МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т G.808.1

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2006)

СЕРИЯ G: СИСТЕМЫ И СРЕДА ПЕРЕДАЧИ,
ЦИФРОВЫЕ СИСТЕМЫ И СЕТИ

Цифровые сети – Общие положения

Обобщенная защитная коммутация – Линейная защита канала и подсети

Рекомендация МСЭ-Т G.808.1

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ G

СИСТЕМЫ И СРЕДА ПЕРЕДАЧИ, ЦИФРОВЫЕ СИСТЕМЫ И СЕТИ

МЕЖДУНАРОДНЫЕ ТЕЛЕФОННЫЕ СОЕДИНЕНИЯ И ЦЕПИ	G.100–G.199
ОСНОВНЫЕ ХАРАКТЕРИСТИКИ, ОБЩИЕ ДЛЯ ВСЕХ АНАЛОГОВЫХ СИСТЕМ ПЕРЕДАЧИ	G.200–G.299
ИНДИВИДУАЛЬНЫЕ ХАРАКТЕРИСТИКИ МЕЖДУНАРОДНЫХ ВЧ-СИСТЕМ ТЕЛЕФОННОЙ СВЯЗИ ПО МЕТАЛЛИЧЕСКИМ ЛИНИЯМ	G.300–G.399
ОБЩИЕ ХАРАКТЕРИСТИКИ МЕЖДУНАРОДНЫХ СИСТЕМ ТЕЛЕФОННОЙ СВЯЗИ НА ОСНОВЕ РАДИОРЕЛЕЙНЫХ ИЛИ СПУТНИКОВЫХ ЛИНИЙ И ИХ СОЕДИНЕНИЕ С МЕТАЛЛИЧЕСКИМИ ПРОВОДНЫМИ ЛИНИЯМИ	G.400–G.449
КООРДИНАЦИЯ РАДИОТЕЛЕФОНИИ И ПРОВОДНОЙ ТЕЛЕФОНИИ	G.450–G.499
ХАРАКТЕРИСТИКИ СРЕДЫ ПЕРЕДАЧИ	G.600–G.699
ЦИФРОВОЕ ОКОНЕЧНОЕ ОБОРУДОВАНИЕ	G.700–G.799
ЦИФРОВЫЕ СЕТИ	G.800–G.899
Общие положения	**G.800–G.809**
Проектные нормы для цифровых сетей	G.810–G.819
Цели качества и готовности	G.820–G.829
Сетевые возможности и функции	G.830–G.839
Характеристики сетей СЦИ	G.840–G.849
Управление транспортной сетью	G.850–G.859
Интеграция радио- и спутниковых систем СЦИ	G.860–G.869
Оптические транспортные сети	G.870–G.879
ЦИФРОВЫЕ УЧАСТКИ И СИСТЕМА ЦИФРОВЫХ ЛИНИЙ	G.900–G.999
КАЧЕСТВО ОБСЛУЖИВАНИЯ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ – ОБЩИЕ И СВЯЗАННЫЕ С ПОЛЬЗОВАТЕЛЕМ АСПЕКТЫ	G.1000–G.1999
ХАРАКТЕРИСТИКИ СРЕДЫ ПЕРЕДАЧИ	G.6000–G.6999
ПЕРЕДАЧА ДАННЫХ ПО ТРАНСПОРТНЫМ СЕТЯМ – ОБЩИЕ ПОЛОЖЕНИЯ	G.7000–G.7999
ETHERNET И АСПЕКТЫ ТРАНСПОРТИРОВКИ СООБЩЕНИЙ	G.8000–G.8999
СЕТИ ДОСТУПА	G.9000–G.9999

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т G.808.1

Обобщенная защитная коммутация – Линейная защита канала и подсети

Резюме

Настоящая Рекомендация определяет обобщенные функциональные модели, характеристики и процессы, связанные с различными схемами линейной защиты для сетей уровня, ориентированного на соединения; например, оптических транспортных сетей (OTN), сетей синхронной цифровой иерархии (СЦИ) и сетей асинхронного способа передачи (ATM).

В ней определяются также цели и прикладные программы для таких схем. Схемы защиты, описанные в настоящей Рекомендации, это защита канала и защита соединений подсети с различными вариантами контроля для отдельных сигналов или групп сигналов. Кроме того, описывается живучесть сети, обеспечиваемая схемой регулирования пропускной способности линии (LCAS).

Обобщенные функциональные модели, характеристики и процессы для кольцевой защиты и схем защиты межсоединений подсети (например, кольцевой) определены в других Рекомендациях.

Источник

Рекомендация МСЭ-Т G.808.1 утверждена 29 марта 2006 года 15-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т G.808.1

Обобщенная защитная коммутация – Линейная защита канала и подсети

1 Сфера применения

В настоящей Рекомендации дается обзор общих аспектов линейной защитной коммутации. Она охватывает схемы защиты, основанные на соединениях OTN, СЦИ и ATM. Обзоры схем межсоединений кольцевой защиты и подсети с двойным узлом (например, кольцевой) будут даны в других Рекомендациях.

2 Ссылки

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

– ITU-T Recommendation G.783 (2006), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*.

– Рекомендация МСЭ-Т G.798 (2004 г.), *Характеристики функциональных блоков иерархического оборудования оптической транспортной сети.*

– ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

– ITU-T Recommendation G.841 (1998), *Types and characteristics of SDH network protection architectures*.

– ITU-T Recommendation G.842 (1997), *Interworking of SDH network protection architectures*.

– ITU-T Recommendation G.873.1 (2006), *Optical Transport Network (OTN): Linear protection*.

– ITU-T Recommendation I.630 (1999), *ATM protection switching*.

– ITU-T Recommendation I.732 (2000), *Functional characteristics of ATM equipment*.

– ITU-T Recommendation M.495 (1988), *Transmission restoration and transmission route diversity: Terminology and general principles*.

3 Термины и определения

3.1 В настоящей Рекомендации используются следующие термины:

– A: Обозначение конечной точки, используемое при описании защищаемой области; A – конечная точка источника защищаемых сигналов, для которой сигналы запроса на переключение инициируются в другой конечной точке Z.

– Z: Обозначение конечной точки, используемое при описании защищаемой области; Z – конечная точка, в которой инициируются сигналы запроса на переключение.

3.2 В настоящей Рекомендации используются следующие термины, определенные в Рекомендации МСЭ-Т G.805:

a) Адаптированная информация (AI).

b) Характеристическая информация (CI).

c) Подключение линии.

d) Сеть.

e) Последовательное подключение составной линии.

f) Подсеть.

g) Канал.

3.3 В настоящей Рекомендации используются следующие термины, встретившиеся в Рекомендации МСЭ-Т G.870/Y.1352:

3.3.1 Действие

3.3.1.1 коммутация: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.2 Протокол APS

3.3.2.1 1-этапный: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.2.2 2-этапный: **См. Рекомендацию МСЭ-Т G.870/Y.1352.**

3.3.2.3 3-этапный: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.3 Класс защиты

3.3.3.1 защита канала: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.3.2 защита подключения подсети: **См. Рекомендацию МСЭ-Т G.870/Y.1352**.

Определение условия отказа на последовательном подключении составной линии в пределах защищаемой области выполняется следующим образом:

3.3.3.2.1 контроль подуровня (/S): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.3.2.2 ненарушающий контроль (/N): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.3.2.3 внутренний контроль (/I): См. Рекомендацию МСЭ-Т G.870/Y.1352

3.3.3.2.4 проверочный контроль (/T): См. Рекомендацию МСЭ-Т G.870/Y.1352

3.3.3.3 защита сетевого подключения: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.3.4 индивидуальная: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.3.5 групповая: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.4 Подкласс защиты

3.3.4.1 сквозные служебные/OAM(e) сигналы: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.4.2 служебные/OAM(s) сигналы подуровня: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5 Компонент

3.3.5.1 защищаемая область: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.2 мост: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.2.1 постоянный мост: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.2.2 широковещательный мост: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.2.3 селекторный мост: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.3 селектор: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.3.1 выборочный селектор: См. Рекомендацию МСЭ-Т G.870/Y.1352

3.3.5.3.2 объединяющий селектор: См. Рекомендацию МСЭ-Т G.870/Y.1352.

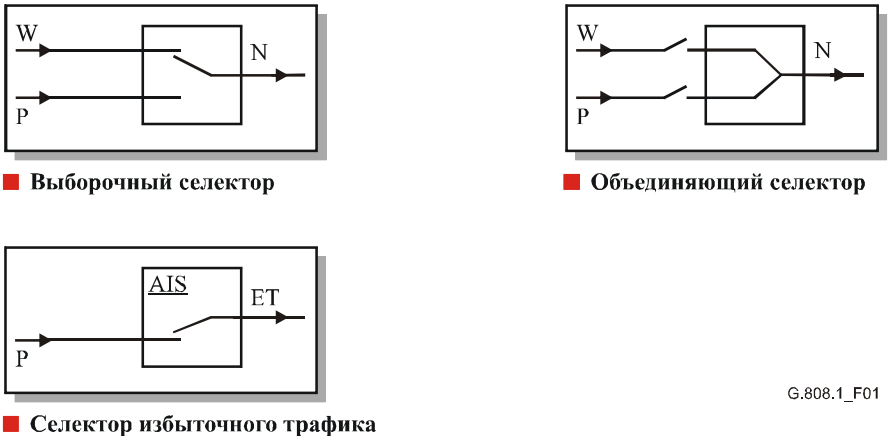


Рисунок 1/G.808.1 – Защитные селекторы

3.3.5.4 головной конец: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.5 хвостовой конец: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.6 узел приемника: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.7 узел источника: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.5.8 промежуточный узел: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.6 Условие отказа

3.3.6.1 сигнал ухудшения (SD): См. Рекомендацию МСЭ-Т G.805.

3.3.6.2 сигнал сбоя (SF): См. Рекомендацию МСЭ-Т G.805.

3.3.6.3 сигнал ухудшения группы (SDG): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.6.4 сигнал сбоя группы (SFG): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.6.5 сигнал ухудшения сервера (SSD): См. Рекомендацию МСЭ-Т G.806.

3.3.6.6 сигнал сбоя сервера (SSF): См. Рекомендацию МСЭ-Т G.806.

3.3.6.7 сигнал ухудшения в канале (TSD): См. Рекомендацию МСЭ-Т G.806.

3.3.6.8 сигнал сбоя в канале (TSF): См. Рекомендацию МСЭ-Т G.806.

3.3.7 Архитектура

3.3.7.1 (защитная) архитектура 1+1: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.7.2 (защитная) архитектура 1:n (n ≥ 1): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.7.3 (защитная) архитектура m:n: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.7.4 защитная архитектура $(1:1)^n$: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8 Внешние команды

3.3.8.1 блокировка защитного транспортного объекта № i (LO #i): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.2 блокировка сигнала нормального трафика № i: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.3 отмена блокировки сигнала нормального трафика № i: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.4 фиксация: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.5 принудительное переключение сигнала нормального трафика № i (FS #i): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.6 принудительное переключение нулевого сигнала (FS #0): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.7 принудительное переключение сигнала избыточного трафика FS #ExtraTrafficSignalNumber): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.8 ручное переключение сигнала нормального трафика № i (MS #i): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.9 ручное переключение нулевого сигнала (MS #0): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.10 ручное переключение сигнала избыточного трафика (MS #ExtraTrafficSignalNumber): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.11 сигнал исполнения № i (EX): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.8.12 отмена (CLR): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.9 Состояния

3.3.9.1 сигнал нормального трафика № i не реверсируется (DNR #i): См. Рекомендацию МСЭ-Т G.870/Y.1352

3.3.9.2 отсутствие запроса (NR): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.9.3 ожидание восстановления сигнала нормального трафика № i (WtR): См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.10 Срабатывание

3.3.10.1 реверсивное (защитное) срабатывание: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.10.2 нереверсивное (защитное) срабатывание: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.11 Сигнал

3.3.11.1 сигнал трафика: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.11.2 сигнал нормального трафика: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.11.3 сигнал избыточного трафика: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.11.4 нулевой сигнал: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.12 Коммутация

3.3.12.1 двунаправленная (защитная) коммутация: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.12.2 однонаправленная (защитная) коммутация: См. Рекомендацию МСЭ-Т G.870/Y.1352.

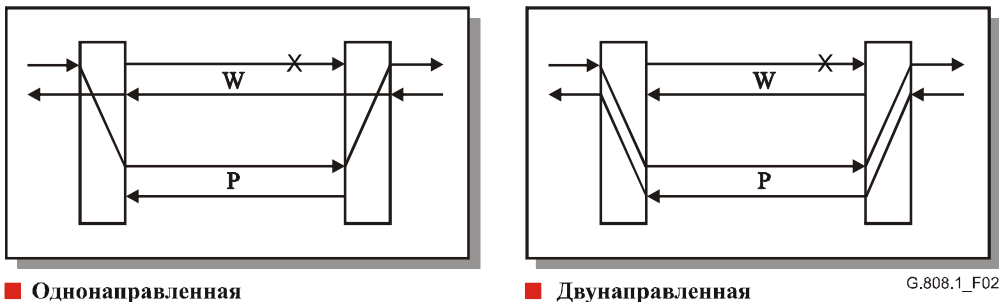


Рисунок 2/G.808.1 – Типы коммутации

3.3.13 Время

3.3.13.1 время обнаружения: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.13.2 время удержания: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.13.3 время ожидания восстановления: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.13.4 время коммутации: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.14 Транспортный объект

3.3.14.1 транспортный объект: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.14.2 защита транспортного объекта: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.14.3 защитный транспортный объект: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.14.4 рабочий транспортный объект: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.14.5 активный транспортный объект: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.14.6 резервный транспортный объект: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.14.7 группа: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.15 защита: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.16 восстановление: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.17 повышение: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.18 бесконтактная защитная коммутация: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.19 неисправность: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.20 живучесть сети: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.21 коэффициент защиты: См. Рекомендацию МСЭ-Т G.870/Y.1352.

3.3.22 взаимодействие подсетей: См. Рекомендацию МСЭ-Т G.870/Y.1352

3.3.23 жизнеспособная сеть: См. Рекомендацию МСЭ-Т G.780/Y.1351.

3.3.24 событие переключения: См. Рекомендацию МСЭ-Т G.870/Y.1352.

4 Сокращения

В настоящей Рекомендации используются следующие сокращения:

ABR	Передача доступной скоростью
AI	Адаптированная информация
AIS	Сигнал индикации аварийного состояния
AP	Точка доступа
APS	Автоматическая защитная коммутация
ATM	Асинхронный способ передачи
AU	Административный блок
B	Полоса пропускания
КОБ	Коэффициент ошибок по битам
BR	Мост
CC	Контроль непрерывности
CI	Характеристическая информация
CP	Точка подключения
DEG	Ухудшенный
ET	(Сигнал) избыточного трафика
F4	Поток № 4 (ATM)

FDI	Прямая индикация неисправности
HO	Удержание
IMG	Инверсная мультиплексированная группа
LCAS	Схема регулирования пропускной способности линии
MPLS	Многопротокольная коммутация с использованием меток
MS	Составной участок
N	Нормальный (сигнал)
NE	Элемент сети
NIM	Ненарушающий контроль
NR	Отсутствие запроса
NUT	Непрерываемый незащищенный трафик
OAM	Эксплуатация, административное управление и техническое обслуживание
OCh	Оптический канал
OH	Служебные сигналы
OTN	Оптическая транспортная сеть
P	Защита
PDH	Плезиохронная цифровая иерархия
POH	Служебные сигналы маршрута
PP	Обработка указателя
PU	Блок порта
RDI	Дистанционная индикация неисправности
REI	Дистанционная индикация ошибки
RI	Дистанционная информация
RS	Участок регенератора
SD	Сигнал ухудшения
SDG	Сигнал ухудшения группы
СЦИ	Синхронная цифровая иерархия
SEL	Селектор
SES	Секунда, пораженная ошибками
SF	Сигнал сбоя
SFG	Сигнал сбоя группы
SIM	Живучесть подключений инверсных мультиплексированных линий
Sm	низший порядок уровня VC-m (n = 11, 12, 2)
Sn	высший порядок уровня VC-n (n = 3, 4, 4-Xc), или низший порядок уровня VC-3
SNC	Подключение подсети
SNC/I	Защита подключения подсети с внутренним контролем
SNC/N	Защита подключения подсети с ненарушающим контролем
SNC/Ne	SNC/N, контроль сквозных OH
SNC/Ns	SNC/N, контроль OH подуровня

SNC/S SNCP с контролем подуровня

SNC/Ss SNC/N, контроль OH подуровня

SNC/T SNCP с контролем испытательного канала

SNC/Te SNC/T, контроль сквозных OH

SNC/Ts SNC/T, контроль OH подуровня

SNCP Защита подключения подсети

Sn-Xv Уровень VC-n-Xv

SOH Служебный сигнал на участке

SSD Ухудшение сигнала сервера

SSF Сбой сигнала сервера

STM-N Синхронный транспортный модуль, уровень N

TCP Точка завершения подключения

TSD Сигнал ухудшения канала

TSF Сигнал сбоя канала

TSI Обмен временными слотами

TT Завершение канала

TU Компонентный блок

UBR Передача с незаданной скоростью

UPSR Однонаправленное кольцо переключения маршрута

VC Виртуальный канал (ATM)

VCG Виртуальная группа сцепления

VC-n Виртуальный контейнер-n

VC-n-Xv Виртуальное сцепление X виртуальных контейнеров (уровня n)

VP Виртуальный маршрут (ATM)

VPI Идентификатор виртуального маршрута

W Рабочий

WTR Ожидание восстановления

X, Y, Z Обозначение размера уровня (для необозначенных уровней) или группы

5 Условные обозначения

Не используются.

6 Концепция индивидуальной и групповой защиты

Концепция индивидуальной защиты применяется к ситуациям, когда полезно защитить только часть сигналов трафика, которая требует высокой надежности. Остальная часть сигналов трафика на сетевом уровне остается незащищенной. Это помогает уменьшить необходимую полосу пропускания в целях защиты.

Концепция групповой защиты применяется к ситуациям, когда:

i) полезно защитить большое количество (но не все) сигналов трафика, транспортируемых по одним и тем же каналам уровня сервера, с интервалами времени защиты того же порядка, что и для индивидуальной защиты (небольшого набора сигналов трафика). Быстрое защитное переключение достигается обработкой логической группы транспортных объектов как единого объекта после начала защитных операций;

ii) защита группы сигналов трафика, при которой создается единый сигнал трафика, например путем виртуального сцепления, инверсного мультиплексирования.

Сложность процесса защиты уменьшается за счет обработки группы сигналов как единого объекта в рамках единого процесса защиты. Статус рабочих и защитных групп представлен индикацией SF-группы и SD-группы.

Сложность можно далее уменьшить за счет введения дополнительного испытательного сигнала (транспортируемого по тем же каналам уровня сервера), индикация SF и SD которого используется для указания статуса группы. *Недостатком* этого последнего способа уменьшения сложности является невозможность контроля связности, непрерывности и качества отдельных сигналов в каждой группе. Один из отказов по этим параметрам одного из сигналов группы может быть не обнаружен, и таким образом не будет обеспечена защита.

7 Типы архитектуры

Защитная архитектура может быть следующих типов: 1+1, 1:n, m:n или $(1:1)^n$.

Возможные достоинства архитектуры типа 1+1:

1) небольшая сложность;

2) для случая однонаправленной коммутации возможность поддержки двухузлового подключения защищаемых подсетей.

Возможные недостатки архитектуры типа 1+1:

3) 100% избыточная пропускная способность.

Возможные достоинства архитектур типов 1:n, m:n, $(1:1)^n$:

1) возможность обеспечения доступа к защите; защитный транспортный объект/полоса пропускания могут передавать сигнал избыточного трафика в течение периодов, когда этот объект/полоса пропускания не требуется для передачи сигнала нормального трафика;

2) дополнительная пропускная способность, ограниченная величиной 100/n % или m × 100/n %;

3) для случая m:n защита возможна для m отказов.

Возможные недостатки архитектуры 1:n, m:n, $(1:1)^n$:

4) сложность;

5) для случая класса защиты SNC потребность в дополнительных функциях завершения подуровня в точках входа и выхода защищаемой области на каждом рабочем и защитном транспортном объекте;

6) не поддерживается межсетевое взаимодействие защищаемых подсетей с двумя узлами;

7) $n \geq 2$: маршрутизация каждого из n рабочих транспортных объектов должна производиться через различные средства и оборудование, чтобы предотвратить наличие общих точек отказа, которые нельзя защитить одиночным защитным транспортным объектом в архитектуре 1:n и $(1:1)^n$.

ПРИМЕЧАНИЕ 1. – Как правило, n+1 альтернативных маршрутов между двумя узлами в сети будут недоступны. Как таковые архитектуры 1:n и $(1:1)^n$, при $n \geq 2$, *не будут обеспечивать адекватной защиты* для n сигналов нормального трафика, передаваемых обычно через n рабочих транспортных объектов. Значение n = 1 представляется единственным разумным выбором.

ПРИМЕЧАНИЕ 2. – В сетях ATM доступ к защите в явном виде не требуется для обеспечения использования обычно неиспользуемой защитной полосы пропускания; трафик ABR и UBR мог бы использовать эту полосу пропускания сверх абонированной ширины полосы сигнала сервера, содержащего защитный транспортный объект. Предполагается, что механизм управления более высокого уровня ABR/UBR уменьшит трафик, когда защита фактически используется. Узлы входа/выхода области защиты не должны совмещаться с узлами входа/выхода трафика ABR/UBR. Это добавляет сети гибкости и уменьшает ее сложность.

7.1 Защитная архитектура 1+1

В архитектуре типа 1+1 защитный транспортный объект назначается резервным средством для рабочего транспортного объекта с сигналом нормального трафика, подключенным к защитному транспортному объекту в конечной точке источника защищаемой области. Нормальный трафик рабочего и защитного транспортного объектов передается одновременно к конечной точке приема защищаемой области, где производится выбор между рабочим и защитным транспортным объектами на основе ряда заранее определенных критериев, таких как индикация сигнала сбоя и сигнала ухудшения. См. рисунок 3.

