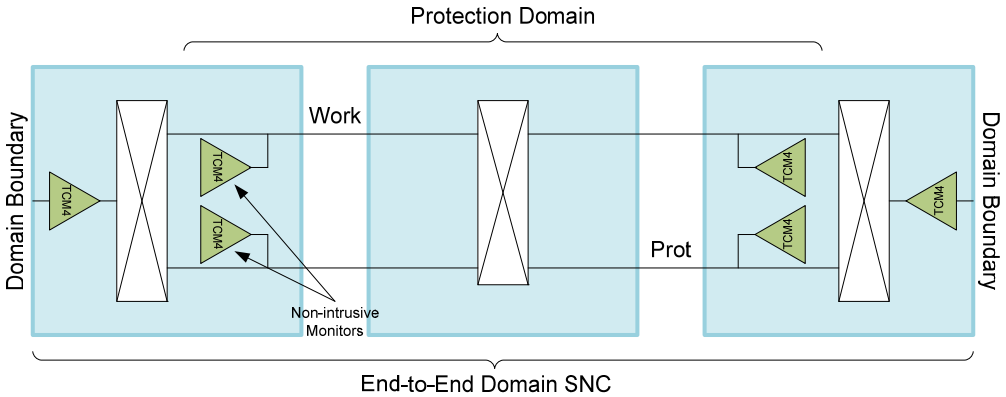

Figure 11: Generic Diagram of an SNC/Ns Protected End-to-End Domain Connection using TCM4

4.4 Application of TCMs to End-to-End Service Connections

4.4.1 End-to-End Service Connection Monitoring

In this role, TCM supports the following functions:

- Service failure/degrade detection
- Service signal quality monitoring
- SLA verification (may function as the Domain Monitor for a single domain service connection)

Recommended TCM mode and level assignment: Operational mode TCM2

Unprotected End-to-End Service Connection Monitoring Points:

In this configuration, the TCM is terminated at the service boundary. This termination is always required regardless of how protection is configured in order to provide the proper service monitoring. Note that administrative domains using TCM4, protection domains using TCM5 and link monitoring using TCM6 may be nested within the service boundaries. It should be noted that there are cases where a service connection traverses only a single administrative domain. In these cases there is no real need to set up separate end-to-end domain connection monitoring and end-to-end service connection monitoring functions. In these cases it is recommended to utilize the end-to-end service connection monitor for both functions thus preserving the intermediate TCM levels for other applications.

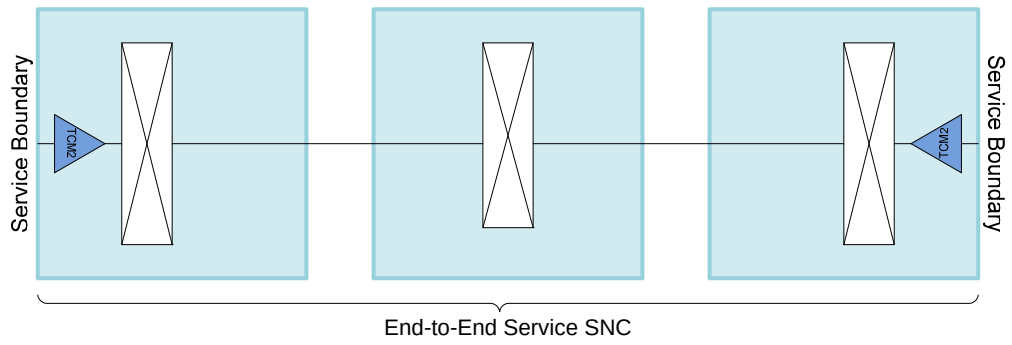

Figure 12: Generic Diagram of End-to-End Service Connection Monitoring using TCM2.

4.4.2 SNC Protection for End-to-End Service Connections

Protection may be required on end-to-end service subnetwork connections. Each end-to-end subnetwork connection may be independently protected.

In this role, TCM supports the following protection configurations:

- SNC/S protection: supports bounded protection domains without sympathetic switching (protection domain is bounded by the TCM)
- SNC/Ns protection: supports unbounded protection domains that may exhibit sympathetic switching (protection domain boundaries are not bounded by the TCM but by non-intrusive monitors)

Recommended TCM mode and level assignment: Operational mode TCM3 for SNC/S and TCM2 for SNC/Ns

SNC/S Protected End-to-End Service Connection Monitoring Points:

In this configuration the TCMs are terminated on the network side of the switch function. The protection switching domain is bounded by the TCM terminations so failures outside the protection domain have no effect on protection switching operation.