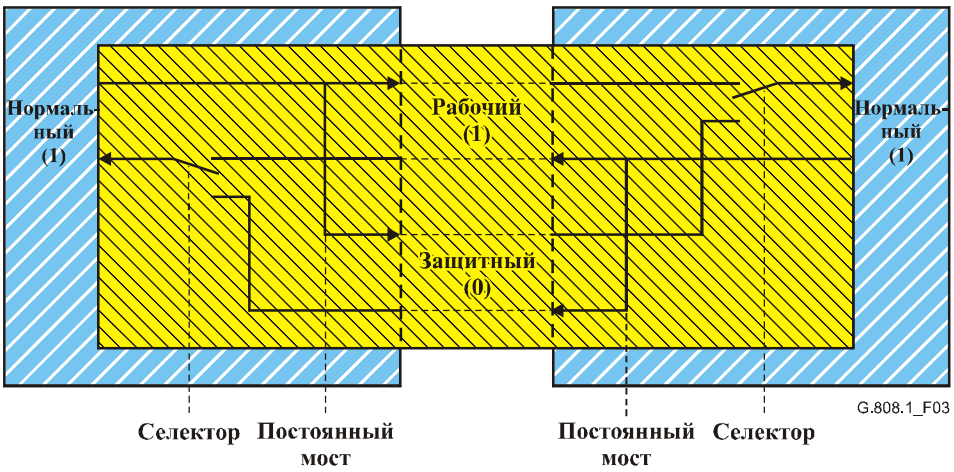


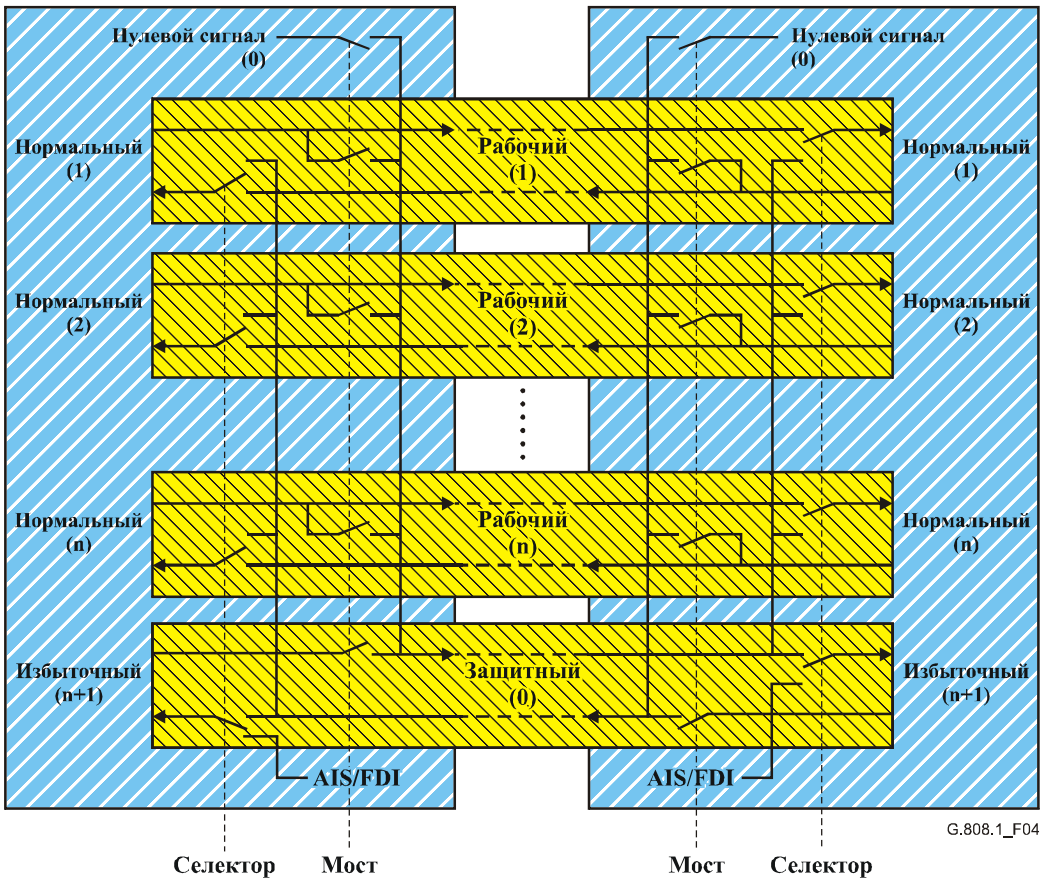
Рисунок 3/G.808.1 – Защитная архитектура 1+1

7.2 Защитная архитектура 1:n

В архитектуре типа 1:n выделенный защитный транспортный объект – это совместно используемое резервное средство для n рабочих транспортных объектов. Полоса пропускания защитного транспортного объекта должна быть распределена так, чтобы можно было защитить любой из n рабочих транспортных объектов в случае, если доступен защитный транспортный объект.

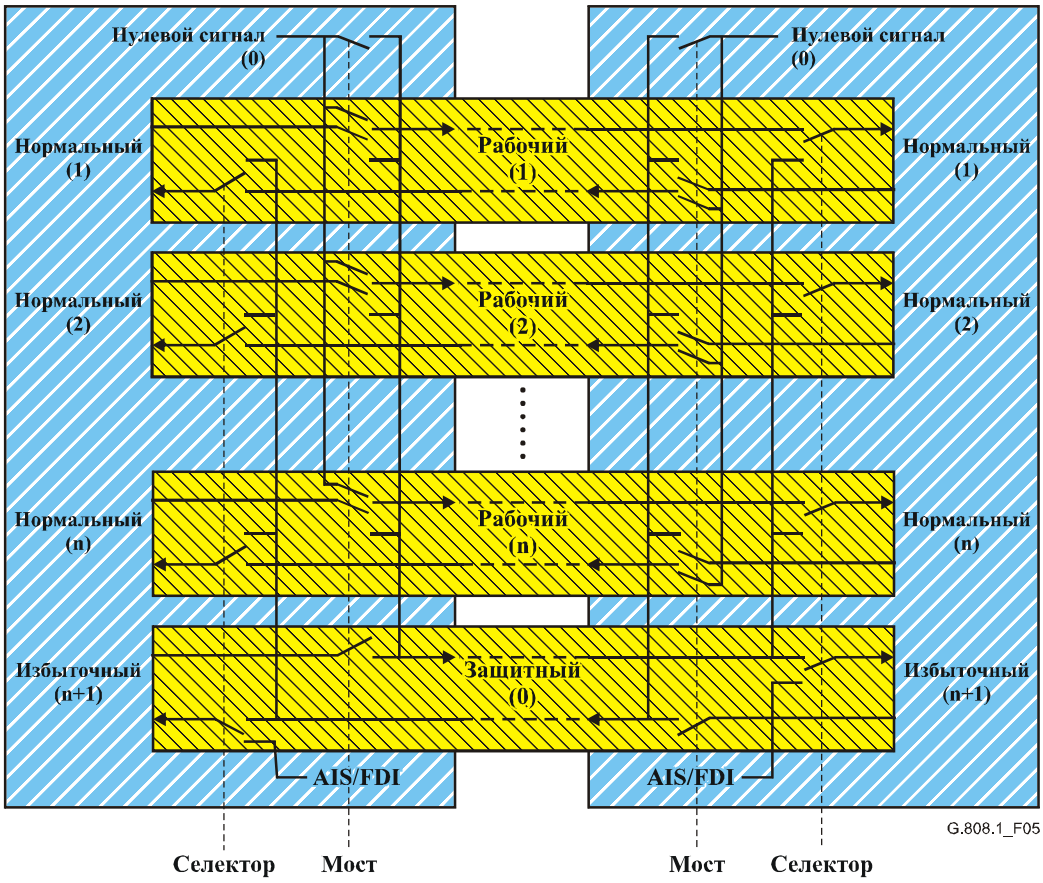
Когда обнаружено, что рабочий транспортный объект поврежден, его сигнал нормального трафика должен быть передан от рабочего к защитному транспортному объекту в конечных точках как источника, так и приема защищаемой области. Отметим, что когда повреждено более одного рабочего транспортного объекта, может быть защищен только один сигнал нормального трафика.

Мост можно реализовать двумя способами: селекторный мост или широковещательный мост. При связи через селекторный мост (рисунок 5) сигнал нормального трафика подключается либо к рабочему транспортному объекту, либо к защитному транспортному объекту. При связи через широковещательный мост (рисунок 4) сигнал нормального трафика постоянно подключен к рабочему транспортному объекту, а иногда также к защитному транспортному объекту. Гарантируется совместная работа этих двух вариантов.



Вариант широковещательного моста: обычно постоянно подключен к рабочему объекту, а иногда – к защитному.

Рисунок 4/G.808.1 – Защитная архитектура 1:n

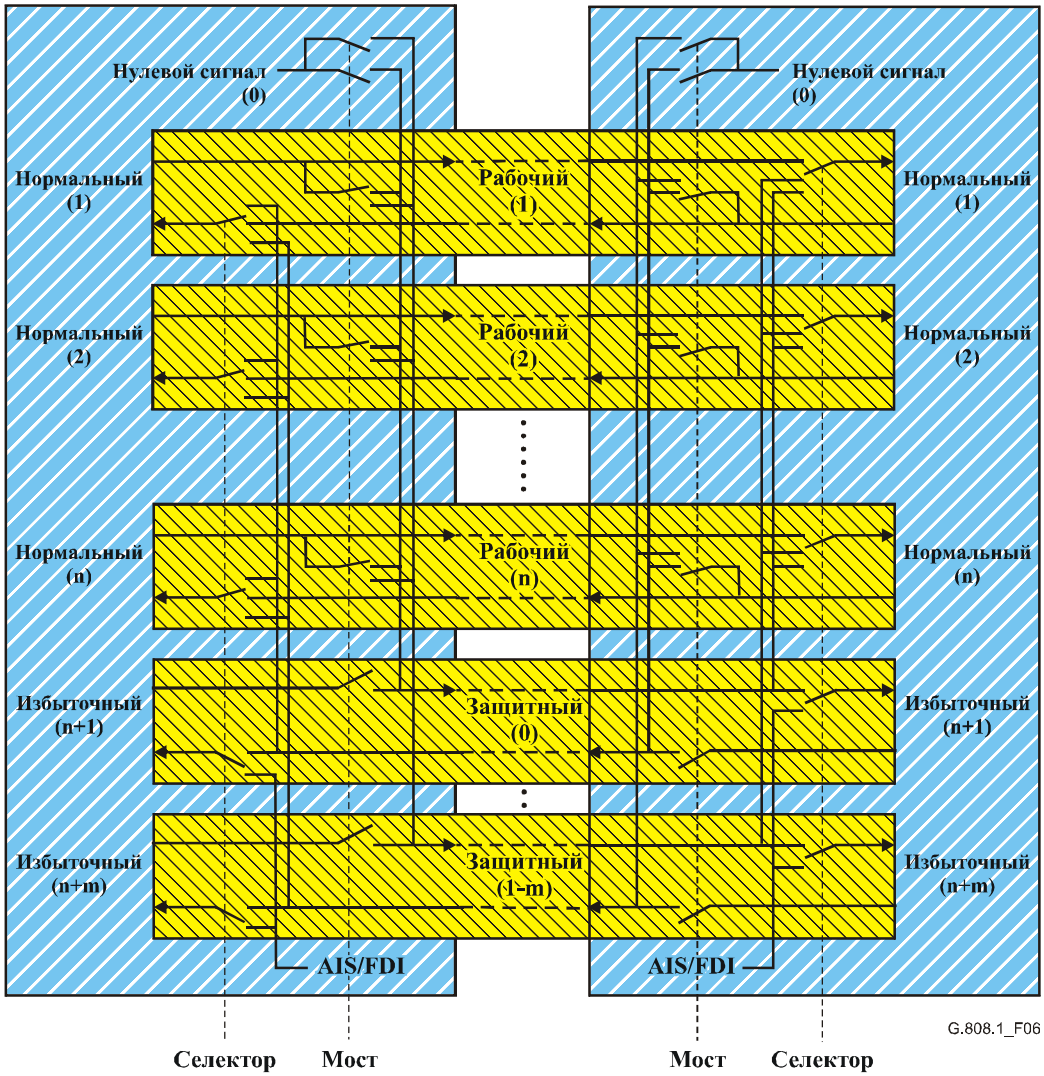


Вариант селекторного моста: обычно постоянно подключен к рабочему или защитному объекту.

Рисунок 5/G.808.1 – Защитная архитектура 1:n

7.3 Защитная архитектура m:n

В архитектуре типа m:n m выделенных защитных транспортных объектов совместно используют резервные средства для n рабочих транспортных объектов, где обычно $m \leq n$. Полоса пропускания каждого защитного транспортного объекта должна быть распределена так, чтобы можно было защитить любой из n рабочих транспортных объектов в случае, если доступен по крайней мере один из m защитных транспортных объектов. Когда обнаружено, что рабочий транспортный объект поврежден, его сигнал нормального трафика сначала должен быть передан доступному защитному транспортному объекту, затем должен быть произведен переход от рабочего к выделенному защитному транспортному объекту в конечных точках как источника, так и приема защищаемой области. Отметим, что когда повреждено более чем m рабочих транспортных объектов, могут быть защищены только m рабочих транспортных объектов. См. рисунок 6.

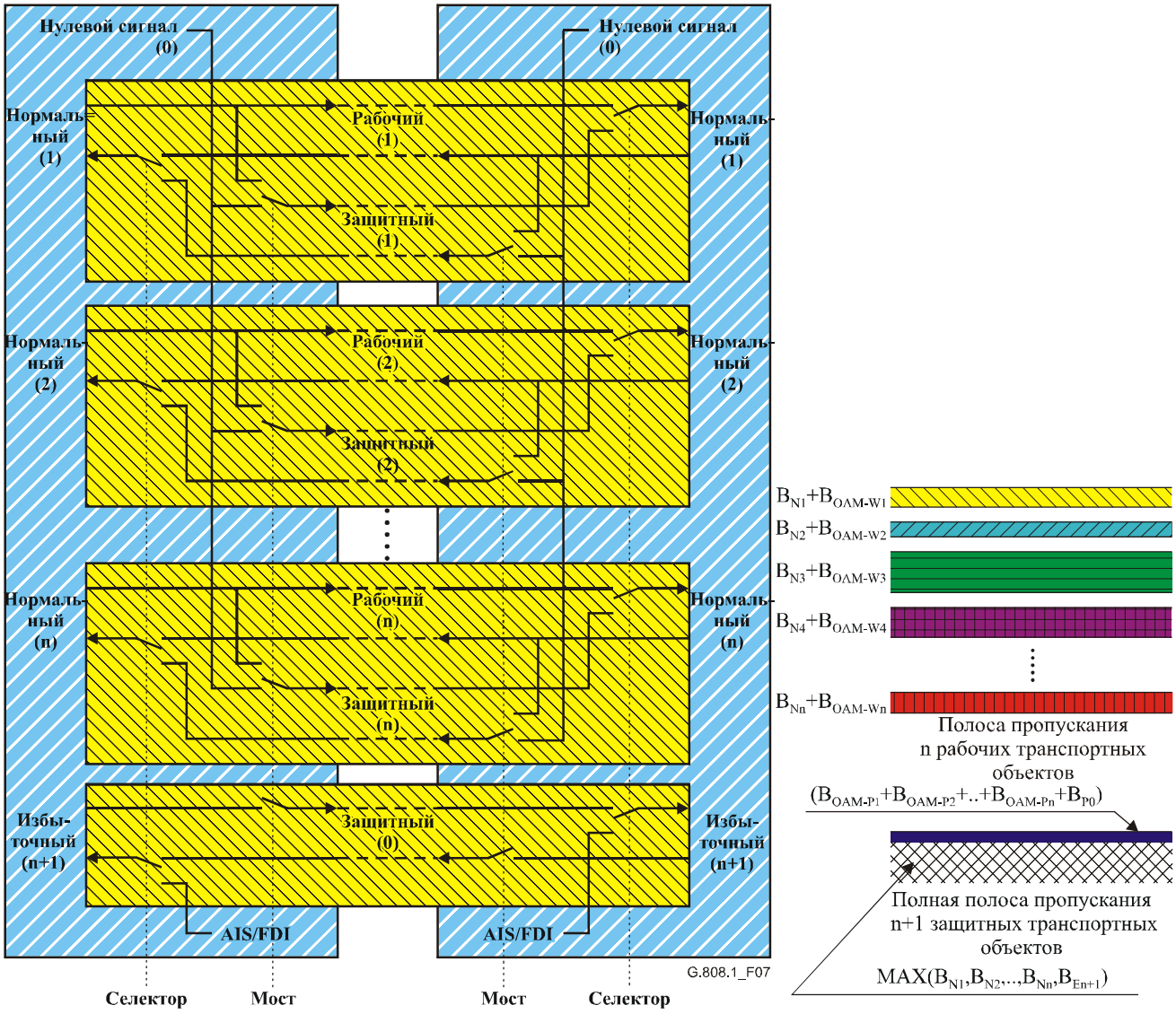


Вариант широковещательного моста: обычно постоянно подключен к рабочему объекту, а иногда – к защитному.

Рисунок 6/G.808.1 – Защитная архитектура m:n

7.4 Защитная архитектура $(1:1)^n$

В защитной архитектуре типа $(1:1)^n$ n выделенных защитных транспортных объектов, совместно использующих одну и ту же полосу пропускания, являются резервными средствами для n рабочих транспортных объектов. Защитная полоса пропускания должна быть распределена так, чтобы можно было защитить любой из n рабочих транспортных объектов в случае, если доступны защитная транспортная полоса и конкретный защитный транспортный объект, связанный с переключаемым рабочим транспортным объектом. Когда обнаружено, что рабочий транспортный объект поврежден, его сигнал нормального трафика сначала должен быть передан доступному связанному защитному транспортному объекту, затем должен быть произведен переход от рабочего к выделенному защитному транспортному объекту в конечных точках как источника, так и приема защищаемой области. Отметим, что когда повреждено более одного рабочего транспортного объекта, может быть защищен только один рабочий транспортный объект. См. рисунок 7.



Вариант широковещательного моста: обычно постоянно подключен к рабочему объекту, а иногда – к защитному.

Рисунок 7/G.808.1 –Защитная архитектура $(1:1)^n$ при совместном использовании полосы пропускания

Маршрутизация всех "n" рабочих транспортных объектов производится через различные средства и аппаратуру (чтобы не допустить наличия общей точки отказа, которую нельзя защитить). Маршрутизация всех "n+1" защитных транспортных объектов производится через одни и те же средства и аппаратуру, отличные от рабочих средств и аппаратуры. За примером следует обратиться к Добавлению IV.

Ширина полосы пропускания, занимаемая каждым рабочим транспортным объектом: $B_{Wi} = B_{Ni}+B_{OAM\text{-}Wi}$; т. е. ширина полосы для сигнала № i нормального трафика плюс ширина полосы для тандемного подключения/сегмента OAM, используемая для контроля рабочего транспортного объекта № i. Ширина полосы пропускания, занятая защитными транспортными объектами: $Bp = MAX(B_{N1},B_{N2},..,B_{Nn},B_{En+1}) + (B_{OAM\text{-}P1}+B_{OAM\text{-}P2}+..+ B_{OAM\text{-}Pn}+B_{OAM\text{-}P0})$. С точки зрения использования полосы пропускания эта защитная архитектура $(1:1)^n$ ведет себя как архитектура 1:n.

Не может произойти неправильного подключения сигнала №i нормального трафика на входе защищаемой области к выходу сигнала № j ($j \neq i$) нормального трафика на выходе защищаемой области. 3-этапный протокол APS как таковой не требуется.

Отметим, что эта архитектура предназначена для трафика, основанного на передаче пакетов/ячеек, а не для трафика с постоянной скоростью передачи битов.

8 Типы коммутации

Защитная коммутация может быть однонаправленной или двунаправленной.

При **однонаправленной** коммутации действия по переключению заканчиваются, когда сигнал трафика (услуга) выбирается из резервного объекта на конце, где обнаружена ошибка. Для случая архитектуры 1+1 используется только селектор на конце приема (без связи с концом источника). Для случая архитектур 1:n, m:n, $(1:1)^n$ используются селектор на конце приема, а также мост на конце источника.

При **двунаправленной** коммутации сигнал (услуга) трафика переключается от активного к резервному транспортному объекту на обоих концах защищаемого участка. Для случая архитектуры 1+1 используются селекторы на концах приема и источника. Для случая архитектур 1:n, m:n, $(1:1)^n$ используются селекторы на концах приема и источника, а также мосты на концах источника и приема.

ПРИМЕЧАНИЕ 1. – Все типы коммутации, кроме однонаправленной коммутации 1+1, требуют наличия канала связи между двумя концами защищаемой области; он называется каналом автоматической защитной коммутации (APS). Канал APS заканчивается в функциях подключения на каждом конце защищаемой области.

Согласно двунаправленным протоколам коммутации, переключение (работающих селектора и моста) только на одном конце не допускается. Два конца соединяются, чтобы инициировать передачу сигнала нормального трафика. Если приоритет запроса конца источника ниже, чем приоритет конца приема, или отсутствует, то конец приема инициирует передачу сигнала нормального трафика, а конец источника отслеживает эту передачу.

Возможные преимущества коммутации однонаправленного типа:

1) Однонаправленная защитная коммутация – схема, простая в реализации, и не требует протокола в архитектуре 1+1.

   ПРИМЕЧАНИЕ 2. – Однонаправленная коммутация в архитектуре 1:n (обычно применяемой в линиях радио/спутниковой связи) требует протокола для работы между двумя конечными точками защищаемой области.

2) В архитектуре 1+1 однонаправленная защитная коммутация может производиться быстрее, чем двунаправленная защитная коммутация, поскольку она не требует протокола.

3) В условиях многочисленных отказов имеется большая вероятность восстановления трафика за счет защитной коммутации, если используется однонаправленная, а не двунаправленная защитная коммутация.

4) Однонаправленная коммутация позволяет обеспечить простую реализацию надежной сети с помощью каскадных защищенных подсетей. Две подсети подключаются с использованием следующего типа архитектуры: подключение с двойным узлом/двойная подсеть.

Возможные преимущества коммутации двунаправленного типа:

1) При двунаправленной защитной коммутации та же аппаратура используется для обоих направлений передачи после отказа. Это означает, что будет меньше перерывов в обслуживании для проведения ремонта и возврата к исходному рабочему маршруту. При однонаправленной коммутации производятся следующие виды переключений:

   i) защитное переключение;

   ii) вынужденное переключение для направления, не затронутого отказом;

   iii) реверсивное переключение.

   При двунаправленной коммутации производятся только два вида переключений:

   i) защитное переключение;

   ii) реверсивное переключение.

   В результате каждого переключения будут иметь место один или два секундных интервала, пораженных ошибками. Меньшее число SES появится в результате двунаправленной коммутации.

2) При двунаправленной защитной коммутации, если имеется отказ в одном транспортном объекте сети, то передача в обоих транспортных объектах между затронутыми узлами переключается на альтернативное направление по всей сети. При этом трафик не передается через неисправный участок сети, и таким образом его ремонт может выполняться без дополнительной защитной коммутации.

3) Двунаправленной защитной коммутацией легче управлять, поскольку в обоих направлениях передачи используется та же аппаратура по всей длине транспортного объекта.

4) При двунаправленной защитной коммутации поддерживаются одинаковые задержки для обоих направлений передачи. Это может быть важно, когда имеется значительный дисбаланс длины транспортных объектов, например, на трансокеанских линиях, где один транспортный объект использует спутниковую линию, а другой – кабельную линию.

5) При двунаправленной защитной коммутации имеется также возможность передачи избыточного трафика на защитный транспортный объект.

9 Типы срабатывания

Возможны следующие типы срабатывания защиты: нереверсивный и реверсивный.

При **реверсивном** срабатывании сигнал (услуга) трафика всегда возвращается на рабочий транспортный объект (или остается на нем), если запросы на коммутацию прекращаются. Это происходит, когда рабочий транспортный объект восстанавливается после сбоя или удаляется внешний запрос.

При **нереверсивном** срабатывании сигнал (услуга) трафика не возвращается на рабочий транспортный объект, если запросы на коммутацию прекращаются.

Некоторые защитные схемы реверсивны в принципе. Другие схемы допускают либо реверсивное, либо нереверсивное срабатывание. Достоинство нереверсивного срабатывания состоит в том, что обычно оно оказывает меньшее влияние на характеристики трафика. Примеры ситуаций, когда может быть уместным реверсивное срабатывание:

1) Когда можно использовать части защитного транспортного объекта, чтобы обеспечить пропускную способность для удовлетворения наиболее срочных потребностей. Например, когда защитный транспортный объект вывести из эксплуатации, чтобы высвободить пропускную способность для применения при восстановлении другого трафика.

2) Когда защитный транспортный объект подвергается частой перегруппировке. Например, когда сеть имеет ограниченную пропускную способность и защитные маршруты часто перераспределяются с целью достижения максимальной эффективности сети, если в ней возникают какие-либо изменения.

3) Когда защитный транспортный объект имеет значительно более низкие характеристики, чем рабочий транспортный объект. Например, когда защитный транспортный объект обладает худшей помехоустойчивостью или имеет более длительную задержку, чем рабочий транспортный объект.

4) Когда оператор должен знать, какие транспортные объекты передают нормальный трафик, чтобы упростить управление сетью.

10 Типы протоколов

За исключением однонаправленной коммутации 1+1, все типы защиты требуют, чтобы на обоих концах, A и Z, защищаемой области координировались операции использования мостов и выбора. В зависимости от типов защиты, селекторов и мостов требуются различные протоколы. Поэтому узлы A и Z связываются друг с другом через канал автоматической защитной коммутации (APS).

Существуют два основных требования к защитному протоколу:

1) Предотвращение неправильных подключений.

2) Сведение к минимуму числа циклов связи между концами A и Z защищаемой области, чтобы сократить до минимума время защитной коммутации. Связь может быть однократной (Z → A), двукратной (Z → A и A → Z), либо трехкратной (Z → A, A → Z и Z → A). Это называется 1-этапным, 2-этапным и 3-этапным протоколами.

Условия, при которых можно использовать различные типы протоколов, указаны в таблице 1.

Таблица 1/G.808.1 – Типы протоколов для различных типов защитной архитектуры и селектора/моста

Тип протокола	Типы защиты, использующей протокол	Тип моста	Тип селектора
Без протокола	Только однонаправленная 1+1	Постоянный	Выборочный
1-этапный	Только однонаправленная $(1:1)^n$	Селекторный	Выборочный или объединяющий
	Только архитектура 1+1	Постоянный	Выборочный
2-этапный	Только однонаправленная $(1:1)^n$	Селекторный	Выборочный или объединяющий
	Только архитектура 1+1	Постоянный	Выборочный
3-этапный	Все типы архитектуры	Любой	Выборочный
		Селекторный	Объединяющий (технологии, базирующиеся на передаче ячеек/пакетов)

Возможные достоинства протокола 3-этапного типа:

1) работает со всеми типами архитектуры;

2) предотвращает неправильные подключения, происходящие при любых обстоятельствах;

3) запускает селектор или мост только после подтверждения приоритета другим концом защищаемой области.

Возможные недостатки протокола 3-этапного типа:

4) необходим трехкратный обмен сообщениями между двумя концами защищаемой области, что увеличивает время коммутации.

Возможные достоинства протокола 2-этапного типа:

1) меньшее время коммутации по сравнению с 3-этапным протоколом;

2) работает только с архитектурой 1+1 и $(1:1)^n$.

Возможные достоинства протокола 1-этапного типа:

1) малое время коммутации из-за необходимости лишь однократного обмена сообщениями между двумя концами защищаемой области;

2) работает с архитектурой 1+1 и $(1:1)^n$.

Возможные недостатки протокола 1-этапного типа:

3) требует установки "n" дополнительных транспортных объектов (по сравнению с архитектурой 1:n) в защитной полосе пропускания, чтобы предотвратить неправильные подключения;

4) запускает мост/селектор до подтверждения приоритета другим концом защищаемой области. Как таковая операция коммутации может быть изменена на обратную или заменена другой операцией моста/селектора, инициируемой другим концом;

5) более сложный протокол, поскольку имеется "n" параллельных типов защиты 1:1.

11 Классы и подклассы защиты

11.1 Защита канала

Защита канала – класс защиты, используемый для защиты канала по всей сети оператора или по сетям нескольких операторов. Она предназначена для сквозной защитной архитектуры, которая может использоваться в различных структурах сети: ячеистой, кольцевой и т. д. Поскольку защита канала – это выделенный защитный механизм, то не существует фундаментальных ограничений на количество NE в пределах канала.

Защита канала работает со всеми сочетаниями типов защитных архитектур, коммутации и срабатывания.

В общем случае защита канала защищает от сбоев на уровне сервера, а также от ошибок связности и ухудшения характеристик на уровне клиента.

В случае использования защиты канала защищается адаптированная информация (AI) (т. е. полезная часть характеристической информации сетевого уровня (CI)). См. рисунок 8.

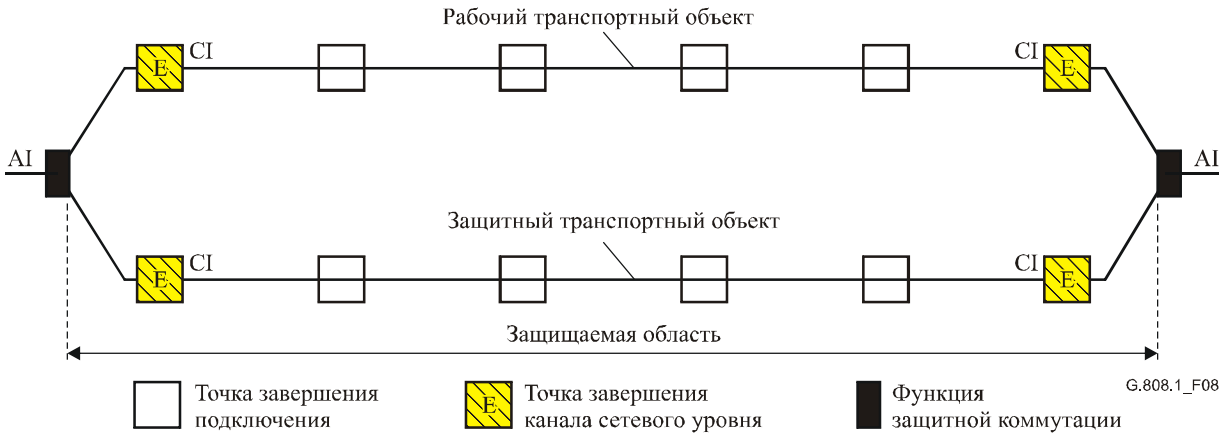


Рисунок 8/G.808.1 – Общая концепция защиты канала

ПРИМЕЧАНИЕ 1. – Поскольку типы 1:1, 1:n, m:n защиты канала являются линейными защитными механизмами, функции завершения канала нормального и избыточного трафика расположены в одном и том же NE. В сетевом приложении это требует, чтобы модели нормального и избыточного трафика совпадали.

Защита канала не поддерживает сетевые архитектуры, в которых используются каскадные защищенные подсети на том же уровне. Соответственно, трафик можно восстановить только в случае одиночной неисправности. Для восстановления трафика в условиях множественных ошибок должна использоваться защита SNC, или защита канала должна дополняться защитой на уровнях серверов.

ПРИМЕЧАНИЕ 2. – Для случая архитектуры 1:1, m:n или $(1:1)^n$ в сетях ATM защитный канал(каналы) должны содержать сигнал, который обеспечивает точный контроль его статуса. В нормальных условиях, когда сигнал нормального трафика транспортируется по рабочему каналу, по защитному каналу сигнал не транспортируется. Если контроль непрерывности (CC) неактивен, то по такому защитному каналу не будет транспортироваться информации в нормальных условиях отсутствия отказов. При возникновении отказа вводятся ячейки AIS. Когда состояние отказа сохраняется только в течение короткого периода (например, из-за "защитной операции физического уровня"), детектор неисправности AIS в конечной точке защитного канала обнаружит состояние неисправности AIS в течение 2–3 секунд согласно требованиям I.610 к определению состояния сигнала AIS. При активированной CC состояния неисправности AIS устраняется после получения ячейки CC, т. е. в течение 1 секунды после устранения прерывания трафика.

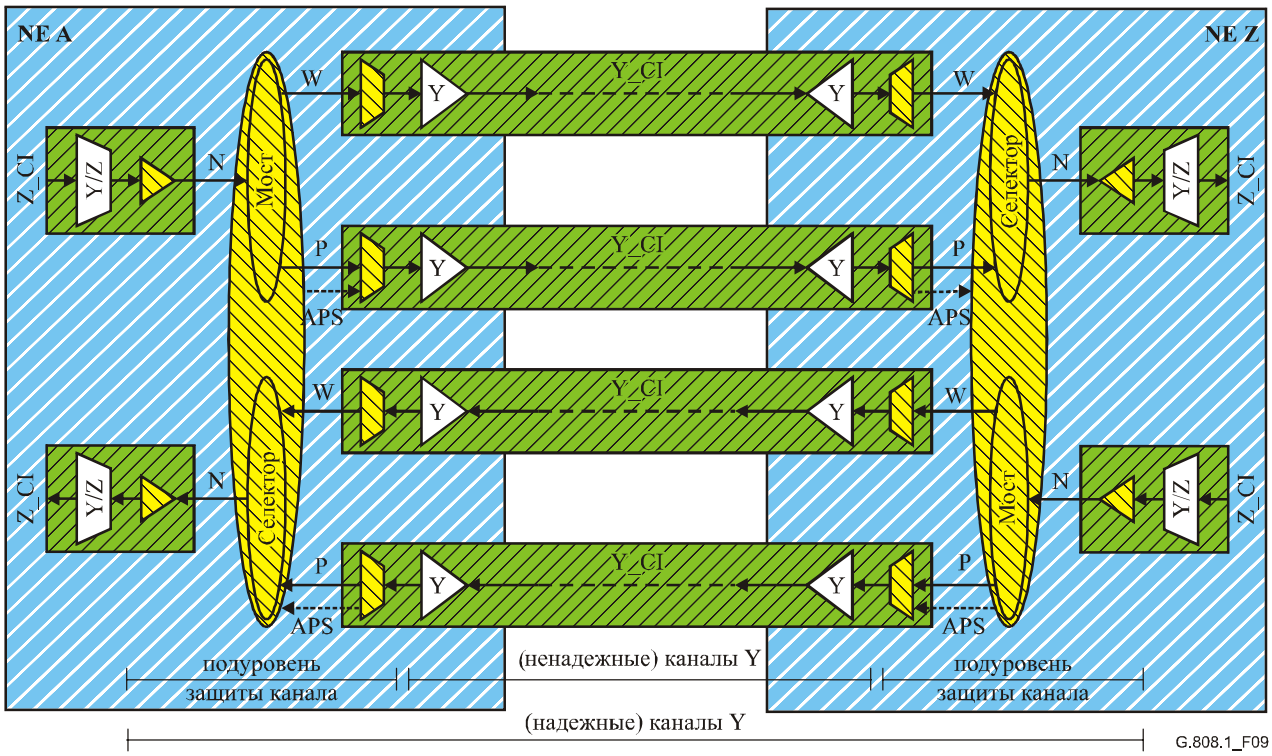
ПРИМЕЧАНИЕ 3. – Если защита канала используется на уровне маршрута, то в результате этого может быть занят дополнительный порт в структуре, по сравнению с защитой SNC. Это происходит, когда селектор защиты расположен в выходном порте аппаратуры.

11.1.1 Индивидуальная защита канала

На рисунке 9 иллюстрируется случай защиты канала 1+1 и защиты канала 1:1 без избыточного трафика между входом и выходом защищаемой области, т. е. между NE A и Z. Имеются два независимых канала (на сетевом уровне Y), которые действуют как рабочий и защитный

транспортные объекты для (защищаемого) сигнала нормального трафика (полезной информации). Функции TT генерируют/вводят и контролируют/извлекают сквозную служебную/OAM информацию для определения статуса рабочего и защитного транспортных объектов. Информация APS транспортируется по защитному каналу, за исключением случая однонаправленной коммутации 1+1.

Случаи архитектур 1:n, m:n и $(1:1)^n$ с избыточным трафиком/без него являются расширениями архитектуры 1+1/1:1 в соответствии с описаниями типов архитектуры в пункте 7.



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 9/G.808.1 – Функциональная модель защиты канала 1+1/1:1

11.1.2 Групповая защита канала

На рисунке 10 иллюстрируется случай групповой защиты канала 1+1/1:1 между NE A и Z. В этом примере имеются 2×3 параллельных независимых канала (на сетевом уровне Y), которые действуют как группы рабочих и защитных транспортных объектов для трех (защищаемых) сигналов нормального трафика (полезной информации). Три параллельных сигнала нормального трафика в группе совместно защищаются функцией подключения подуровня защиты канала. Функции TT генерируют/вводят и контролируют/извлекают сквозную служебную/OAM информацию для определения статуса рабочих и защитных транспортных объектов. Информация APS транспортируется по одному из защитных каналов, за исключением случая однонаправленной коммутации 1+1.

Случаи архитектур 1:n, m:n и $(1:1)^n$ с избыточным трафиком/без него являются расширениями архитектуры 1+1/1:1 в соответствии с описаниями типов архитектуры в пункте 7.

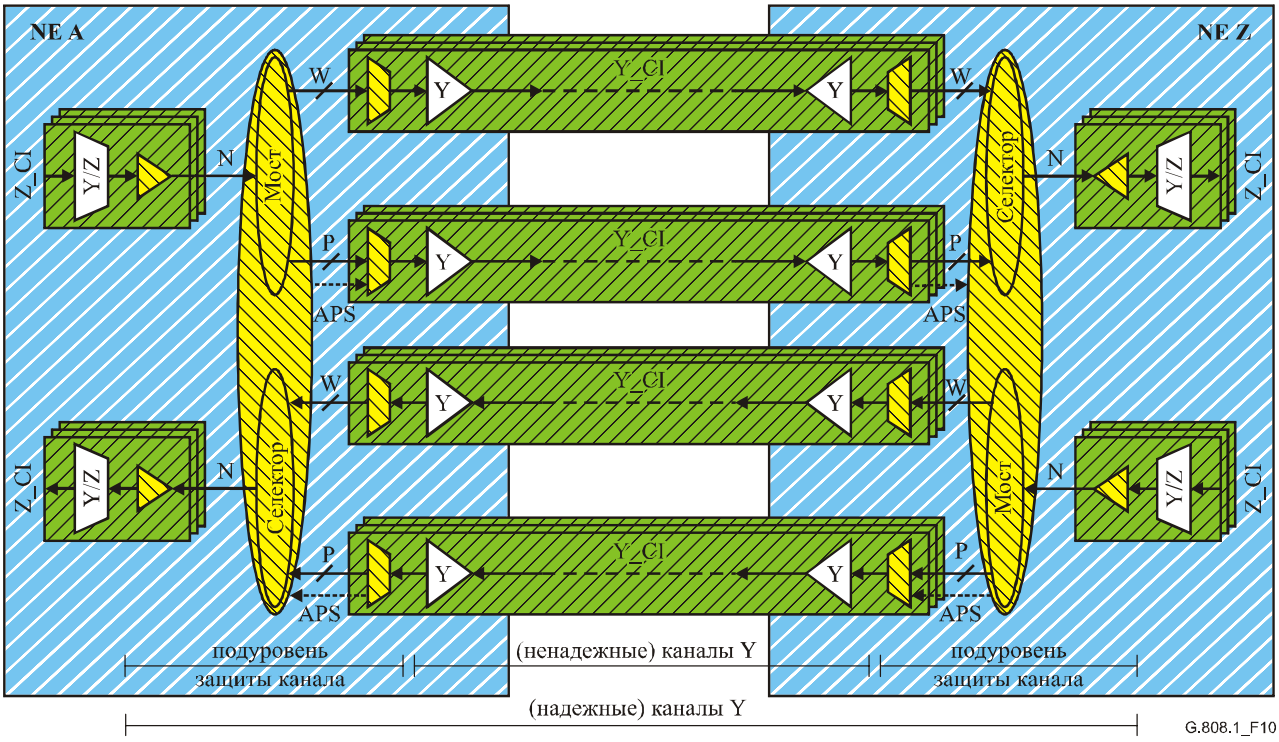


Рисунок 10/G.808.1 – Функциональная модель групповой защиты канала 1+1/1:1

На рисунке 11 представлены дополнительные сведения, касающиеся процессов реализации этой функции подключения защиты. Специфическим для групповой защиты является логический процесс SFG/SDG. Этот процесс "объединяет" три отдельных сигнала о сбое сигнала в канале (TSF) в единую группу SF (SFG), а отдельные сигналы об ухудшении параметров сигнала в канале (TSD) – в единую SDG.

Логика SFG/SDG может работать в различных режимах:

- W-SFG = W1-TSF, или W2-TSF, или W3-TSF

  P-SFG = P1-TSF, или P2-TSF, или P3-TSF;
- W-SFG = W1-TSF

  P-SFG = P1-TSF;
- W-SFG = X% сигналов Wi-TSF активны

  P-SFG = X% сигналов Pi-TSF активны;
- то же, для SDG.

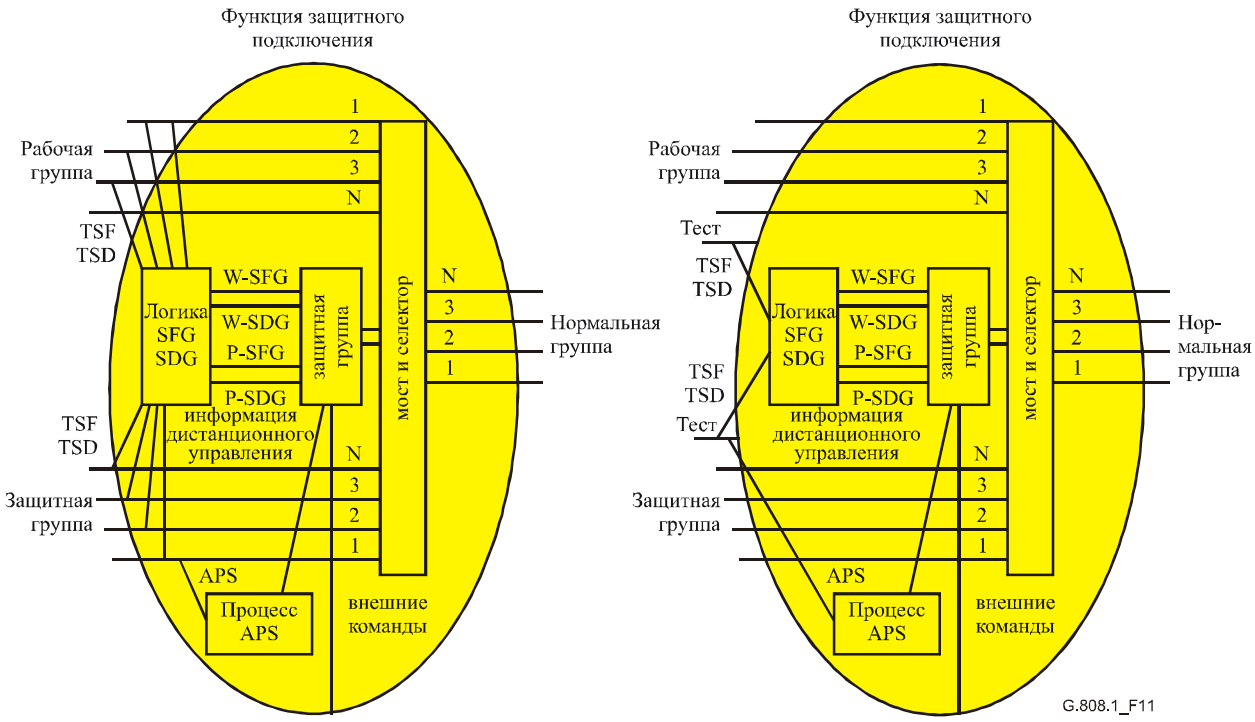


Рисунок 11/G.808.1 – Логика SFG/SDG в процессе групповой защиты

В результате наличия большого числа дополнительных временных интервалов в некоторых технологиях передачи (например, в ATM), избыточные дополнительные временные интервалы в сигналах рабочего и защитного уровня сервера могут быть выделены для транспортировки испытательных сигналов через испытательные транспортные объекты (рисунки 12 и 13). Эти испытательные сигналы (один – на рабочий объект, один – на транспортный объект) могут использоваться вместо информации SFG, SDG, как описано выше. Сигнал APS транспортируется через испытательный тестовый защитный транспортный объект.

Логика SFG/SDG работает следующим образом:

- W-SFG = Wt-TSF
  P-SFG = Pt-TSF;
- W-SDG = Wt-TSD
  P-SDG = Pt-TSD.

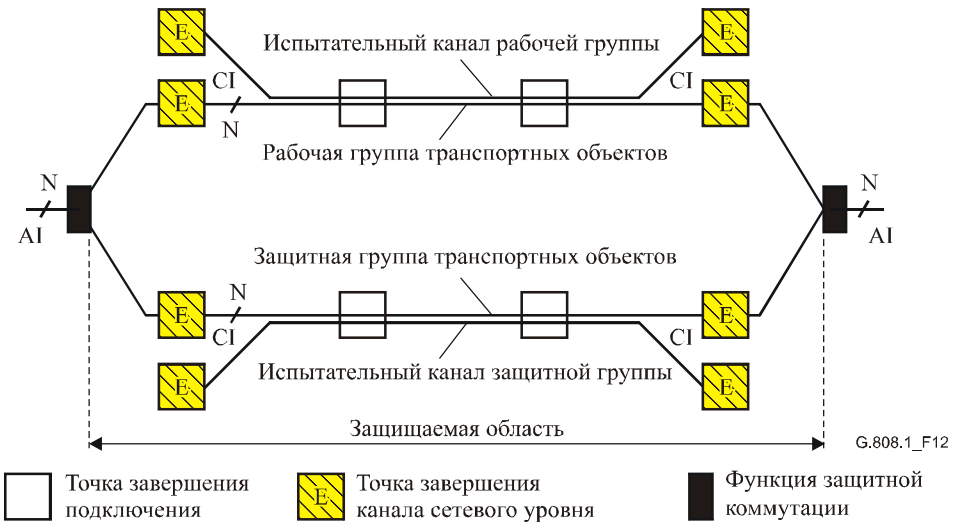


Рисунок 12/G.808.1 – Общая концепция групповой защиты канала/T

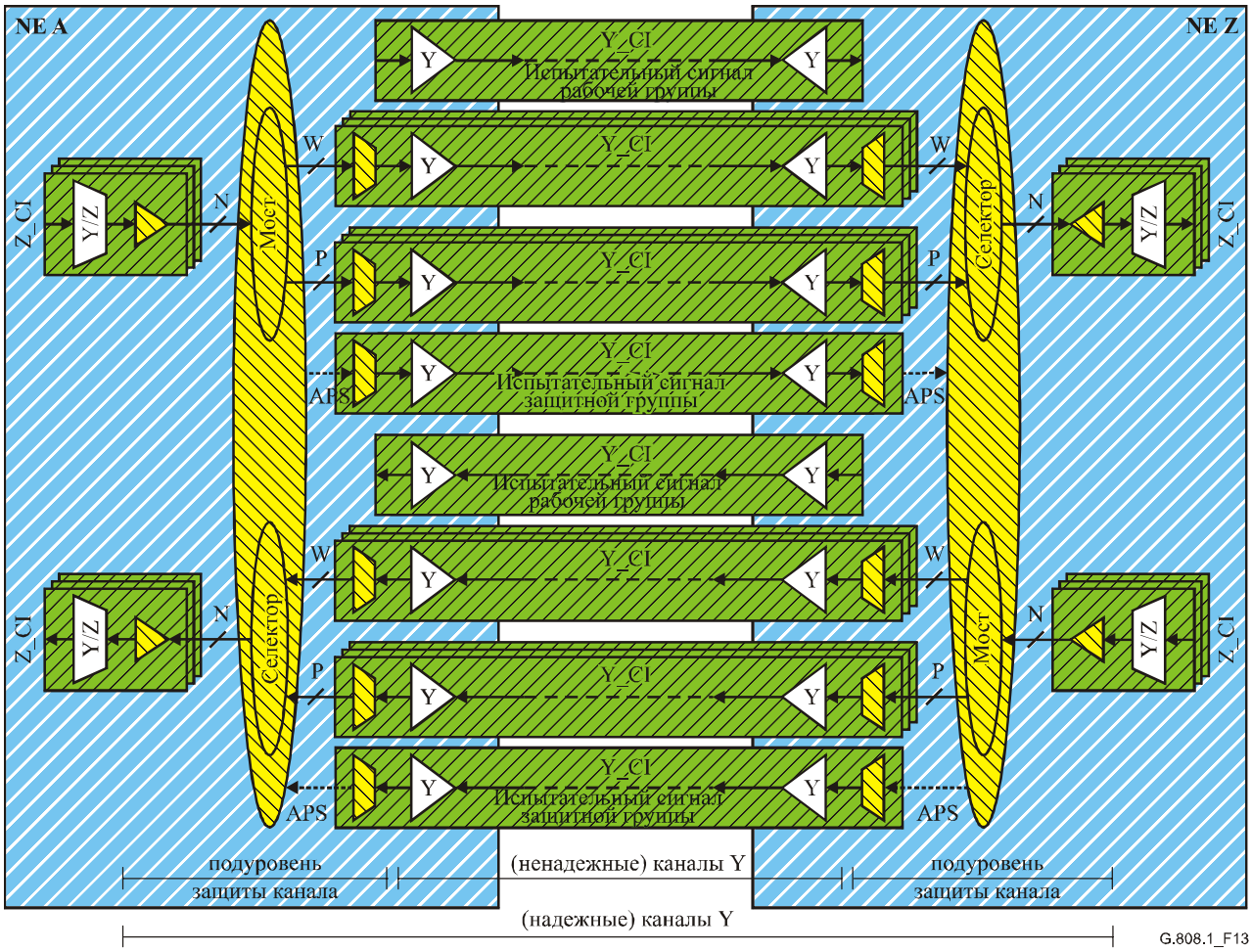


Рисунок 13/G.808.1 – Функциональная модель групповой защиты T/канала 1+1/1:1

11.2 Защита SNC

Защита подключения подсети – класс защиты, используемый для защиты части канала (например, той части, где имеются два отдельных маршрута) в сети оператора или сетях нескольких операторов.