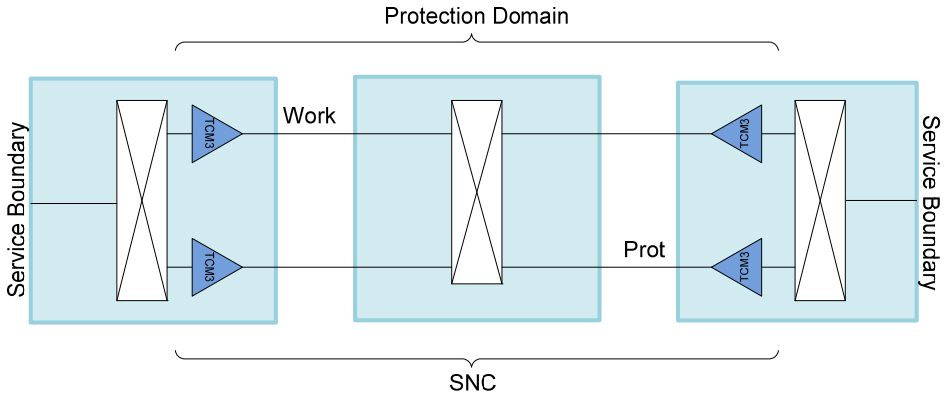

Figure 13: Generic Diagram of an SNC/S Protected Service Connection using TCM3.

SNC/Ns Protected End-to-End Service Connection Monitoring Points using TCM2:

In this configuration, TCM2 is reused to support end-to-end service protection. This is the preferred configuration for SNC/Ns protected service connections as it preserves TCM3 for other uses. SNC/Ns protection is appropriate in this application since the service termination and the non-intrusive monitors would be located within the same node.

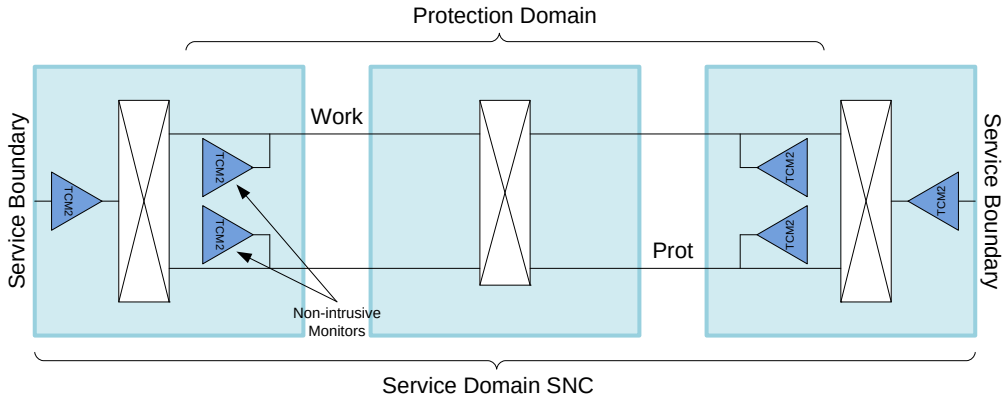

Figure 14: Generic Diagram of an SNC/Ns Protected End-to-End Service Connection using TCM2

4.5 Customer TCM

In this role, TCM supports the following functions:

- Service provider service quality verification

Recommended TCM mode and level assignment: Operational mode TCM1

In this role, a TCM is reserved for end-to-end customer use. This corresponds to the service requesting administrative domain from Rec. G.872. A service provider may utilize this TCM level when the mapping of the client signal (e.g., Ethernet client, SONET/SDH client, etc.) into an ODUk is provided by the service provider equipment.

4.6 Maintenance Operations

The TCM assignments for the roles described in the previous sections provide the means for monitoring various connection levels to determine connection quality, to detect connection failure, and to drive protection switching operations. These monitors also support the process of defect and fault sectionalization/localization by being able to determine the domain or link in which the defect or failure has occurred. By themselves they may not be sufficient for isolating a defect or failure to a specific facility (e.g., fiber optic span) or equipment (i.e., specific network element). Additional monitoring may be required to perform these operations. In some cases, use of the OTU layer section monitor may be sufficient, but that may not address all cases. When required additional tandem connection monitors may be assigned on an as needed basis to support defect and fault isolation of any arbitrary connection within a domain or link.

One of the issues with the use of TCM for arbitrary connection monitoring to support additional maintenance operations is the determination of the TCM level to be used for these functions. As can be seen from the roles based TCM assignments described in the previous sections, many or even all of the TCM levels may already be in use for specific roles. Insertion of a maintenance TCM level at an improper point could cause conflict with other TCMs already assigned. Even if a TCM level is available, maintenance personnel would be required to determine which TCM levels are already in use, including those outside the domain of interest, in order to make the proper level selection. In multi-domain environments this may often be difficult and time consuming.

A second issue that may arise is the actual ability to activate the chosen TCM level at the desired point within the network. As was described in section 2.6, ITU Recommendation G.7710 defines two possible implementations for TCM assignment: assignment of TCM levels in any order, or strict ordering of TCM levels within a network element (e.g., level 6 nested within level 5, level 5 nested within level 4, etc.). This means that if a TCM level is available for use, depending on the point of insertion and the network element capability, it may not be possible to actually utilized the level where intended.

An alternative to the assignment of a TCM level for maintenance functions is the re-use of the existing TCM levels, defined for the roles described in the previous section, to provide additional maintenance support, particularly with regard to defect or fault sectionalization/localization. As described in section 3, tandem connection monitors support several modes of operation. One of those modes is the Monitor Mode which is applicable to trail termination sink and adaptation sink functions. A trail termination sink function, when operated in Monitor Mode, provides the same behavior as a trail termination sink in Operational Mode. However, an adaptation sink operating in Monitor Mode, unlike one in Operational Mode, passes TCM overhead transparently and does not take any consequent actions upon detection of termination defects. This means that a TCM sink function (both trail termination and adaptation) operating in Monitor Mode and at the same level as the TCM level already being utilized for a particular end-to-end connection monitoring role, coupled with at Transparent TCM source function (both trail termination and adaptation), may be inserted at any point along the end-to-end connection to monitor the connection up to the insertion point. By inserting the Monitor Mode TCM at successive downstream monitoring points, it is possible to locate the source of a defect or fault along the connection. This process does not utilize any additional TCM levels, therefore never suffers from TCM level conflicts, and only requires that maintenance personnel understand which TCM level is being used for the particular connection they intend to monitor.

The process described above would generally require that Monitor Mode TCMs be inserted in both directions of a connection (to address unidirectional defects and faults in either direction), and requires that data provided by the Monitor Mode TCM sink function (BIP errors, fault detection, etc.) be directly accessible in order to determine the location of the defect or fault. In some cases it may be desirable to monitor both directions of a connection simultaneously. In this case, coupling a Monitor Mode TCM sink with an Operational Mode TCM source, and inserting that at intermediate points along the connection, not only allows both directions up to the insertion point to be independently monitored,

but allows the monitoring data for both directions to be accessible at the original TCM endpoint using the single-ended maintenance functions (BDI/BEI) provided by the TCMs.

Figure 15 below illustrates the process of successive insertion of a bidirectional Monitor Mode TCM for sectionalization/localization of defects/failures along an inter-domain or intra-domain link connection. Figure 16 illustrates the process of successive insertion of a bidirectional Monitor Mode TCM for sectionalization/localization of defects/failures along an administrative domain connection.