Защищаемое подключение подсети может иметь место между двумя точками подключения (CP) (рисунок 14), между CP и точкой завершения подключения (TCP) (рисунок 15), или речь может идти о полном сквозном сетевом подключении между двумя TCP (рисунок 16).

Поскольку защита подключения подсети является выделенным защитным механизмом, то она может использоваться в любой физической структуре (т. е. ячеистой, кольцевой или смешанной), и принципиальное ограничение на количество NE внутри подключения подсети отсутствует. Она может применяться на любом уровне сети, структурированной по уровням.

Защита SNC работает во всех сочетаниях типов защитных архитектур, коммутации и срабатывания.

SNCP может далее подразделяться на подклассы, представляющие условия появления неисправностей, которые вносят вклад в SF/SD:

1) Внутренняя защита: функции завершения и адаптации канала уровня сервера используются для определения состояния SF/SD. Она поддерживает только обнаружение состояния неисправности на уровне сервера.

2) Ненарушающая защита: функции ненарушающего контроля используются для определения состояния SF/SD.

   a) Сквозная защита: обнаружение состояния неисправности на уровне сервера, состояния нарушения непрерывности/связности в сети уровня и состояния ухудшения показателя ошибок в сети уровня. Используются сквозные служебные/OAM сигналы.

   b) Защита на подуровне: обнаружение состояний неисправности на уровне сервера, состояний нарушения непрерывности/связности в сети уровня и состояний ухудшения показателя ошибок в сети уровня. Используются служебные/OAM сигналы подуровня.

3) Защита на подуровне: Функции подуровня тандемного подключения/сегмента используются для определения состояния SF/SD. Она поддерживает обнаружение состояния неисправности на уровне сервера, состояния нарушения непрерывности/связности в сети уровня и состояния ухудшения показателя ошибок в сети уровня. Используются служебные/OAM сигналы подуровня.

В общем случае защита SNC требует создания каналов подуровня (тандемные подключения, сегменты) на рабочем и защитном транспортных объектах для различения отказа ухудшения параметров, происходящих "перед" и "внутри" защищаемой области. Когда канал подуровня содержит единственный канал уровня сервера, этот канал уровня сервера может использоваться взамен (обеспечивая внутренний контроль). Если канал подуровня нельзя создать или единственный канал уровня сервера между точками входа и выхода защищаемой области недоступен, то защиту SNC можно осуществить за счет подачи сигнала нормального трафика как на рабочий, так и на защитный транспортные объекты, ненарушающего контроля обеих копий сигнала в выходной точке и сравнения статуса SF/SD, полученных с обоих мониторов. Если отказ или ухудшение параметров происходит перед защищаемой областью, то и рабочий, и защитный мониторы обнаружат неисправность, и операции переключения не произойдет. В противном случае только один из двух мониторов обнаружит состояние SF/SD, и трафик может быть восстановлен посредством операции переключения.

ПРИМЕЧАНИЕ 1. – Для СЦИ, за счет обработки указателей AU/TU при состоянии TSF уровня сервера, схема 1+1 SNC/I может использоваться вместо 1+1 SNC/N, если нужно обеспечить защиту только от неисправностей на уровне сервера.

Для случая защиты SNC защищается характеристическая информация (CI) (т. е. полезная информация и служебные сигналы соответствующего уровня). См. рисунки 14–17.

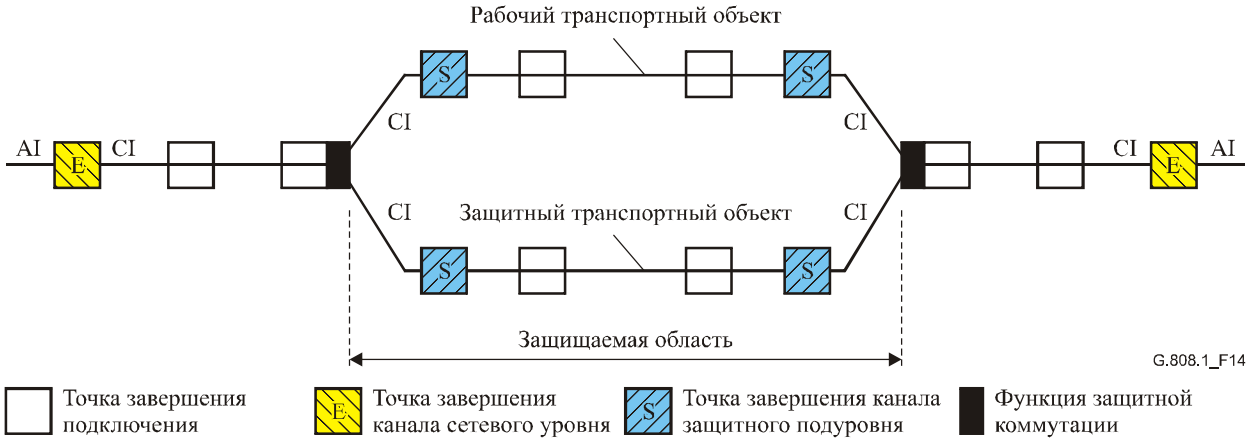


Рисунок 14/G.808.1 – Пример 1 защиты SNC/S

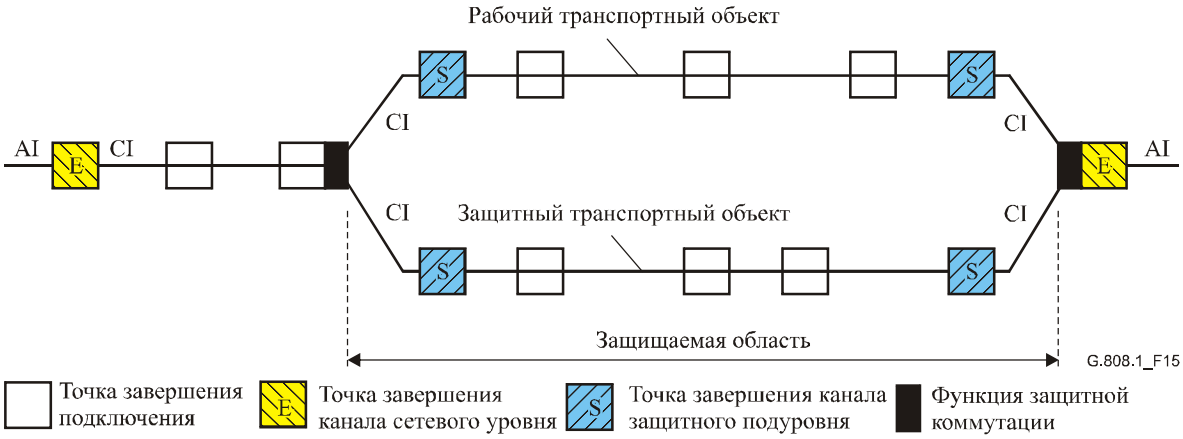


Рисунок 15/G.808.1 – Пример 2 защиты SNC/S

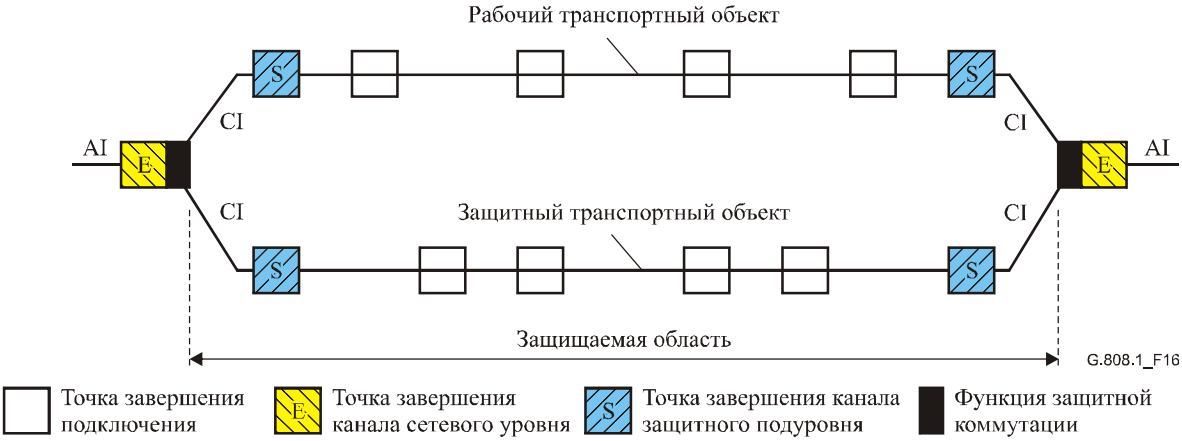


Рисунок 16/G.808.1 – Пример 3 защиты SNC/S

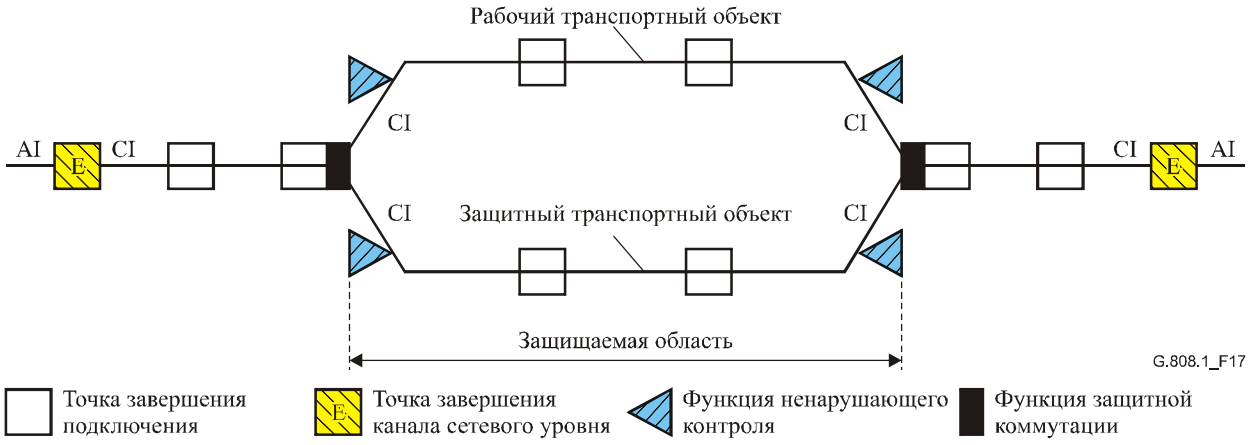


Рисунок 17/G.808.1 – Защита 1+1 SNC/N

Защита SNC поддерживает сетевые архитектуры, в которых используются каскадные защищенные подсети. Такие сетевые архитектуры могут восстанавливать трафик в случае многочисленных отказов (один отказ на защищаемую подсеть); см. рисунок 18.

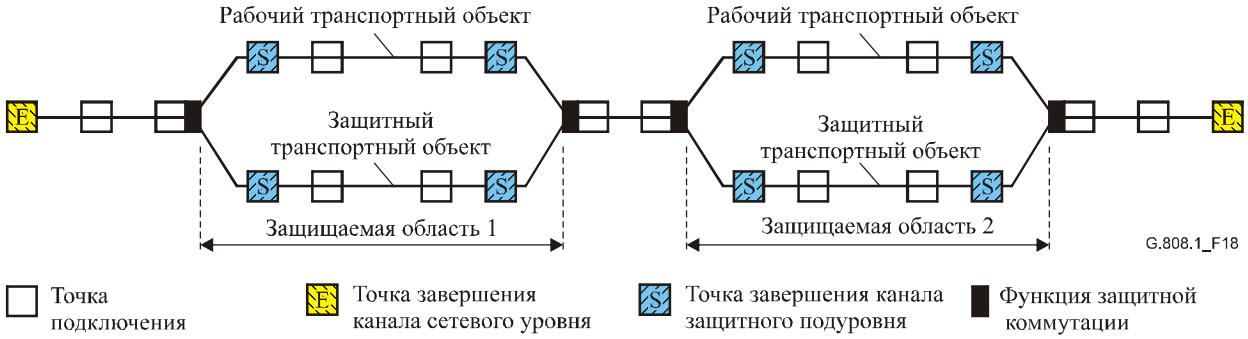


Рисунок 18/G.808.1 – Каскадная защита SNC/S

Сохранение работоспособности при отказах (и надежность) подсетей с каскадной защитой SNC возрастает, когда соединение между подсетями дублируется (рисунок 19), удаляя единственную точку отказа. Это требует использования типов защиты 1+1, однонаправленной коммутируемой SNC/N или SNC/I. Использование защиты 1:n, m:n, $(1:1)^n$ и/или двунаправленной коммутации невозможно.

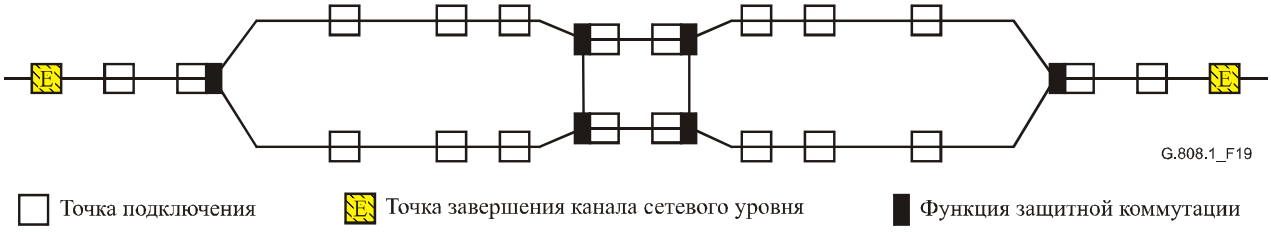


Рисунок 19/G.808.1 – Каскадная защита 1+1 SNC с соединениями подсетей, устойчивых к отказам

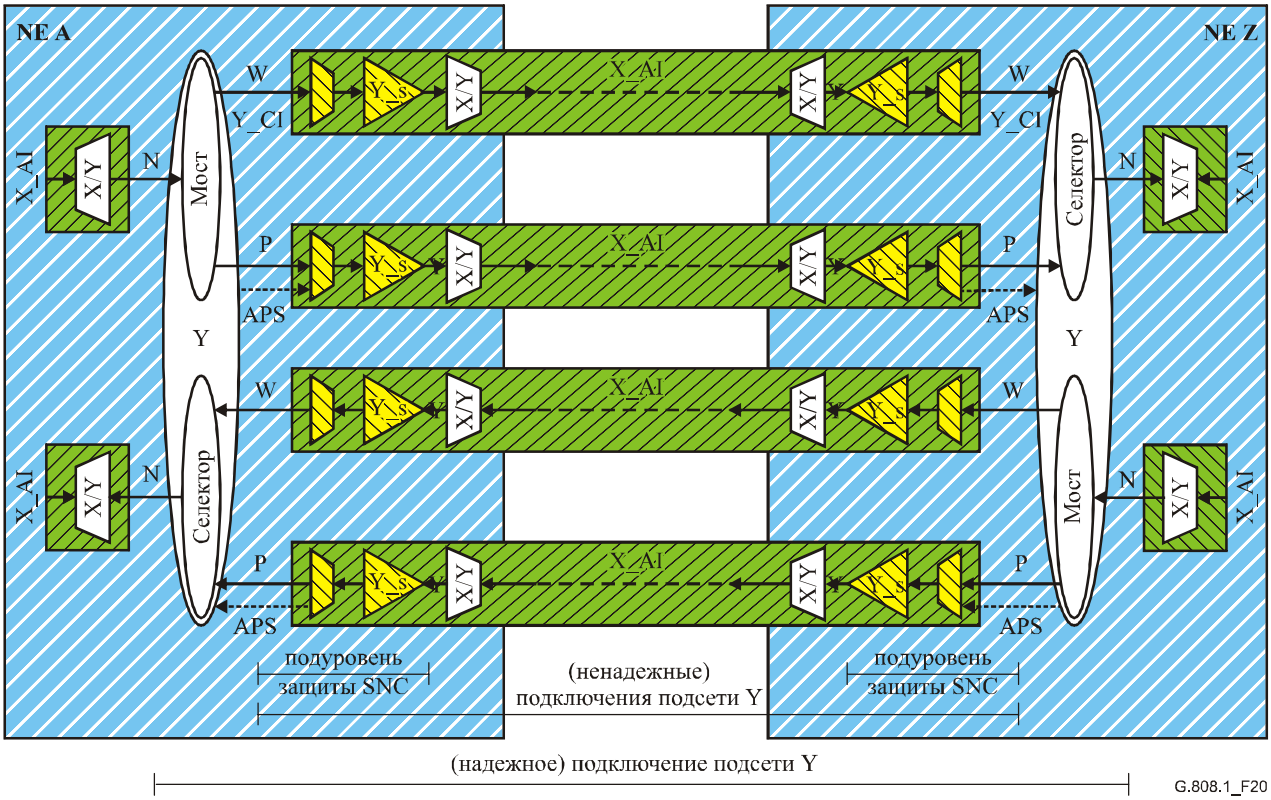
ПРИМЕЧАНИЕ 2. – Для случая архитектуры 1:1, m:n или $(1:1)^n$ в сетях ATM, соединение(соединения) защитной подсети должны содержать сигнал, который позволяет осуществлять точный контроль ее статуса. В обычных условиях, когда сигнал нормального трафика транспортируется через рабочую SNC, сигнал через защиту не передается. Если CC неактивен, то такая защитная SNC не будет транспортировать информации при нормальных состояниях отсутствия отказов. При появлении отказа включаются ячейки AIS. Когда отказ имеет место только в течение короткого периода (например, из-за "защитной операции физического уровня"), детектор появления неисправности AIS в конечной точке защитного сегмента обнаружит состояние неисправности AIS в течение 2–3 секунд согласно требованиям I.610 к определению состояния AIS. При активированном CC состояние неисправности AIS будет устранено по получении ячейки CC, т. е. в течение 1 секунды после прекращения прерывания трафика.

11.2.1 Индивидуальная защита SNC

11.2.1.1 Защита SNC/S 1+1, 1:n, m:n, $(1:1)^n$

На рисунке 20 иллюстрируется случай защиты SNC/S 1+1 и SNC/S 1:1 без избыточного трафика между входом и выходом защищаемой области, т. е. между NE A и Z. Имеются два независимых канала подуровня, которые действуют как рабочий и защитный транспортные объекты для (защищаемого) сигнала нормального трафика. Функции подуровня TT генерируют/вводят и контролируют/извлекают служебную/OAM информацию подуровня для определения статуса рабочего и защитного транспортных объектов. Информация APS транспортируется через защиту SNC, за исключением случая однонаправленной коммутации 1+1.

Случаи архитектур 1:n, m:n и $(1:1)^n$ с избыточным трафиком/без него являются расширениями архитектуры 1+1/1:1, в соответствии с описаниями типов архитектуры в пункте 7.



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

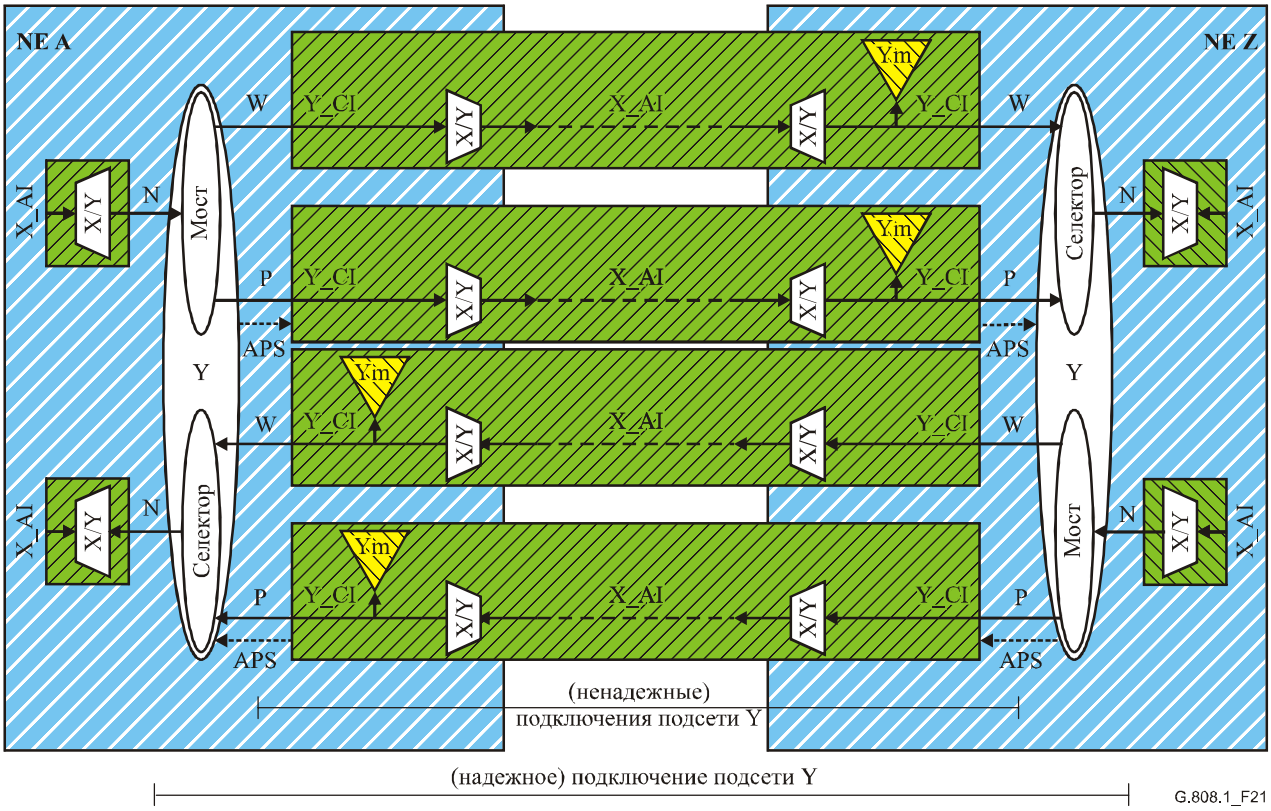
Рисунок 20/G.808.1 – Функциональная модель защиты SNC/S 1+1/1:1

ПРИМЕЧАНИЕ. – Функции подуровня завершения канала (например, функции завершения тандемного подключения/сегмента) используются для административных целей (для контроля качества услуги транспортировки через административную область сети) и защитных целей. Для целей защиты расположение завершений канала подуровня должно быть таким, как показано на рисунках, касающихся SNC/S. Для административных целей оптимальным является расположение на другой стороне функции подключения.