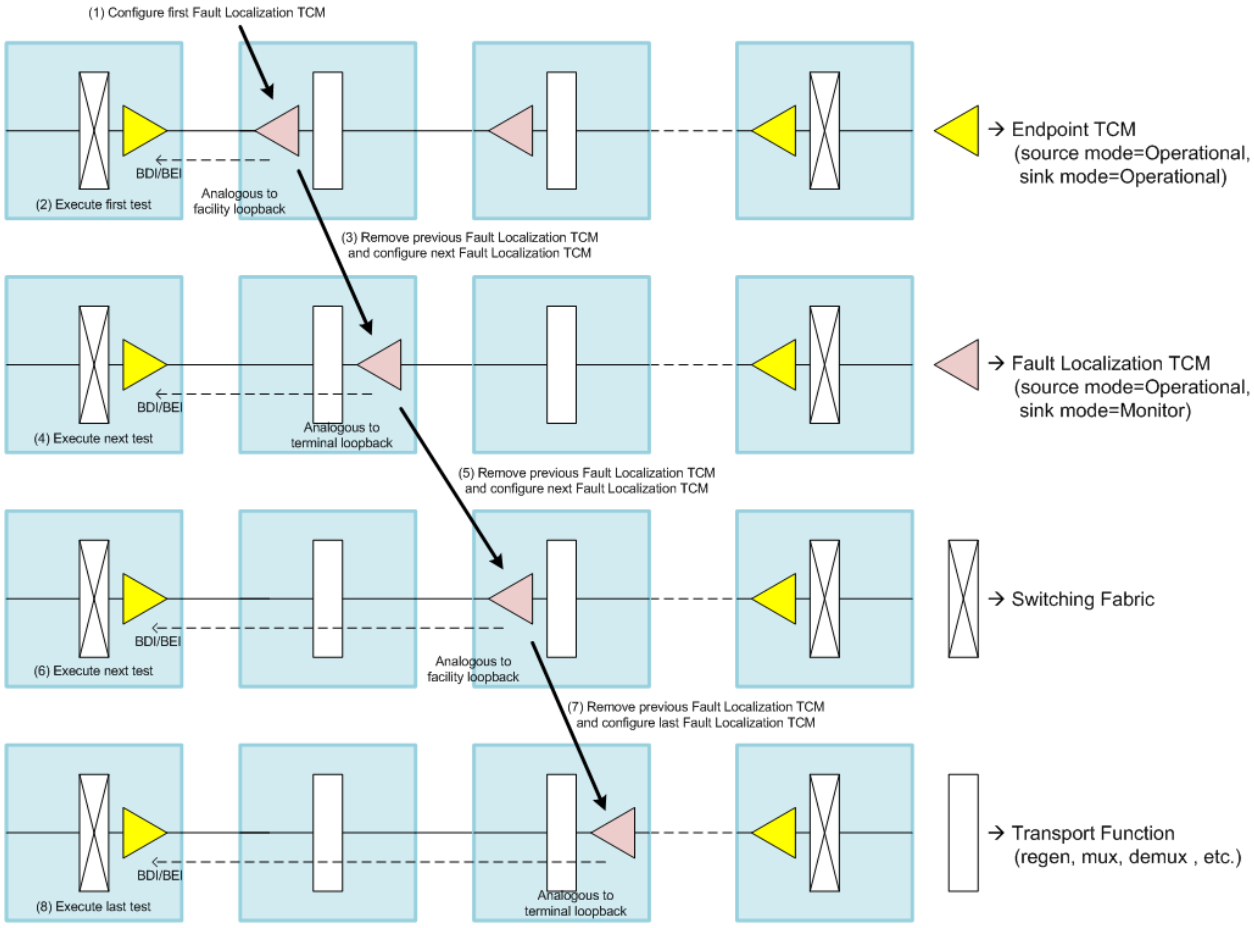

Figure 15: Bidirectional Fault Localization Process of a Link Using Monitor Mode TCMs