11.2.1.2 Защита SNC/N 1+1

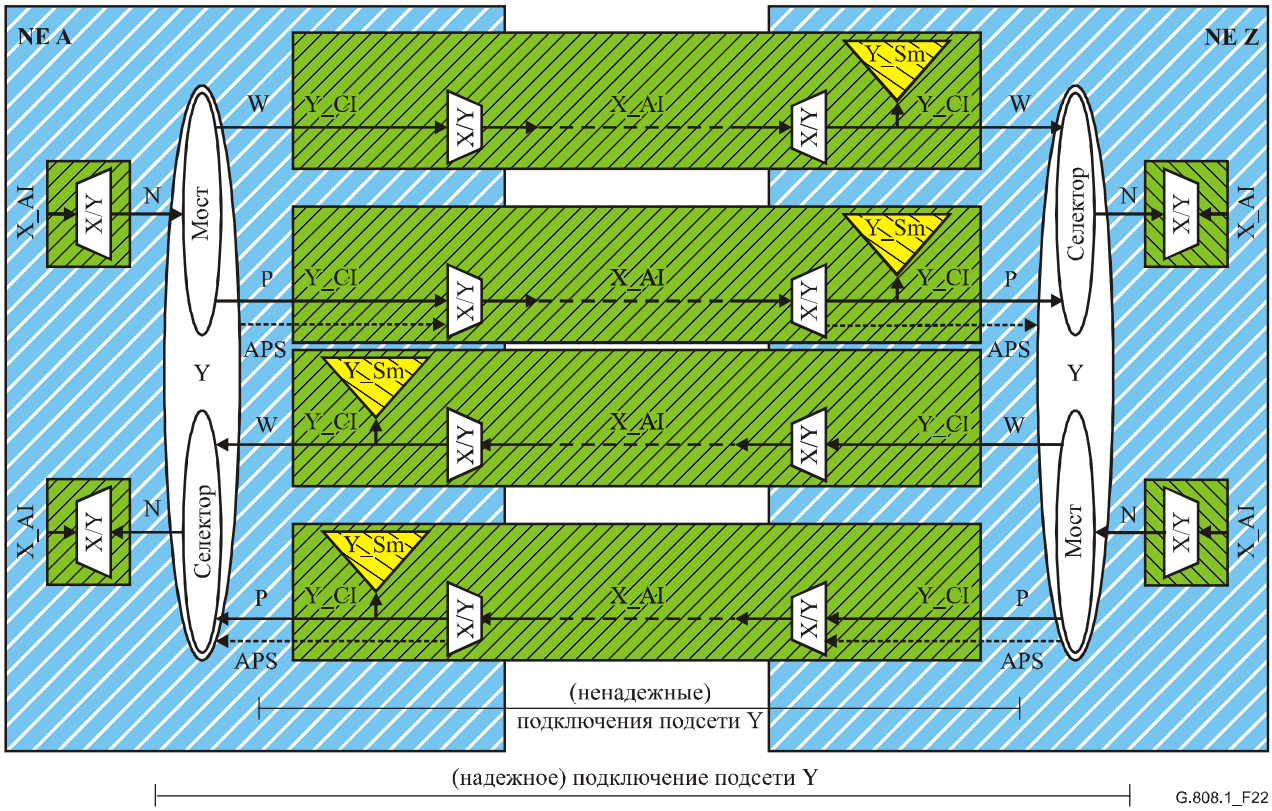
Для случая защиты SNC 1+1 определена схема *пониженной сложности*: SNC/N.

На рисунках 21 и 22 иллюстрируется случай защиты SNC/N 1+1 между входом и выходом защищаемой области, т. е. между NE A и Z. Имеются два независимых соединения подсети, которые действуют как рабочий и защитный транспортные объекты для (защищаемого) сигнала нормального трафика. Функции ненарушающего контроля (NIM) (Ym_TT_Sk, Y_Sm_TT_Sk) контролируют сквозную (SNC/Ne) или подуровневую (SNC/Ns) служебную/OAM информацию для определения статуса рабочего и защитного транспортных объектов. Информация APS транспортируется через защиту SNC, за исключением случая однонаправленной коммутации 1+1.



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 21/G.808.1 – Функциональная модель защиты SNC/Ne 1+1



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 22/G.808.1 – Функциональная модель защиты SNC/Ns 1+1

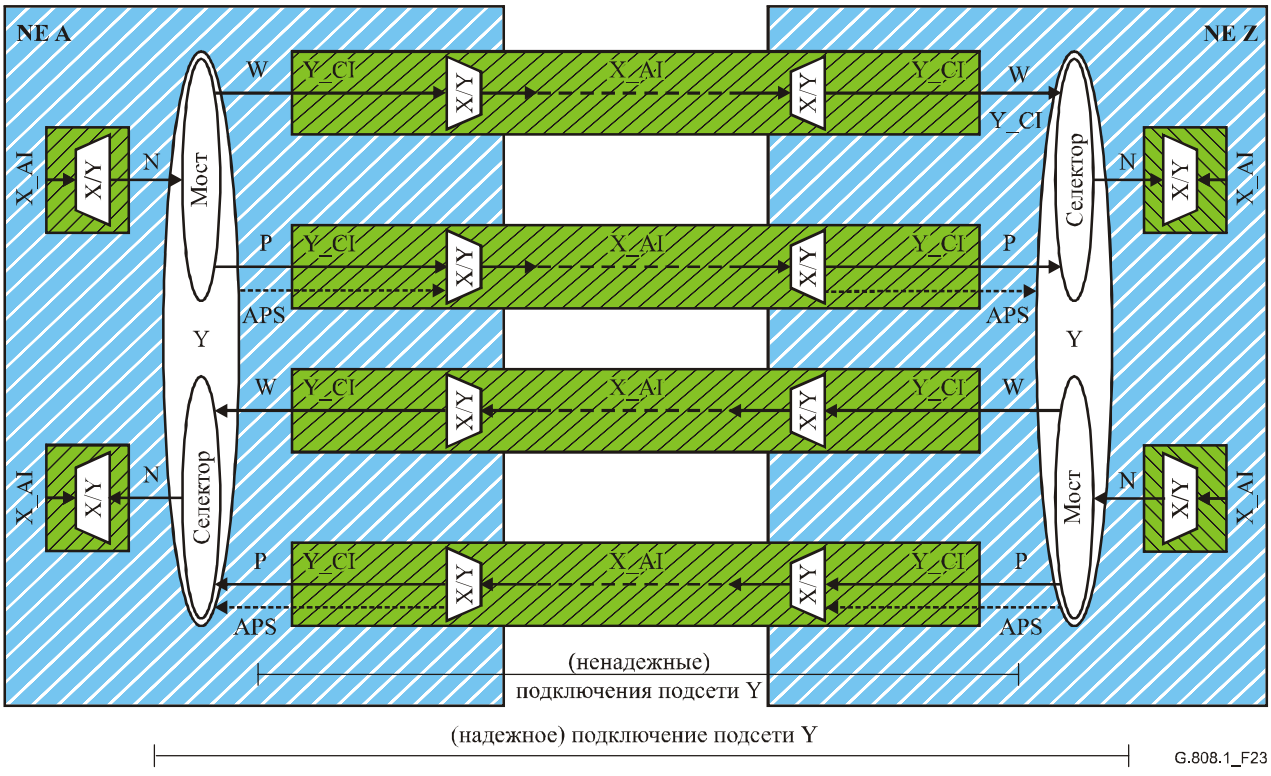
11.2.1.3 Защита SNC/I 1+1/1:n

Для случая защиты SNC 1+1/1:n используется еще одна схема *пониженной сложности*: SNC/I.

На рисунке 23 иллюстрируется случай защиты SNC/I 1+1/1:1 между входом и выходом защищаемой области, т. е. между NE A и Z. Имеются два независимых соединения подсети, которые действуют как рабочий и защитный транспортные объекты для (защищаемого) сигнала нормального трафика. Функции адаптации X/Y контролируют адаптированную информацию уровня сервера в отношении сбоя сигнала, чтобы определить статус рабочего и защитного транспортных объектов. Информация APS транспортируется через защиту SNC, за исключением случая однонаправленной коммутации 1+1.

В общем случае защита SNC/I – это защитная схема для подключения одиночной линии (охватывающего только один канал уровня сервера), поскольку функции адаптации получают свои данные SSF и SSD из сигналов TSF/TSD канала уровня сервера. Данные о статусе TSF пересылаются в виде сигнала обслуживания AIS/FDI клиентского уровня и не различаются как таковые функциями адаптации нисходящего потока. Информация TSD не передается.

Имеется исключение для защиты СЦИ VC-n SNC/I; защита SNC/I способна защитить подключение последовательной составной линии, поскольку сигнал обслуживания AIS обнаруживается в каждом нисходящем потоке функции адаптации точки подключения.



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 23/G.808.1 – Функциональная модель защиты SNC/I 1+1/1:1

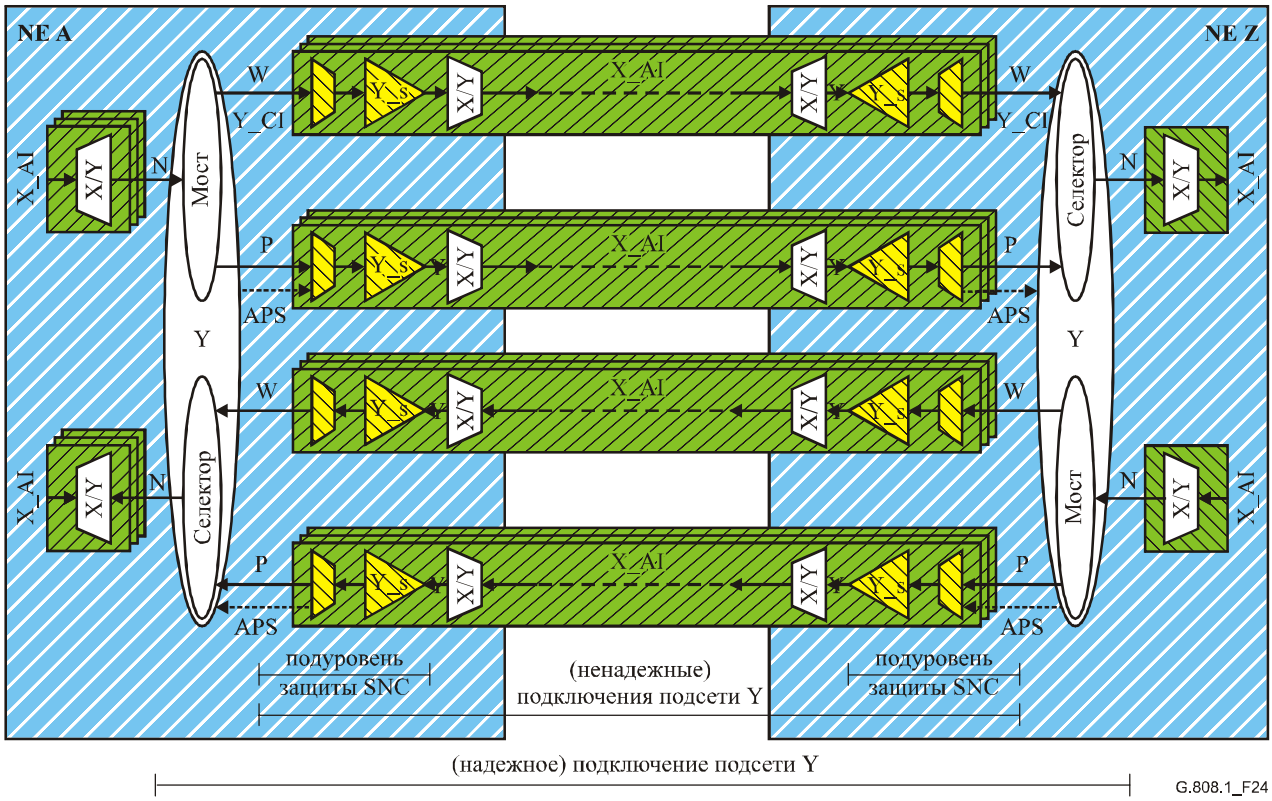
11.2.2 Групповая защита SNC

11.2.2.1 Защита SNC/S

На рисунке 24 иллюстрируется случай групповой защиты SNC/S 1+1/1:1 между NE A и Z. В этом примере имеются 2×3 параллельных независимых подключения подсети, контролируемых каналом подуровня, которые действуют как группы рабочих и защитных транспортных объектов для трех (защищаемых) сигналов нормального трафика. Три параллельных сигнала нормального трафика в группе совместно защищаются функцией подключения уровня. Функции TT подуровня генерируют/вводят и контролируют/извлекают служебную/OAM информацию подуровня для определения статуса рабочих и защитных транспортных объектов. Информация APS

транспортируется через одно из защитных SNC, за исключением случая однонаправленной коммутации 1+1.

Случаи архитектур 1:n, m:n и $(1:1)^n$ с избыточным трафиком/без него являются расширениями архитектуры 1+1/1:1 в соответствии с описаниями типов архитектуры в пункте 7.



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 24/G.808.1 – Функциональная модель групповой защиты SNC/S 1+1/1:1

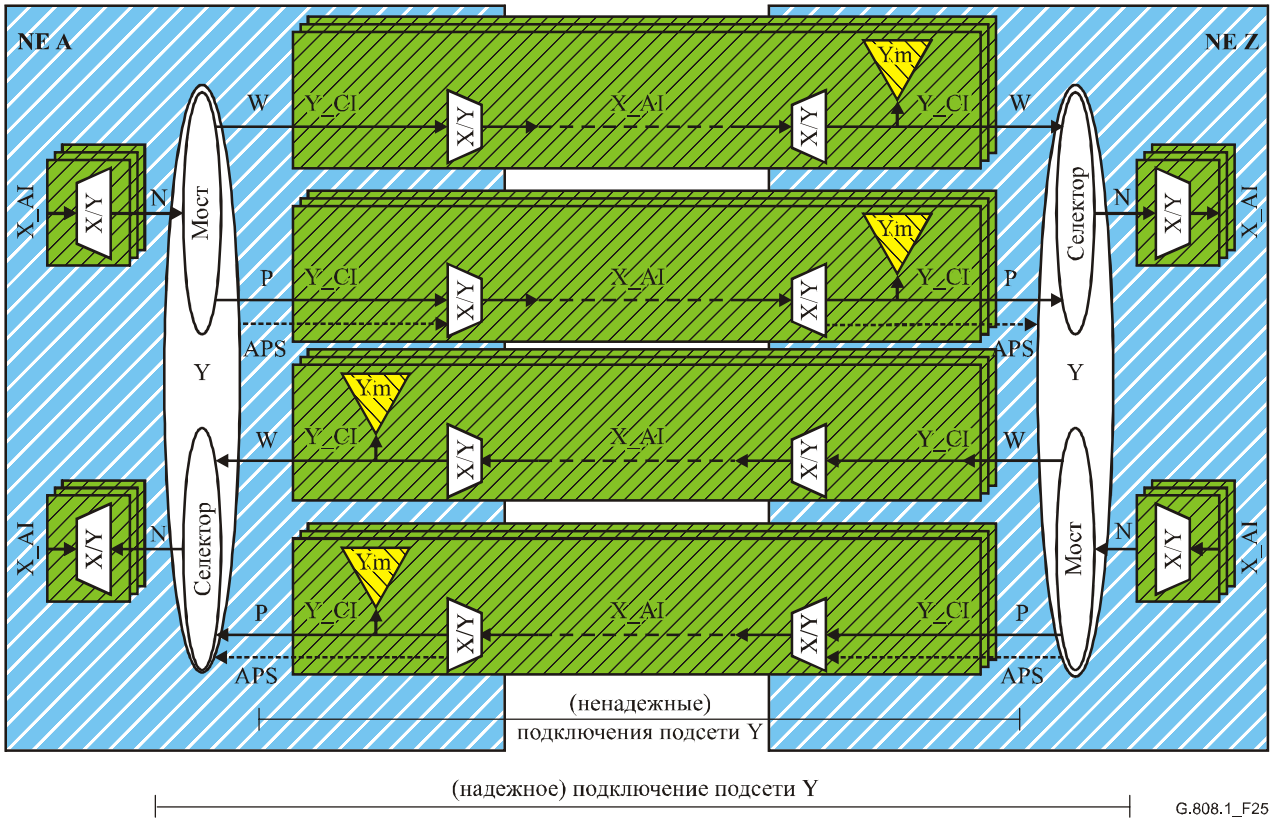
На рисунке 11 представлены дополнительные сведения, касающиеся процессов реализации этой функции подключения защиты. Специфическим для групповой защиты является логический процесс SFG/SDG. Этот процесс "объединяет" три отдельных сигнала о сбое сигнала в канале (TSF) в единую группу SF (SFG), а отдельные сигналы об ухудшении параметров сигнала в канале (TSD) – в единую группу SDG.

Логика SFG/SDG может работать в различных режимах:

- W-SFG = W1-TSF, или W2-TSF, или W3-TSF; P-SFG = P1-TSF, или P2-TSF, или P3-TSF;
- W-SFG = W1-TSF; P-SFG = P1-TSF;
- W-SFG = X% от сигналов Wi-TSF активны; P-SFG = X% от сигналов Pi-TSF активны;
- то же, для SDG.

11.2.2.2 Защита SNC/N 1+1

На рисунке 25 иллюстрируется случай групповой защиты SNC/N 1+1 между NE A и Z. В этом примере имеются 2×3 параллельных независимых подключения подсети, которые действуют как группы рабочих и защитных транспортных объектов для трех (защищаемых) сигналов нормального трафика. Три параллельных сигнала нормального трафика в группе совместно защищаются функцией подключения уровня. Функции NIM контролируют сквозную (SNC/Ne) или подуровневую (SNC/Ns) служебную/OAM информацию для определения статуса рабочих и защитных транспортных объектов. Информация APS транспортируется через одно из защитных SNC, за исключением случая однонаправленной коммутации 1+1.



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 25/G.808.1 – Функциональная модель групповой защиты SNC/Ne 1+1

На рисунке 11 представлены дополнительные сведения, касающиеся процессов реализации этой функции защитного подключения. Специфическим для групповой защиты SNC/N 1+1 является логический процесс SFG/SDG. Этот процесс "объединяет" три отдельных сигнала о сбое сигнала в канале (TSF) в единую группу SF (SFG), а отдельные сигналы об ухудшении параметров сигнала в канале (TSD) – в единую группу SDG.

Логика SFG/SDG может работать в различных режимах:

- W-SFG = (W1-TSF и не P1-TSF), или (W2-TSF и не P2-TSF), или (W3-TSF и не P3-TSF);

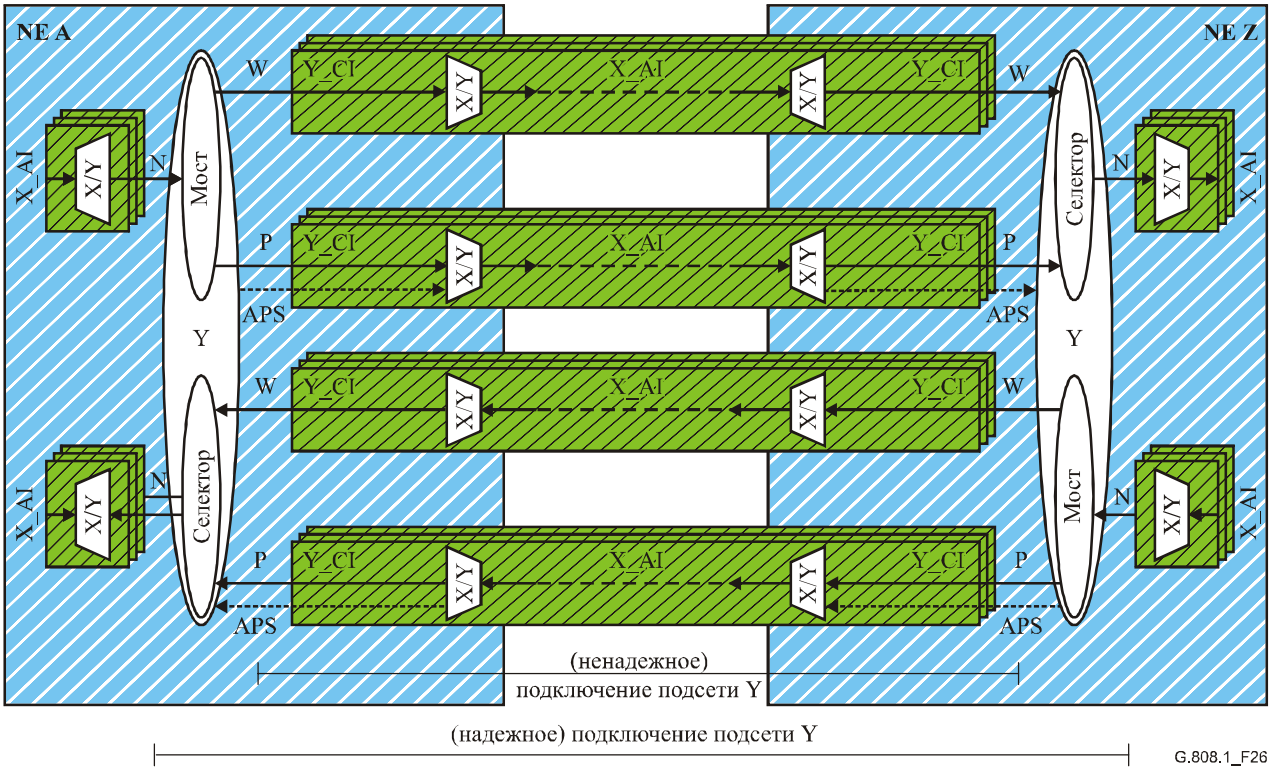
  P-SFG = (P1-TSF и не W1-TSF), или (P2-TSF и не W2-TSF), или (P3-TSF и не W3-TSF);
- W-SFG = (W1-TSF и не P1-TSF); P-SFG = (P1-TSF и не W1-TSF);
- W-SFG = X% от сигналов (Wi-TSF и не Pi-TSF) активны; P-SFG = X% от сигналов (Pi-TSF и не Wi-TSF) активны;
- то же, для SDG.

Для виртуальных сцепленных сигналов СЦИ VC-n (VC-n-Xv), должна устанавливаться группа условий SF и SD, как только происходит сбой или ухудшение параметров одного из X сигналов в группе.

- W-SFG = W1-TSF, или W2-TSF, или W3-TSF; P-SFG = P1-TSF, или P2-TSF, или P3-TSF;
- то же, для SDG.

11.2.2.3 Защита SNC/I 1+1

На рисунке 26 иллюстрируется случай групповой защиты SNC/I 1+1 между NE A и Z. В этом примере имеются 2×3 параллельных независимых соединений подсети, которые действуют как группы рабочих и защитных транспортных объектов для трех (защищаемых) сигналов нормального трафика. Три параллельных сигнала нормального трафика в группе совместно защищаются функцией подключения уровня. Функции адаптации X/Y контролируют адаптированную информацию уровня сервера в отношении сбоя сигнала, чтобы определить статус рабочих и защитных транспортных объектов. Информация APS транспортируется через одно из защитных SNC, за исключением случая однонаправленной коммутации 1+1.



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 26/G.808.1 – Функциональная модель групповой защиты SNC/I 1+1

На рисунке 11 представлены дополнительные сведения, касающиеся процессов реализации этой функции подключения защиты. Специфическим для групповой защиты SNC/I 1+1 является логический процесс SFG. Этот процесс "объединяет" три отдельных сигнала о сбое сигнала сервера (SSF) в единую группу SF (SFG).

Логика SFG/SDG может работать в различных режимах:

- W-SFG = (W1-SSF и не P1-SSF), или (W2-SSF и не P2-SSF), или (W3-SSF и не P3-SSF);

  P-SFG = (P1-SSF и не W1-SSF), или (P2-SSF и не W2-SSF), или (P3-SSF и не W3-SSF);
- W-SFG = (W1-SSF и не P1-SSF); P-SFG = (P1-SSF и не W1-SSF);
- W-SFG = X% от сигналов (Wi-SSF и не Pi-SSF) активны; P-SFG = X% от сигналов (Pi-SSF и не Wi-SSF) активны.

Для виртуальных сцепленных сигналов СЦИ VC-n (VC-n-Xv) должна устанавливаться группа условий SF и SD, как только происходит сбой или ухудшение параметров одного из X сигналов в группе.

- W-SFG = W1-SSF, или W2-SSF, или W3-SSF; P-SFG = P1-SSF, или P2-SSF, или P3-SSF;
- то же, для SDG.

11.2.2.4 Защита SNC/T

Из-за наличия большого числа дополнительных временных интервалов в некоторых технологиях передачи (например, в ATM), избыточные дополнительные временные интервалы в сигналах рабочего и защитного уровня сервера могут быть выделены для транспортировки испытательных сигналов через испытательные транспортные объекты (рисунки 27 и 29). Эти испытательные сигналы (один – на рабочий объект, один – на защитный объект) могут использоваться вместо информации SFG, SDG, как описано выше. Сигнал APS транспортируется через испытательный защитный транспортный объект.

Логика SFG/SDG работает следующим образом:

- W-SFG = Wt-TSF;

  P-SFG = Pt-TSF;
- W-SDG = Wt-TSD;

  P-SDG = Pt-TSD.

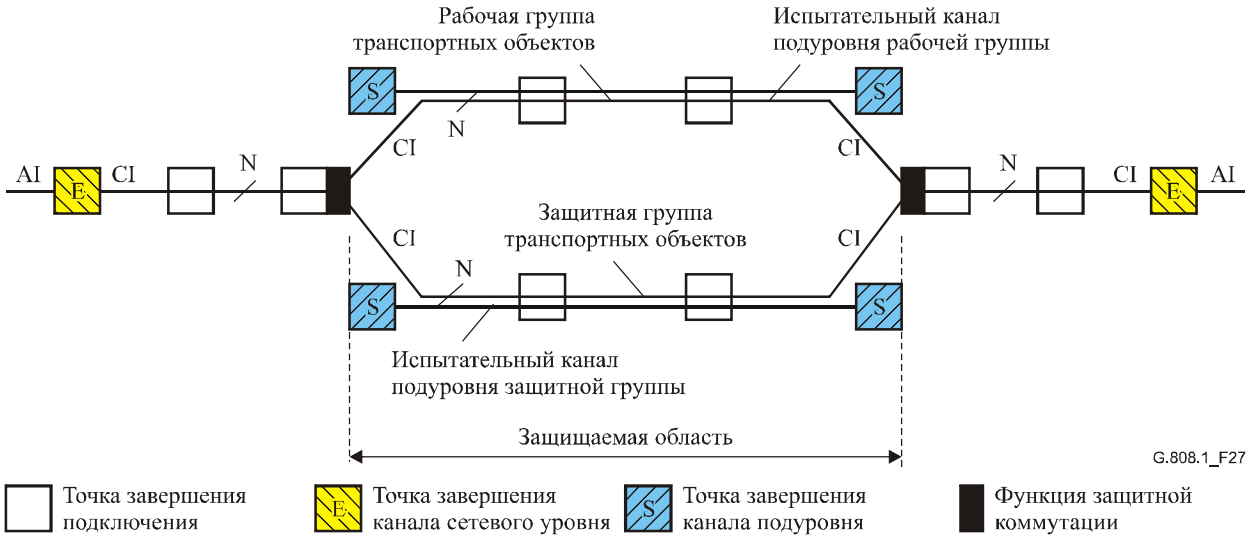


Рисунок 27/G.808.1 – Групповая защита SNC/Ts 1:1 или 1+1, использующая завершения канала подуровня

Группа защиты SNC/T может использовать также сквозные служебные/OAM сигналы для создания сквозного канала сетевого уровня в качестве испытательного канала (рисунок 28). В конструкциях аппаратуры эти функции завершения уровня обычно расположены в блоках порта, на "другой стороне" функции подключения; т. е. не готовы постоянно для целей создания испытательного канала групповой защиты.

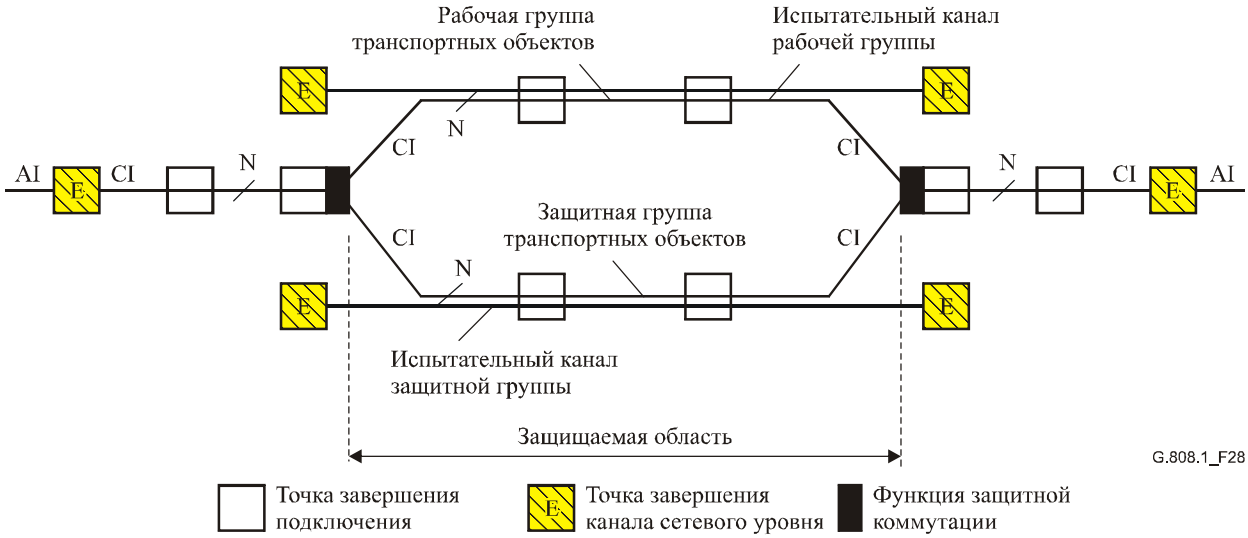
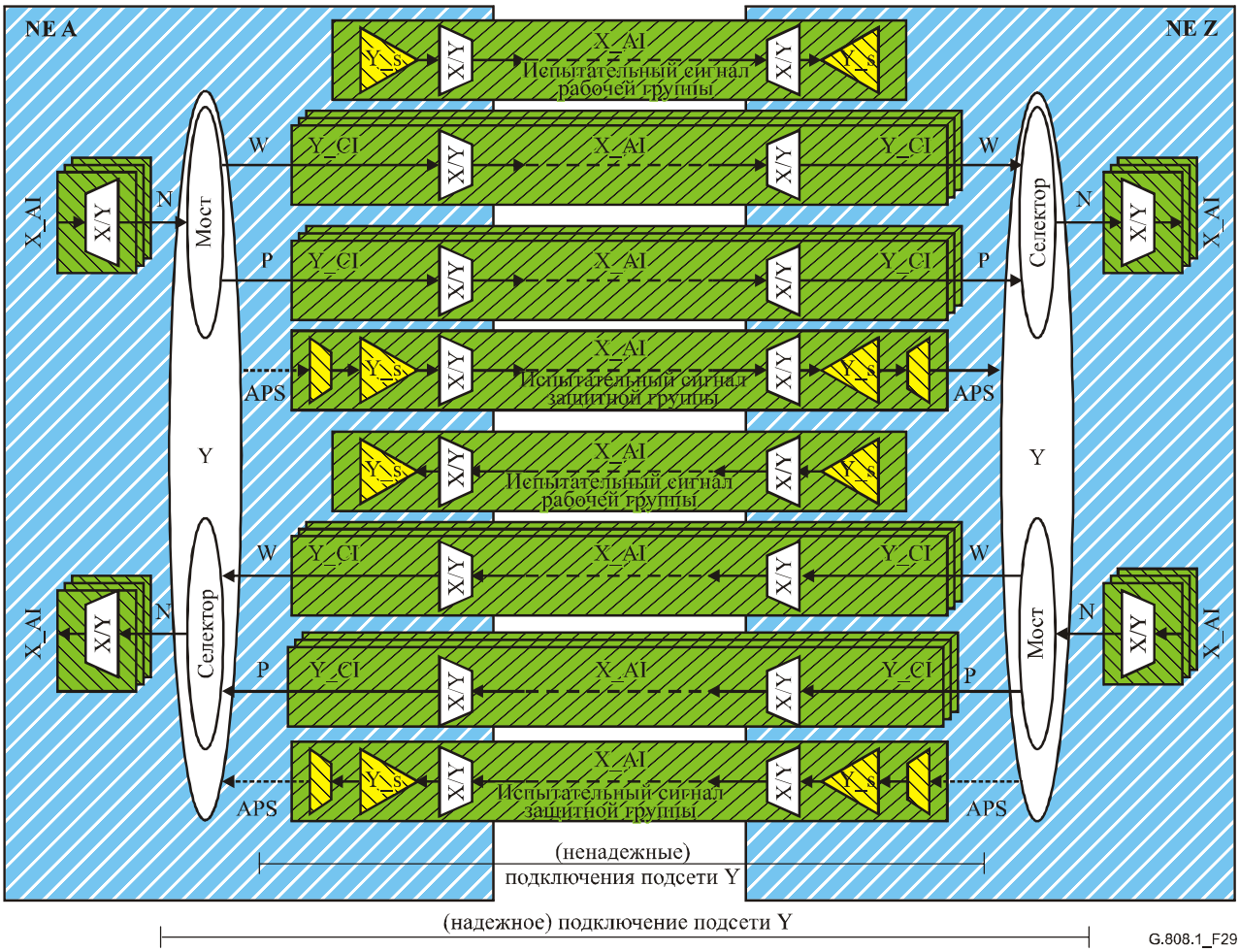


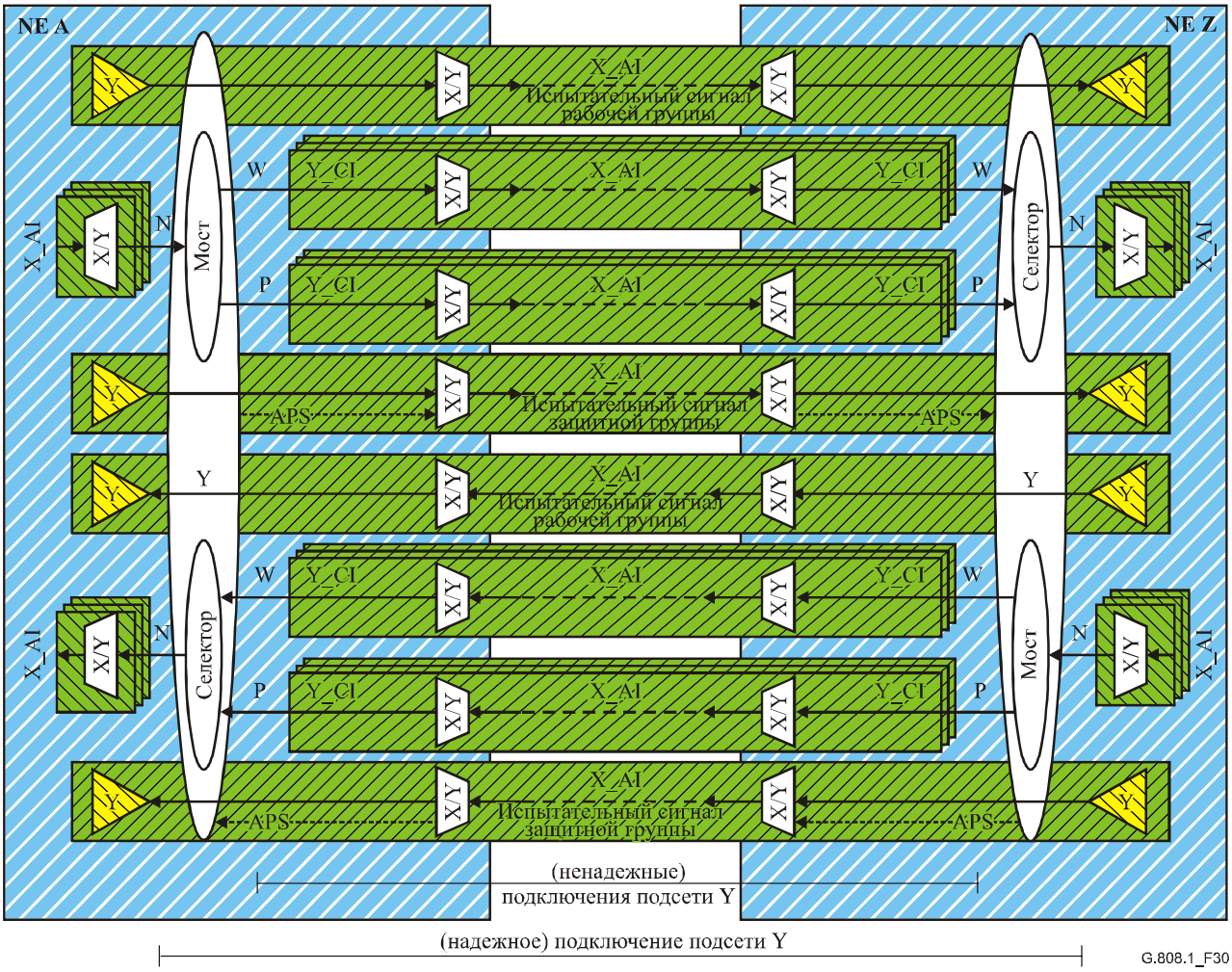
Рисунок 28/G.808.1 – Групповая защита SNC/Te 1:1 или 1+1, использующая завершения канала сетевого уровня



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 29/G.808.1 – Функциональная модель групповой защиты SNC/Ts 1+1/1:1, использующая завершения канала подуровня

ПРИМЕЧАНИЕ. – Для случая ATM испытательный канал (подуровня) должен содержать испытательный сигнал, который имеет активированный контроль непрерывности (CC). Если CC неактивен, то такой испытательный канал (подуровня) не будет транспортировать информации при нормальных условиях отсутствия отказов. При появлении отказа включаются ячейки AIS. Когда отказ сохраняется только в течение короткого периода (например, из-за "защитной операции физического уровня"), детектор появления неисправности AIS в конечной точке испытательного канала (подуровня) обнаружит состояние неисправности AIS в течение 2–3 секунд в соответствии с указанным в I.610 определением состояния AIS. При активированном CC состояние неисправности AIS будет устранено после получения ячейки CC, т. е. в течение 1 секунды после прекращения прерывания трафика.



ПРИМЕЧАНИЕ. – Сигнал APS не применяется для случая однонаправленной коммутации 1+1.

Рисунок 30/G.808.1 – Функциональная модель групповой защиты SNC/Te 1+1/1:1, использующая завершения канала сетевого уровня

12 Живучесть подключений инверсных мультиплексированных линий (SIM).

Существуют методологии транспортирования, поддерживающие инверсное мультиплексирование. Инвесное мультиплексирование может использоваться для транспортирования клиентского сигнала путем распределения полезной нагрузки и передачи фрагментов через ряд индивидуальных какалов в сети. Индивидуальные каналы, содержащие фрагменты, могут рассматриваться в качестве элементов инверсной мультиплексированной группы (IMG).

Схемы инверсного мультиплексирования, которые обеспечивают приспособление к отказам в сети (напр.виртуальное сцепление с LCAS), могут использоваться для обеспечения живучести контроля сигнала P-X во всей сети оператора или нескольких сетях операторов. Это сквозная архитектура живучести, которая может использоваться в различных топологиях, например: ячеистых сетях, кольцевых сетях и т. д. Поскольку это выделенный механизм, то не существует принципиального ограничения количества NE в пределах каналов.

SIM будет работать во всех сочетаниях типов защитных архитектур, коммутации и срабатывания.

SIM в общем случае защищает от отказов на уровне сервера, нарушений связности и ухудшения характеристик на уровне клиента.

SIM защищает адаптированную информацию (AI) (т. е. полную полезную часть индивидуальной характеристической информации сетевого уровня (CI)). См. рисунок 31.

Аккомодация заключается в удалении раздробленной полезной информации, транспортируемой любым элементом IMG, в котором имеет место условие отказа транспортного объекта. Результат – уменьшение объема полезной информации AI.

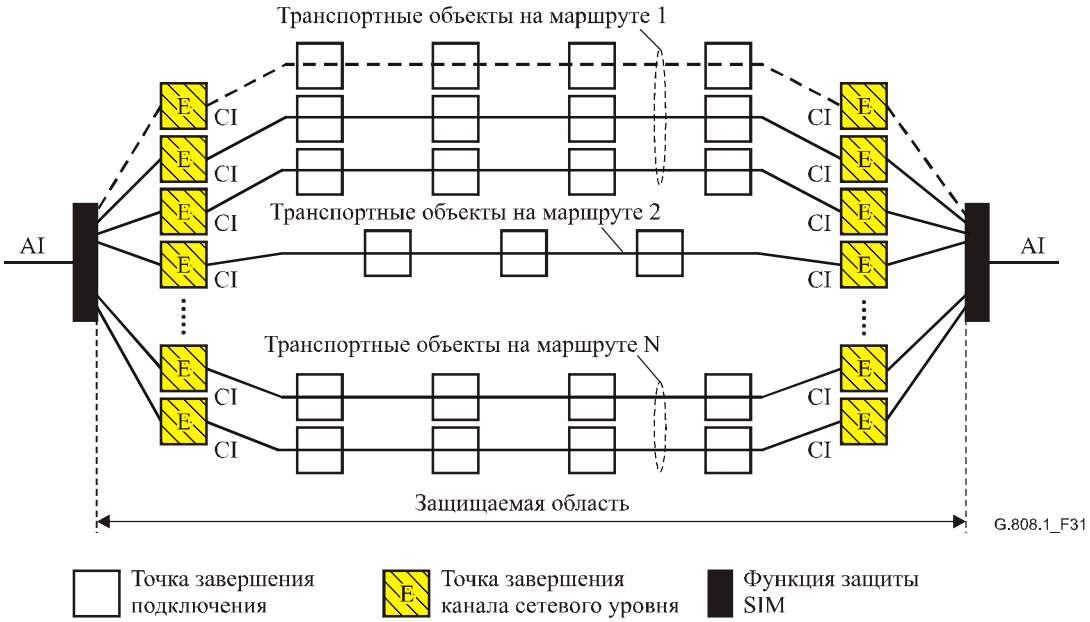


Рисунок 31/G.808.1 – Общая концепция живучести инверсного мультиплексированного канала

AI транспортируется с использованием IMG, содержащей X элементов, распределенных по N маршрутов, где:

- N = число маршрутов ($1 \le N \le X$), каждый из которых содержит одно или несколько сетевых подключений в пределах IMG.
- X = число элементов в IMG, которые требуются для транспортировки AI в полосе пропускания клиента + обеспечения избыточной/защитной пропускной способности Z ($X \ge 1, Z \ge 0$).
- B = общая полоса пропускания элементов X+Z в группе $B = \sum_{i}^{X+Z} B_i$.
- B_{ACT} = фактически транспортируемая полезная информация ($0 \le B_{ACT} \le B$); из-за отказа на одном или нескольких каналах элементов полоса пропускания одного или нескольких элементов IMG не будет использоваться для транспортировки AI.

Схема SIM независима от защиты на уровнях сервера.

12.1 Функциональная модель SIM

На рисунке 32 иллюстрируется случай SIM для транспортировки между NE A и Z. Множество независимых каналов (на уровне сети Y) используются как транспортные объекты для сигнала нормального (полезного) трафика Z_CI. Функции Y_TT завершения канала X генерируют/вводят и контролируют/извлекают сквозную служебную информацию, чтобы определить статус отдельных транспортных объектов. Функции инверсного мультиплексированного адаптирования Y-Xv/Y-X_A генерируют/вводят и контролируют/извлекают сквозную инверсную мультиплексированную служебную информацию, чтобы определить и выровнять состояние элементов X в IMG.

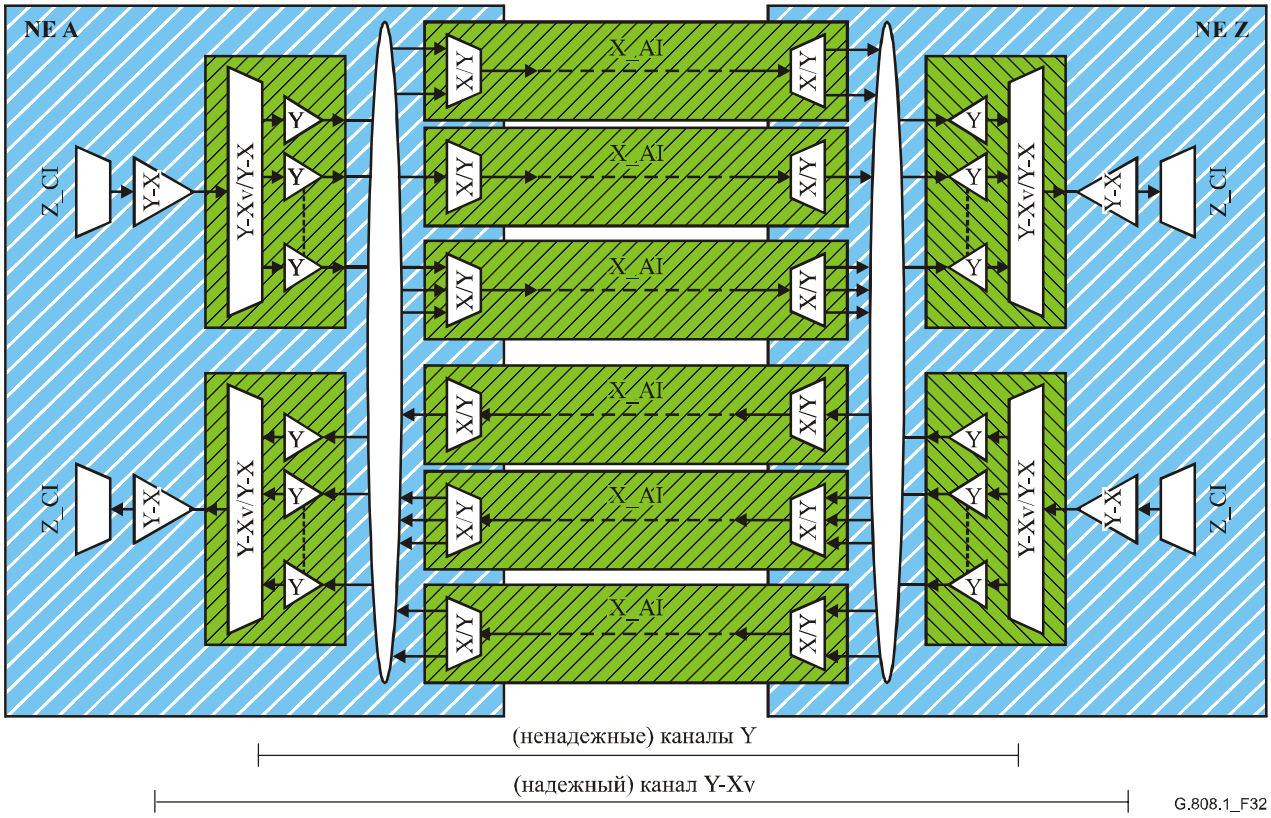


Рисунок 32/G.808.1 – Функциональная модель SIM

Функции инверсного мультиплексированного адаптирования Y-Xv/Y-X_A распределяют/собирают транспортируемую полезную информацию, используя имеющиеся X_{ACT} каналов сетевого уровня Y вне предоставляемых X каналов сетевого уровня Y.

13 Характеристики защитной коммутации

Временная модель защитной коммутации, основанная на Рекомендации МСЭ-Т M.495, иллюстрируется на рисунке 33. Параметры модели определяются следующим образом.

13.1 время обнаружения, T_1: Интервал времени между возникновением неисправности в сети и обнаружением сбоя сигнала (SF) или ухудшения параметров сигнала (SD), которые вызваны этой неисправностью в сети.

13.2 время удержания, T_2: Интервал времени между обнаружением SF или SD и его подтверждением как состояния, требующего процедуры защитной коммутации.