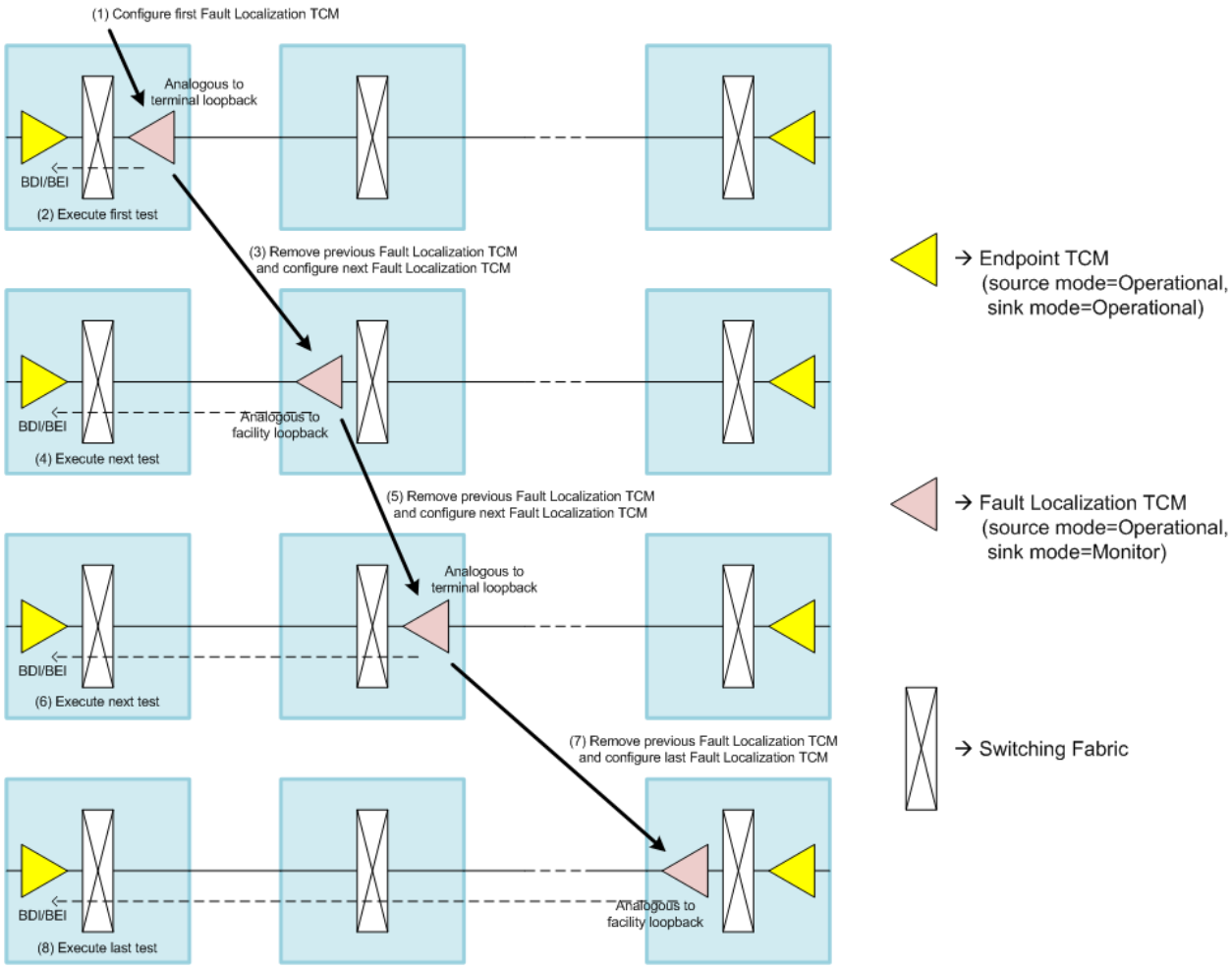

Figure 16: Bidirectional Fault Localization Process of an Administrative Domain Connection Using Monitor Mode TCMs

5 Configurations Not Covered by This Whitepaper

The intentions of this white paper are to present a recommended set of guidelines for TCM utilization and the assignment of default TCM levels to cover the majority of application configurations required by network providers. It is expected that for a majority of configurations the default usage of TCM levels will be sufficient and provide service providers and equipment vendors with a common understanding when setting default TCM levels. However, not all possible network configurations may be addressed in this document. Configurations that are not addressed are candidates for future study.

The following are some examples where the default TCM modes defined above may not be applicable (note that this list is not intended to be exhaustive and may be expanded in the future):

(1) "Shadow" TCM assigned mode as described in Section 3.2 Table 1: In this mode the TCM termination does not reset the TCM overhead bytes at the destination end of the TCM (i.e.

the TCM shadow data continues to propagate and is monitored further downstream). This is useful, in the case where an end-to-end service provider needs access to all the TCM data at the various monitoring points within the network, e.g., in an undersea network configuration. In general this is not a desirable mode of operation because it ends up using up the TCM levels quickly (i.e. the TCM levels can no longer be concatenated), but for specific systems this may be necessary.

(2) Two or more nested operator domains within a service provider's network: Since TCM level 4 is the suggested end-to-end domain operation, TCM4 of a nested domain could be overwritten.

For these, and other similar cases, manual TCM configuration is required by means of negotiation of TCM usage between the multiple carriers and vendors.

6 Control Plane Impacts of TCM

The application of control plane to the control of TCM configuration and modification is for further study.

7 Security

As TCM introduces new capabilities into the transport network, it is appropriate to consider whether any new security risks are introduced. TCM is a part of the OTN header information. It should be noted that TCM is not used as a control channel for exchange of signaling messages, as is provided by the GCC fields in OTN. As shown in Figure 2, TCM consists of a set of subfields with specific purposes, similar to other header fields such as frame alignment, APS, etc.

Interference with TCM requires direct access to the bit-stream or access to TCM control via the management interface into the network element. The potential impacts of tampering or misconfiguration of TCM include:

- Inadvertent or improper failing of a connection (or masking of failure)
- Inadvertent or improper failure action such as protection switching (or prevention of such action)
- Incorrect fault localization or attribution

It should be noted that tampering with TCM would not by itself introduce the potential for misrouting of data to a different destination than intended. TCM does not introduce new vulnerability to threats, as access to the bit stream and management interface are existing threats. Securing of the management interface is a general problem that is addressed by OIF Implementation Agreements [OIF SMI-03.0].