ПРИМЕЧАНИЕ. – В Рекомендации МСЭ-Т M.495 время T_2 определяется как “время ожидания”.

13.3 время срабатывания сигнала защитной коммутации, T_3: Интервал времени между подтверждением SF или SD и завершением обработки и передачи управляющих сигналов, необходимых для выполнения защитной коммутации.

13.4 время передачи защитной коммутации, T_4: Интервал времени между завершением обработки и передачи управляющих сигналов, необходимых для выполнения защитной коммутации, и завершением операций защитной коммутации.

13.5 время восстановления, T_5: Интервал времени между выполнением операций защитной коммутации и полным восстановлением защищаемого трафика.

ПРИМЕЧАНИЕ. – Сюда может входить время, требуемое для выполнения проверки операций коммутации, ресинхронизации цифровой передачи и т. д.

13.6 время подтверждения, T_c: Интервал времени между появлением неисправности в сети и моментом, когда подтверждается, что генерированные сигналы SF или SD требуют операций защитной коммутации: $T_c = T_1 + T_2$.

13.7 время передачи, T_t: Интервал времени между подтверждением того, что сигналы SF и SD требуют операций защитной коммутации, и выполнением операций защитной коммутации: $T_t = T_3 + T_4$.

13.8 время восстановления защищаемого трафика, T_r: Время, прошедшее от появления неисправности в сети до восстановления защищаемого трафика:

$$T_r = T_1 + T_2 + T_3 + T_4 + T_5 = T_c + T_t + T_5.$$

ПРИМЕЧАНИЕ. – Предполагаемая неисправность в сети может обнаруживаться аппаратурой и не подтверждаться после подтверждающих операций. В этом случае учитываются только интервалы времени T_1 и T_2.

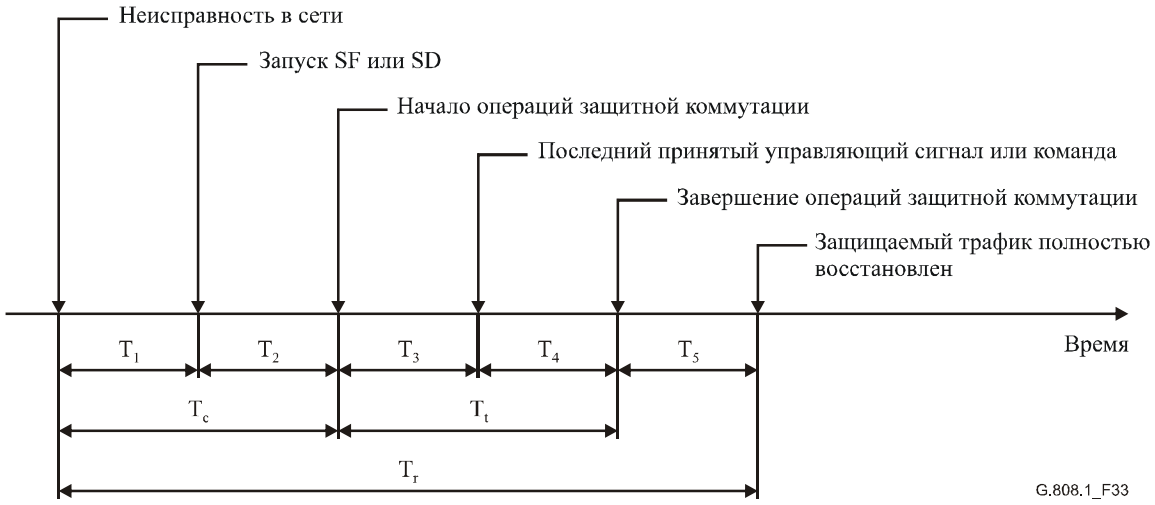


Рисунок 33/G.808.1 – Временная модель защитной коммутации

14 Таймер удержания

Таймеры удержания предназначены для работы в случаях, когда защита сигнала осуществляется с помощью вложенной защиты. Они позволяют внутренней защитной группе восстановить трафик, прежде чем это попытается сделать внешняя защитная группа, чтобы ограничить число операций переключения.

Таймеры удержания применяются также в типах защиты SNC/N и SNC/I 1+1, чтобы предотвратить слишком раннюю коммутацию из-за различия дифференциальной задержки между коротким и длинным маршрутами.

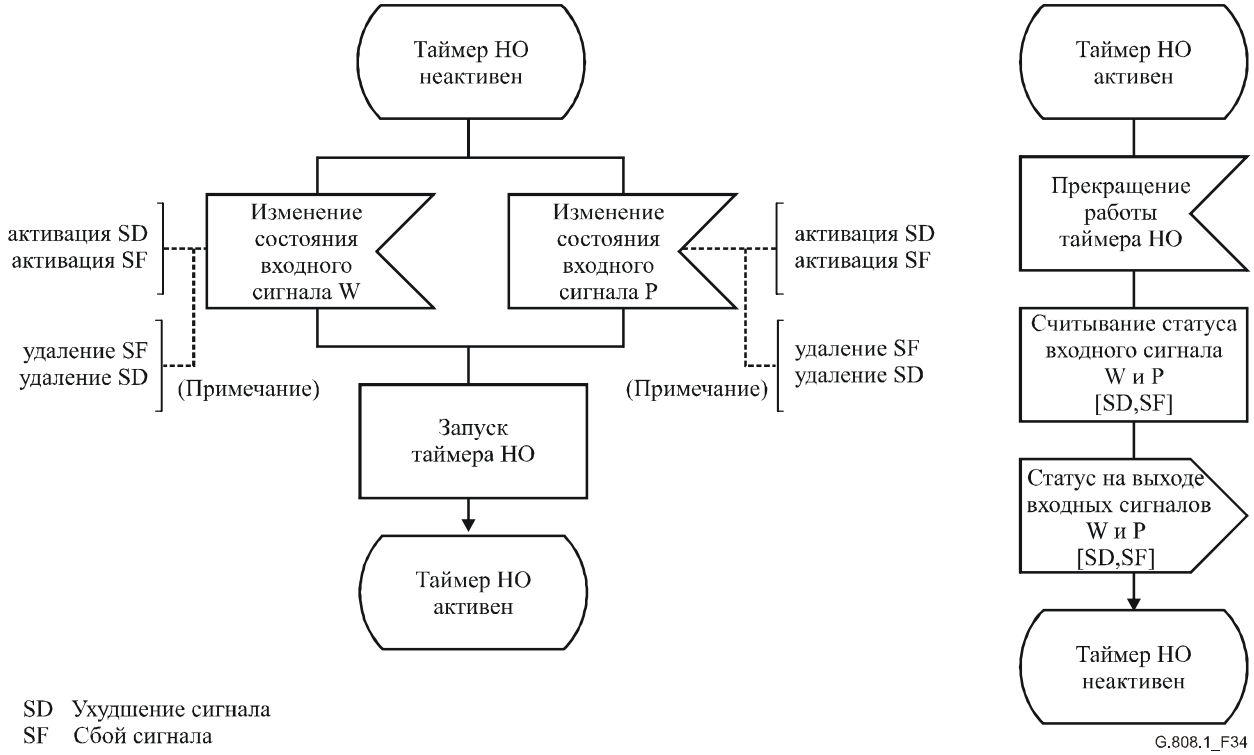
Каждый защитный селектор может иметь один таймер удержания.

Таймер запускается, когда становится активным одно или несколько состояний SF или SD в защитной группе, и работает без сброса в течение периода от 0 до 10 с с шагом X мс. X равен 100 мс (СЦИ, OTN) и 500 мс (ATM).

В течение этого периода измененные статусы SF/SD не пропускаются к процессу защитной коммутации.

Когда период работы таймера истекает, статус SF/SD всех сигналов считывается и пропускается к процессу защитной коммутации. Процесс защитной коммутации будет реагировать на новый статус SF/SD в этой точке.

ПРИМЕЧАНИЕ. – Состояние SF/SD необязательно присутствует на протяжении всего периода удержания, имеет значение только состояние по истечении работы таймера удержания. Далее состояние SF/SD, которое запускает таймер удержания, необязательно является тем же, что и состояние по истечении периода удержания.



SD Ухудшение сигнала
SF Сбой сигнала

ПРИМЕЧАНИЕ. – Использование событий устранения SD/SF для запуска таймера удержания не является обязательным, но рекомендуется с целью предотвращения ненужных защитных коммутаций, которые в противном случае могут происходить при определенных обстоятельствах.

Рисунок 34/G.808.1 – Работа таймера удержания

15 Таймер ожидания восстановления

В реверсивном режиме работы, чтобы предотвратить частое срабатывание защитного переключения из-за повторяющейся неисправности (например, при колебаниях КОБ вокруг порога SD), неисправный рабочий транспортный объект должен перейти в состояние исправности (например, КОБ меньше порога восстановления). После того как неисправный рабочий транспортный объект будет соответствовать этому критерию, должен закончиться установленный период времени, прежде чем сигнал нормального трафика будет использовать его снова. Этот период, называемый периодом ожидания восстановления (WTR), имеет длительность порядка 5–12 минут и должен допускать соответствующую установку. Состояние SF или SD отключает WTR.

В реверсивном режиме работы, когда защита больше не требуется, т. е. неисправный рабочий транспортный объект больше не находится в состоянии SD или SF (считая, что другие запрашивающие транспортные объекты отсутствуют), будет активизировано локальное состояние ожидания восстановления. Так как это состояние приобретает самый высокий приоритет, то оно обозначается сигналом APS (если он применим) и поддерживает сигнал нормального трафика с ранее неисправного рабочего транспортного объекта на защитном транспортном объекте. Это состояние в обычных условиях истекает, и оно становится нулевым сигналом отсутствия запроса (или сигналом отсутствия запроса избыточного трафика, если это применимо). Таймер ожидания восстановления выключается раньше, если это состояние прерывается любым запросом более высокого приоритета.

16 Сигнал автоматической защитной коммутации (APS)

Сигнал APS используется для синхронизации операций на концах A и Z защищаемой области. Сообщаются:

– Тип запроса/состояния;

– Запрашиваемый сигнал;

– Подключаемый через мост сигнал;

– Конфигурация защиты.

В данных о типе запроса/состояния определяется состояние отказа, состояние внешней команды или процесса защиты самого высокого приоритета.

Информация, переносимая сигналом, запрашиваемым и подключаемым через мост, при транспортировке в поле из n битов, определяет:

0 нулевой сигнал;

1.. $2^n - 2$ сигнал нормального трафика, от 1 до $2^n - 2$;

$2^n - 1$ сигнал избыточного трафика.

Информация о конфигурации защиты определяет:

– использование канала APS;

– архитектуру защиты (1+1, 1:n);

– тип коммутации (одно-, двунаправленная);

– тип срабатывания (нереверсивное, реверсивное).

Сигнал APS транспортируется по каналу APS. В принципе можно выделить канал APS на каждом транспортном объекте. Выделение этого канала на одном рабочем транспортном объекте, однако, не обеспечило бы достаточной живучести; т. е. если рабочий транспортный объект выйдет из строя, то связь между двумя конечными точками также нарушится, и защита невозможна. Поэтому канал APS выделяется на одном или нескольких защитных транспортных объектах.

17 Непрерываемый незащищаемый трафик (NUT)

Непрерываемый незащищаемый трафик – это один из трех классов трафика в схемах защиты (1:1) и $(1:1)^n$, остальные – защищаемый трафик и избыточный трафик. NUT не имеет связанной с ним защиты, но не может прерываться в сети, чтобы обеспечить защиту другого трафика.

Избыточный трафик или доступ к защитному каналу позволяют использовать защитные объекты для дополнительного трафика при нормальном функционировании в архитектурах (1:1) или $(1:1)^n$. Когда происходит защитная коммутация, этот трафик прерывается. Избыточный трафик обеспечивает более дешевую услугу, чем защищаемый трафик либо непрерываемый незащищаемый трафик. Он не относится к защищаемому трафику, исходящему от другого заказчика, и может использоваться, например, для обеспечения дополнительной пропускной способности в случае какого-либо значительного события.

18 Избыточный трафик служебных/OAM сигналов (защитного) транспортного объекта

Для случая защиты SNC/S $(1:1)^n$ с избыточным трафиком избыточный трафик (защитного) транспортного объекта не требует добавления завершения канала подуровня. Избыточный трафик (защитного) транспортного объекта имеет выделенный второстепенный временной интервал в пределах совокупного сигнала, отличный от второстепенных временных интервалов защитных транспортных объектов, используемых для переноса сигнала нормального трафика.

Статус избыточного трафика (защитного) транспортного объекта не влияет на функционирование защитной коммутации и как таковой не требует контроля этого транспортного объекта.

19 Внешние команды

Автономное поведение процесса защитной коммутации при состоянии отказа его транспортных объектов можно изменять с помощью внешних (коммутирующих) команд; т. е. внешняя (коммутирующая) команда делает соответствующий внешний запрос процессу защиты.

ПРИМЕЧАНИЕ. – Можно произвести только одну внешнюю (коммутирующую) команду на каждую защитную группу. Внешние команды, которые прерываются или подавляются другими условиями, состояниями или запросами с более высоким приоритетом, отклоняются.

Определены внешние команды, разрешающие следующие типы операций (более точное описание внешних команд см. в пункте 3.3.8, выше):

1) Изменения конфигурации и операций обслуживания, которые следует выполнить в защитной группе или ее транспортных объектах:
   - **блокировка защиты** временно отключает доступ к защитному транспортному объекту для всех сигналов;
   - **принудительное переключение сигнала № i** принудительно производит временную маршрутизацию сигнала № i через защитный транспортный объект;
   - **ручное переключение сигнала № i** производит временную маршрутизацию сигнала № i через защитный транспортный объект, если только условие сбоя (SF, SD) не требует, чтобы через этот транспортный объект направлялся другой сигнал.

2) Блокировка сигналов защитного процесса:
   - **блокировка сигнала № i** временно отключает доступ к защитному транспортному объекту для конкретного сигнала;
   - **отмена блокировки сигнала № i**.

3) Фиксация защитного процесса:
   - **фиксация** временно блокирует выполнение любой коммутирующей операции и поэтому фиксирует текущее состояние. Пока фиксация не отменена, дополнительные внешние команды на ближнем конце отклоняются, а изменения состояния отказа и полученные сообщения APS игнорируются.
   - **отмена фиксации**: Когда команда фиксации отменяется, состояние защитной группы повторно оценивается на основе условий отказа и полученного сообщения APS.

4) Проверка защитного процесса и канала APS между двумя конечными точками:
   - **упражнение:** моделирует запрос на переключение без выполнения фактической коммутирующей операции, если только не используется защитный транспортный объект.

5) Отмена предыдущей внешней (коммутирующей) команды:
   - **отмена:** отменяет все коммутирующие команды.

20 Состояния процесса защитной коммутации

Имеются следующие состояния процесса защитной коммутации:

Невозвращение сигнала нормального трафика № i (DNR #i) – При нереверсивном срабатывании это состояние используется для поддержки выборки сигнала нормального трафика из защитного транспортного объекта.

Отсутствие запроса (NR) – Все сигналы нормального трафика выбираются из своих соответствующих рабочих транспортных объектов. Защитный транспортный объект переносит нулевой сигнал или избыточный трафик, либо служит мостом для одиночного сигнала нормального трафика в защитной группе 1+1.

Ожидание восстановления сигнала нормального трафика № i (WtR) – При реверсивном срабатывании после отмены SF или SD на рабочем транспортном объекте № i поддерживает выборку сигнала нормального трафика № i из защитного транспортного объекта, пока не истечет время таймера ожидания восстановления. Если время таймера истечет до любого другого события или команды, то состояние будет изменено на NR. Оно используется для предотвращения частого срабатывания селектора в случае периодических отказов.

21 Приоритет

Определены относительные приоритеты состояний отказов, внешних команд и состояний защиты по отношению друг к другу. Приоритет применяется к этим условиям/командам/ состояниям локально в каждой конечной точке и между двумя конечными точками.

По поводу этих приоритетов следует обращаться к конкретным Рекомендациям, касающимся защитной коммутации.

22 Условия срабатывания SF и SD

Условием SF является TSF или SSF, что зависит от типа защиты.

На рисунке 35 иллюстрируются правила сочетаний неисправностей. Сигнал SSF задействуется присущими функции адаптации неисправностями и AI_TSF. Сигнал TSF задействуется любой неисправностью канала сети уровня и CI_SSF.

Условие срабатывания SF или непосредственно обнаруживается функцией завершения канала сети защищенного уровня, или проходит через один или несколько уровней согласно правилам сочетаний конкретных неисправностей, CI_SSF и AI_TSF.

Сигнал TSD – единственное условие срабатывания SD. Он выдается при обнаружении dDEG. TSD всегда локален по отношению к функции завершения канала, т. е. он не переходит границ уровня.

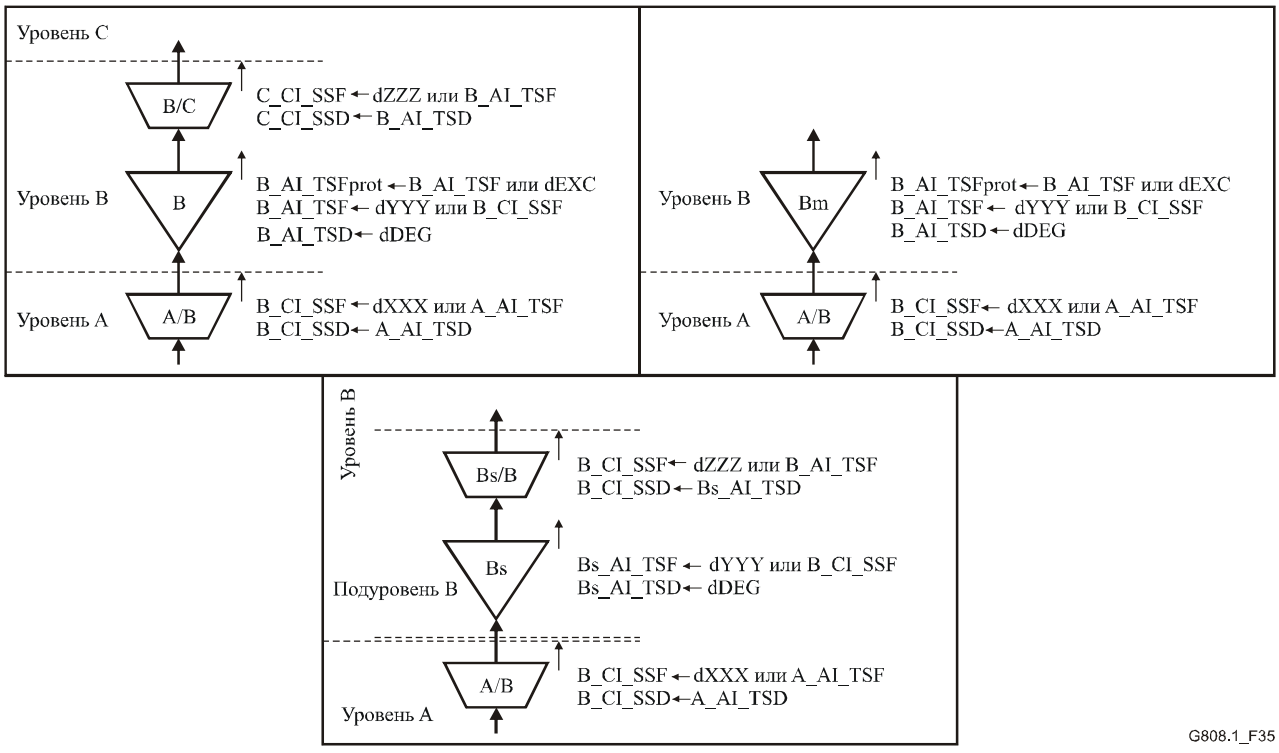


Рисунок 35/G.808.1 – Правила сочетаний неисправностей

22.1 Обзор условий SF

В таблице 2 дается обзор дефектов, которые способствуют формированию условий SF в нескольких технологиях передачи. По поводу конкретных определений SF следует обращаться к Рекомендациям, касающимся аппаратуры (например, Рекомендациям МСЭ-Т G.783, G.798 и I.732).

Таблица 2/G.808.1 – Обзор неисправностей, которые способствуют формированию условия SF

	ATM	OTN	СЦИ
Нарушения непрерывности	LOC	LOS, LOS-P, LCK, LTC	LOS, LTC
Нарушения связности	Нет	TIM, OCI	TIM, UNEQ
Нарушения адаптации	LCD	MSIM, LOM, PLM, LOFLOM	LOF, LOM, LOP, PLM
Нарушения восходящего трафика уровня сервера (Примечание 1)	AIS	FDI, FDI-P	AIS
Канал с чрезмерными ошибками			EXC (Примечание 2)
Нарушения виртуального сцепления (Примечание 3)		LOM, LOA	LOM, LOA
ПРИМЕЧАНИЕ 1. – Любая обнаруженная неисправность вызывает генерирование сигнала AIS/FDI уровня пользователя, который транспортируется в нисходящем потоке. В зависимости от конкретного уровня сигнал AIS/FDI может быть обнаружен в функции адаптации или в функции приема завершения канала. ПРИМЕЧАНИЕ 2. – EXC не вносит вклада в TSF и, следовательно, это только локальное условие срабатывания для сети защищенного уровня (через TSFprot), а не для любого уровня клиента. ПРИМЕЧАНИЕ 3. – Нарушения виртуального сцепления применимы только к LCAS.			

22.2 Обзор условий SD

В таблице 3 дается обзор неисправностей, которые способствуют формированию условий SD в нескольких технологиях передачи. По поводу конкретных определений SD следует обращаться к Рекомендациям, касающимся аппаратуры (например, Рекомендациям МСЭ-Т G.783, G.798).

Таблица 3/G.808.1 – Обзор неисправностей, которые способствуют формированию условий SD

	ATM	OTN	СЦИ
Ухудшения в цифровом сигнале	Нет	DEG	DEG
Ухудшения в оптическом тракте	Не применяется	ffs (Примечание)	Нет
ПРИМЕЧАНИЕ. – Пороги для ухудшений в оптическом тракте будут изучены дополнительно. Вносят ли ухудшения служебного сигнала OTM (OOS) вклад в формирование SD будет изучено дополнительно, поскольку OOS еще не задан.			

23 Выделение рабочего и защитного объектов

Линейная защитная коммутация 1+1 может использоваться как защитное приложение на физическом кольце. Поскольку кольцо часто является частью более обширной сети и только часть канала пересекает кольцо, это приложение обычно используется для транспортных объектов подключения подсети.

Двунаправленный трафик может маршрутизироваться двумя способами:

- Рабочие транспортные объекты для обоих направлений могут применять **различные** физические маршруты, и может использоваться полное кольцо. Этот способ называется однонаправленным кольцом коммутации маршрута (UPSR) и показан на рисунке 36. Этот способ определяется в SONET. В общем случае он может использоваться в архитектурах SNC/I, SNC/N. Он не должен использоваться в архитектурах SNC/S и архитектурах защиты канала.

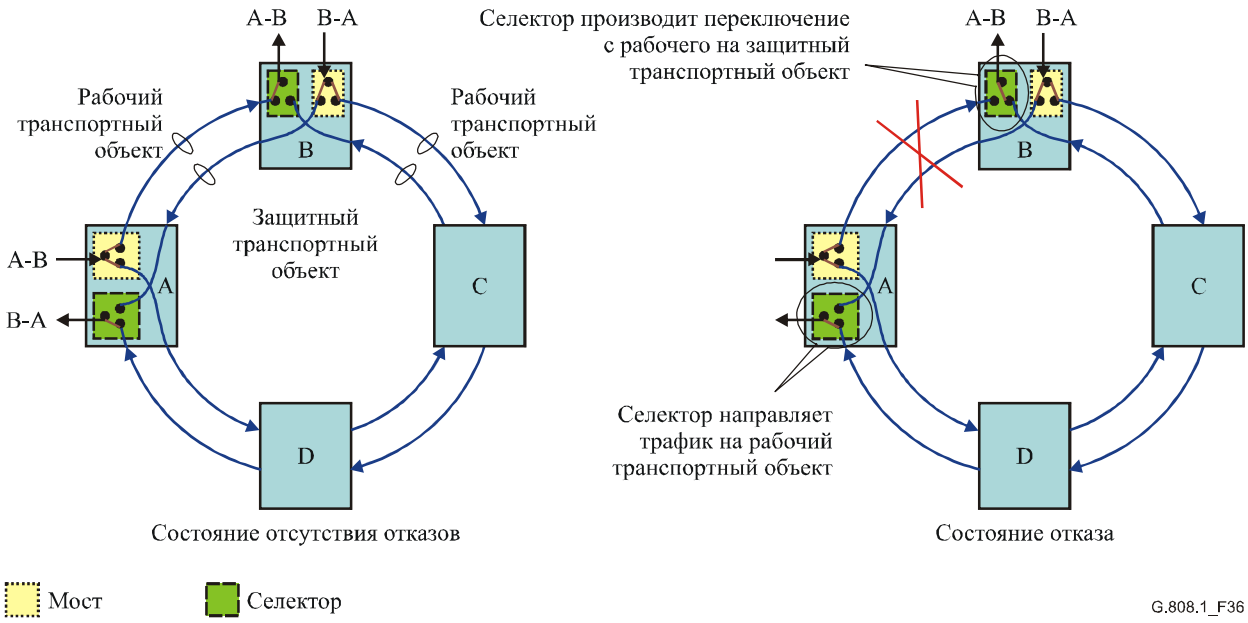


Рисунок 36/G.808.1 – Однонаправленное кольцо коммутации маршрута (UPSR)

- Рабочие транспортные объекты для обоих направлений используют **один** физический маршрут, обычно самый короткий. Защитные транспортные объекты используют другую часть кольца. Это показано на рисунке 37 и называется защитой подключения подсети (SNCP). В ситуации отсутствия отказов это приложение сводит к минимуму задержку передачи и одинаково для обоих направлений. Оно определено в СЦИ, OTN и ATM и может использоваться во всех защитных архитектурах. Однонаправленное кольцо коммутации маршрута может также использоваться подобным образом.

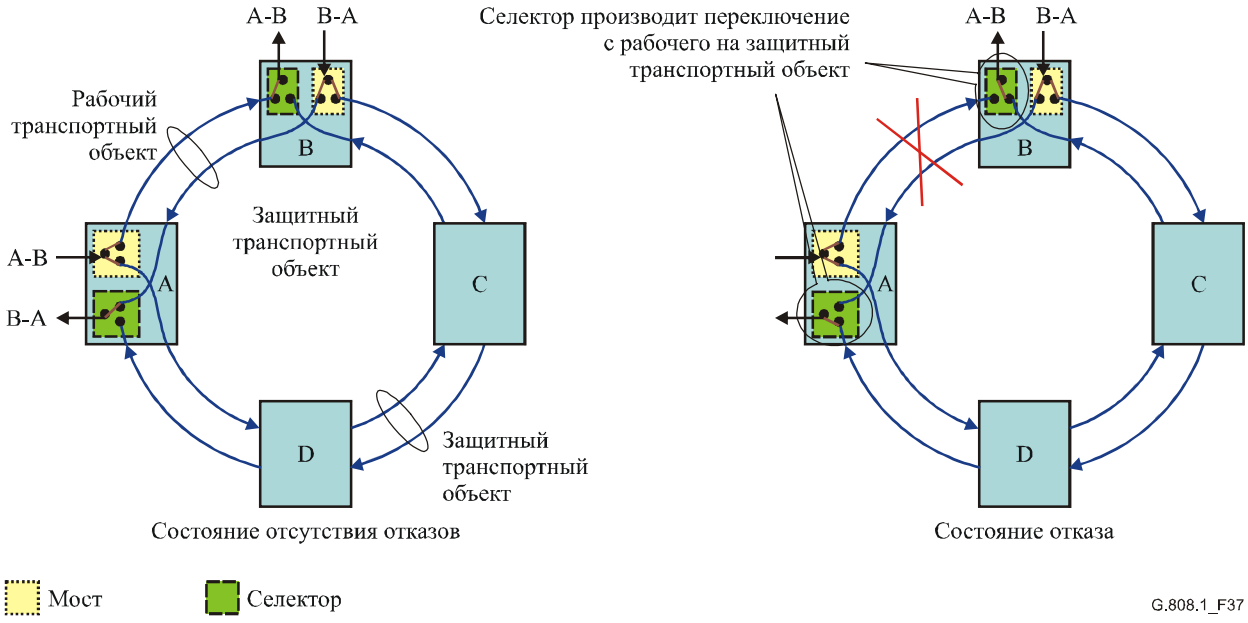


Рисунок 37/G.808.1 – Кольцо защиты подключения подсети (SNCP)

24 Протокол APS

Общие определения типов протоколов APS даются в пункте 3.3.2. В настоящем пункте рассматриваются характеристики поведения протоколов и их применимость к различным типам защитных архитектур, определенных в настоящей Рекомендации. Подробности, относящиеся к схемам кодирования протокола, а также идентификация служебных каналов, используемых для транспортировки протокола, определены в Рекомендациях, касающихся защитной коммутации для конкретных технологий (например, Рекомендациях МСЭ-Т G.841, G.873.1 и I.630).

3-этапный

– для всех типов архитектуры;

– предотвращает неправильное подключение при всех обстоятельствах;

– задействует селектор или мост только после подтверждения приоритета.

2-этапный

– для архитектур 1+1 и $(1:1)^n$;

– более короткое время защитной коммутации.

1-этапный

– для архитектур 1+1 и $(1:1)^n$;

– самое короткое время защитной коммутации;

– задействует селектор/мост до подтверждения приоритета;

– более сложный протокол.

24.1 1-этапный протокол

Средство выравнивания двух концов защищаемой области через обмен единичным сообщением (Z → A).

Может применяться в архитектурах $(1:1)^n$ и 1+1.

Мост/селектор в точке Z срабатывает прежде, чем будет известно, имеет ли условие в Z приоритет над условием в A.

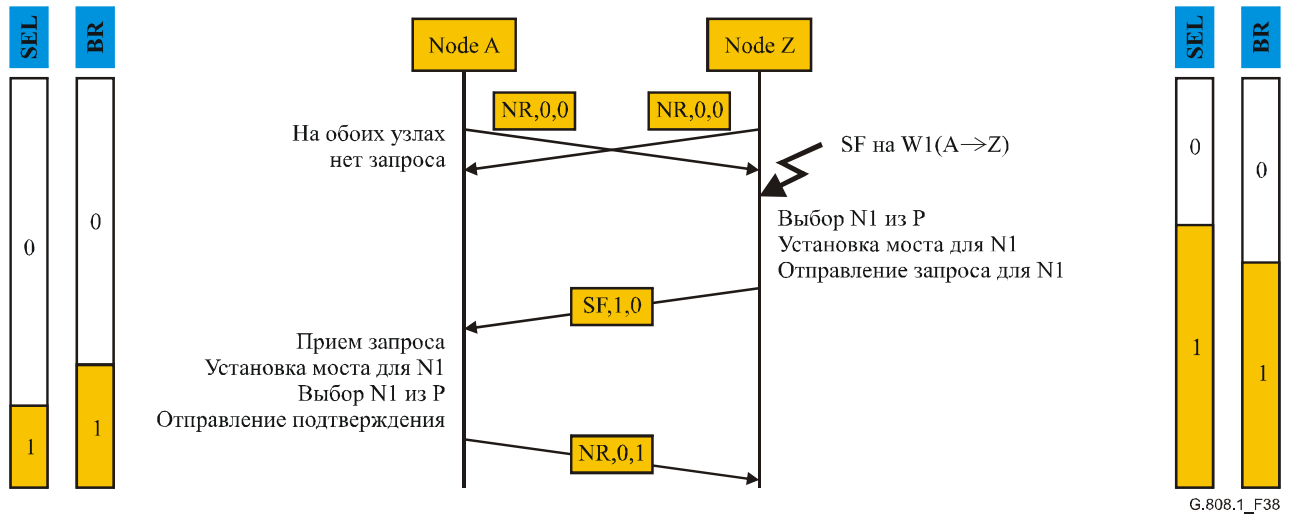


Рисунок 38/G.808.1 – Пример 1-этапного протокола

24.2 2-этапный протокол

Средство выравнивания двух концов защищаемой области через обмен двумя сообщениями (Z → A, A → Z).

Может применяться в архитектуре $(1:1)^n$ и архитектуре 1+1 со своими постоянными мостами.

Для случая архитектуры $(1:1)^n$ Z не выполняет коммутирующих операций, пока A не подтвердит приоритет условия в Z. Когда A подтверждает приоритет, срабатывает селектор и мост. После получения подтверждения в Z срабатывает соответствующий селектор и мост.

В случае архитектуры 1+1 со своими постоянными мостами селекторы срабабывают только так как это описано в случае архитектуры $(1:1)^n$

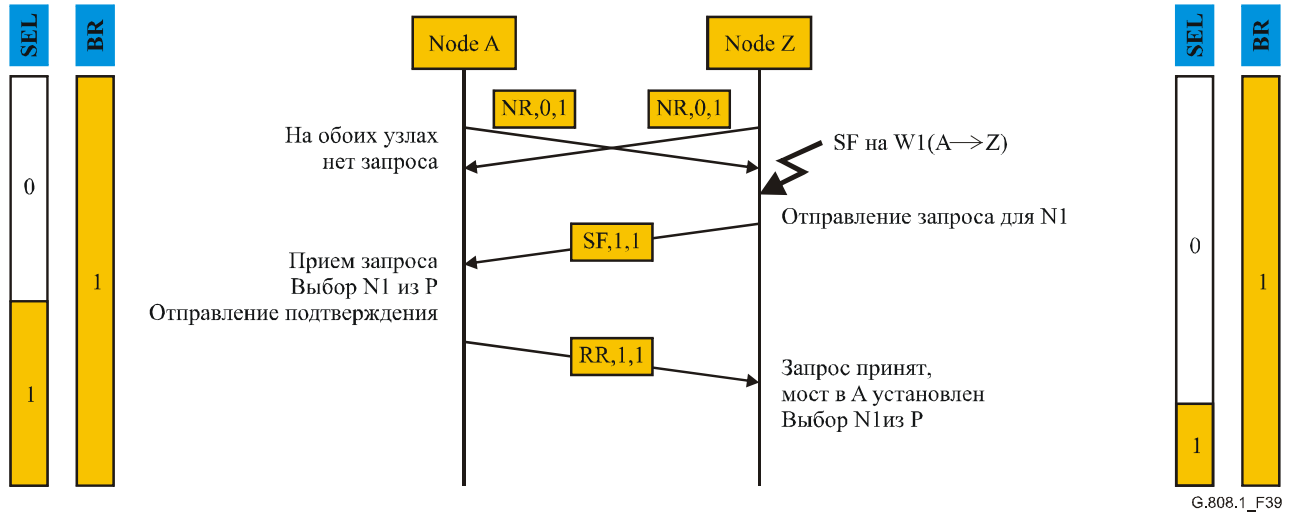


Рисунок 39/G.808.1 – Пример 2-этапного протокола

24.3 3-этапный протокол

Средство выравнивания двух концов защищаемой области через обмен тремя сообщениями (Z → A, A → Z, Z → A).

Может применяться в архитектурах 1:n и m:n и архитектурах 1+1 со своими постоянными мостами.

Для случая архитектур 1:n, m:n Z не выполняет коммутирующих операций, пока A не подтвердит приоритет условия в Z. Когда A подтверждает приоритет, срабатывает селектор. После получения подтверждения в Z срабатывает соответствующий селектор и указывает действие моста на A. В заключение срабатывает селектор в A.

В случае архитектуры 1+1 со своими постоянными мостами селекторы используются только так, как описано для случая 1:n.

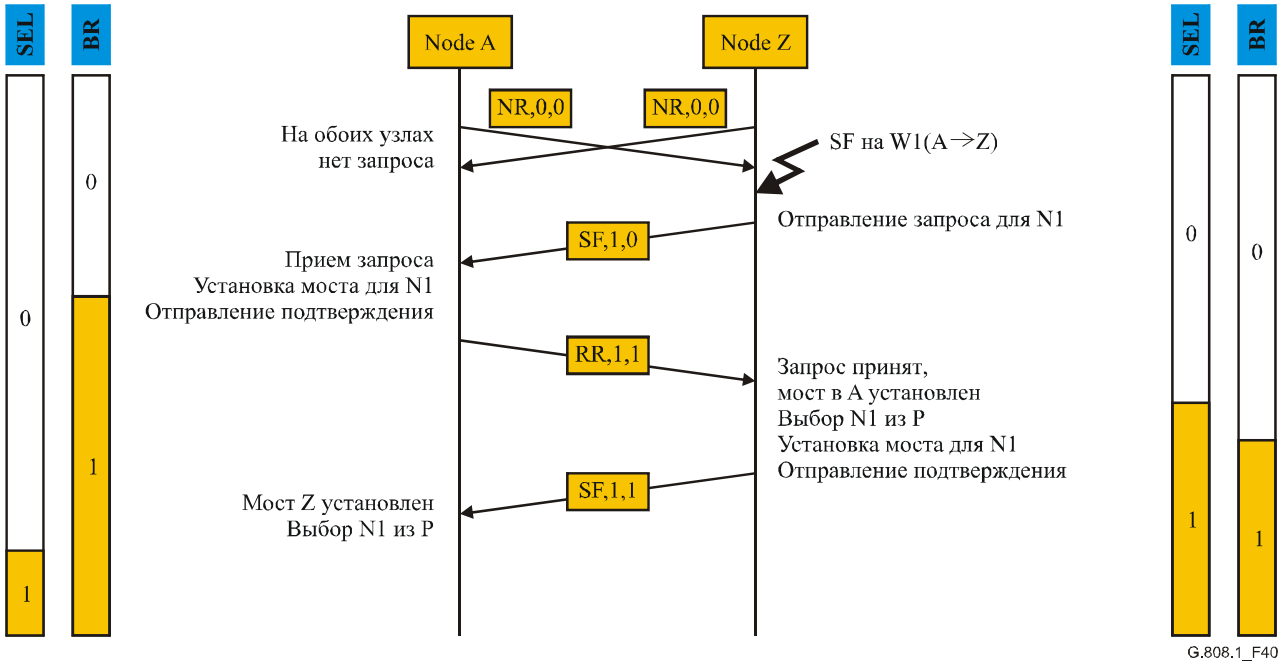


Рисунок 40/G.808.1 – Пример 3-этапного протокола

Добавление I

Реализация таймера удержания

Для реализации функции таймера удержания может использоваться вычитающий счетчик, который срабатывает каждые X миллисекунд. Такая дискретизация вводит ограничение точности при реализации времени удержания. На рисунке I.1 представлены два примера: срабатывание счетчика на понижение каждые 10 мс [25 мс]. Для времени удержания 100 мс в счетчик удержания может быть загружено значение 10 [4] в момент прохождения сигнала SF/SD, со срабатыванием через каждые 10 мс [25 мс] и прекращением работы при достижении значения 0. В этом примере реализуется время удержания 95 ± 5 мс [82,5 ± 12,5 мс].

ПРИМЕЧАНИЕ. – Для случая периода срабатывания на понижение в 100 мс время удержания фактически составляет 50 ± 50 мс; т. е. оно находится между 0 и 100 мс.

Вместо загрузки значения 10 [4] счетчик может загружаться значением 11 [5], которое реализует значения времени удержания 105 ± 5 мс [112,5 ± 12,5 мс].

Точность этого типа таймера удержания составляет 0,5 от периода срабатывания.

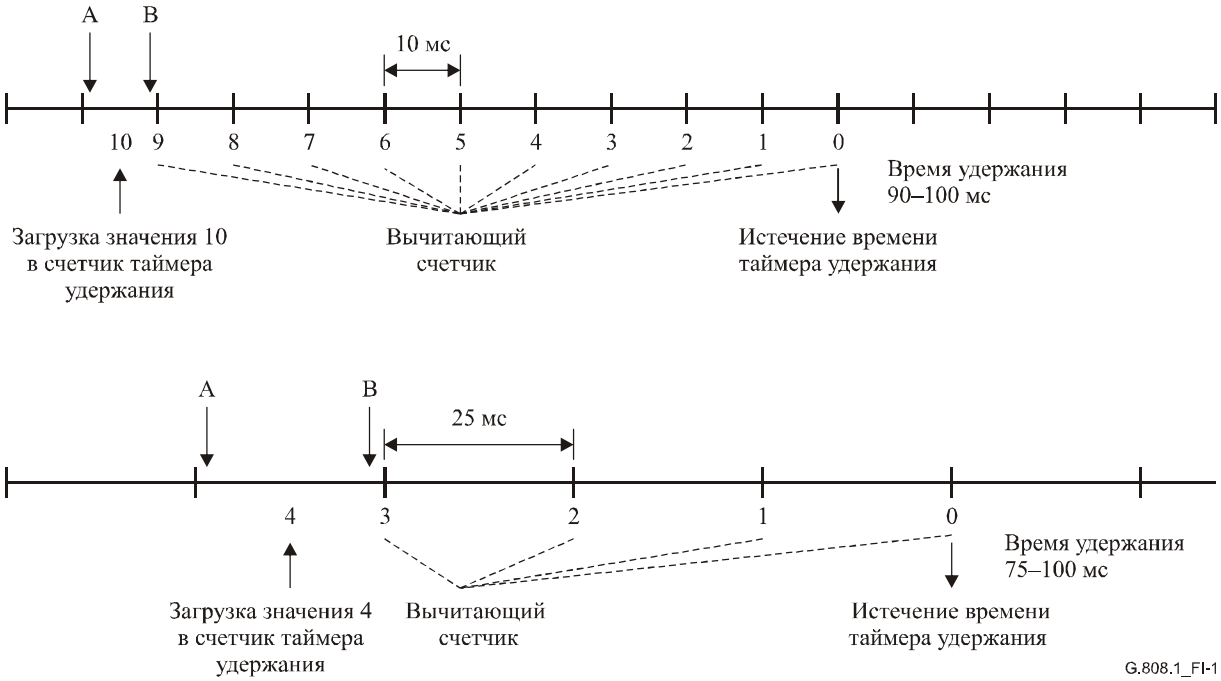


Рисунок I.1/G.808.1 – Точность таймера удержания

При периоде срабатывания в 10 мс влияние различий в задержках передачи между рабочим и защитным транспортными объектами в схемах защиты SNC/I и SNC/N 1+1 можно компенсировать, если выбрано время удержания "0". Когда таймер удержания фактически используется (а не заблокирован) и счетчик загружен значением "2", можно компенсировать различие в задержках, равное 10 мс. См. Рекомендацию МСЭ-Т G.873.1.

Добавление II

Автоматические условия (SF, SD) в защите SNC для группы

В схеме защиты SNC/N [и SNC/I] 1+1 условиями SF и SD для группы являются сигналы SFG и SDG условий SF и SD, которые являются входными сигналами для процесса защиты SNC. Логика, которая вычисляет условия SFG и SDG, работает следующим образом:

- Рабочий SFG = (W-SF1 и не P-SF1), или (W-SF2 и не P-SF2), или и т.д.
- Защитный SFG = (P-SF1 и не W-SF1), или (P-SF2 и не W-SF2), или и т.д.
- Рабочий SDG = (W-SD1 и не P-SD1), или (W-SD2 и не P-SD2), или и т.д.
- Защитный SDG = (P-SD1 и не W-SD1), или (P-SD2 и не W-SD2), или и т.д.

Это определение SFG и SDG позволяет различать сбой, происходящий "перед" или "внутри" защищаемой области. Сбой перед защищаемой областью в одиночном сигнале не будет активизировать ни W-SFG [SDG], ни P-SFG [SDG], тогда как и в W-группе, и в P-группе SF-i будет активизирован; значением элементов "(W-SF-i, и не P-SF-i)" и "(P-SF-i, и не W-SF-i)" будет, однако, "ложь".

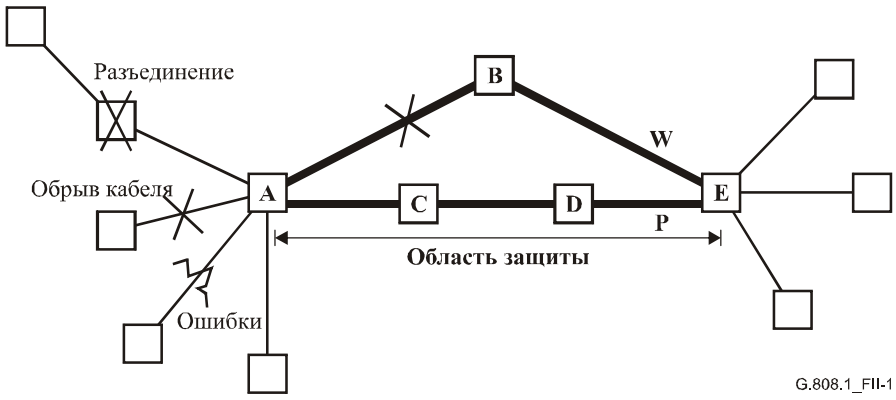


Рисунок II.1/G.808.1 – Пример отказа внутри защищаемой области

Сбой между сетевыми элементами (NE) A и B (рисунок II.1) вызовет активацию W-SFG [или W-SDG]. Если это сбой сигнала сервера, все сигналы в пределах группы войдут в состояние SF. Если это нарушение связности, то в состояние SF перейдет единичный сигнал. Обе ситуации вызовут активацию W-SFG.

Если в то же время, например, происходит разъединение или обрыв кабеля до точки A NE (влияющее на один из сигналов в группе), то будут активироваться W-SF-i и P-SF-i. Когда сбой в области защиты является сбоем сервера, W-SFG будет оставаться активным, а P-SFG – пассивным. В другом случае (нарушение связности в защищаемой области) группа будет переключена, если неисправные сигналы перед областью защиты и внутри нее различны.

ПРИМЕЧАНИЕ. – В особом случае, когда сбой всех сигналов уже произошел перед областью защиты, пассивны W-SFG и P-SFG. Но этот особый случай не нарушает работу процесса защиты; защищать при этом нечего.

Ошибки/сбои внутри защищаемой области, которые вызывают неисправности AIS и DEG, производят это во всех элементах группы в тот же момент (при условии, что требуется, чтобы все сигналы внутри группы *транспортировались в одном сигнале сервера*). По существу, "ORing" отдельных условий SF и SD могут использоваться для срабатывания.

Что касается нарушений, связанных с потерей сигнала (например, потеря непрерывности, необработанный сигнал), или нарушений связности (например, несоответствие идентификатора маршрута), то это поведение группы может не иметь места. Сигналы (в принципе) индивидуально перекрестно подключаются в каждом элементе сети. По существу, ORing отдельных сигналов будет инициировать защитную коммутацию для группы, когда только один (или подмножество) сигналов имеет условие нарушения, связанное с потерей сигнала. Это *следствие снижения сложности*.

Добавление III

Обсуждение вопросов реализации

В технологии СЦИ, повсеместно доступной и используемой в настоящее время, или в другой технологии (например, ATM, OTN), сетевые элементы NE состоят из "блоков порта" (PU) и "блоков коммутации". Блоки коммутации выполняют перекрестное подключение/коммутацию, блоки порта выполняют всю необходимую обработку служебных сигналов СЦИ [PDH] (и OAM ATM).

Для VC-12 СЦИ, перекрестно соединяющего сетевые элементы (NE), блок порта будет выполнять обработку указателя SOH, AU4, а также указателя VC-4 POH и TU12 (рисунок III.1). Затем результирующие сигналы VC-12 СЦИ передаются на блок коммутации для маршрутизации на соответствующие выходные блоки порта.

Можно использовать тот же блок порта, когда сигнал VC-4 СЦИ должен не прекращаться, а проходить как сигнал VC-4.

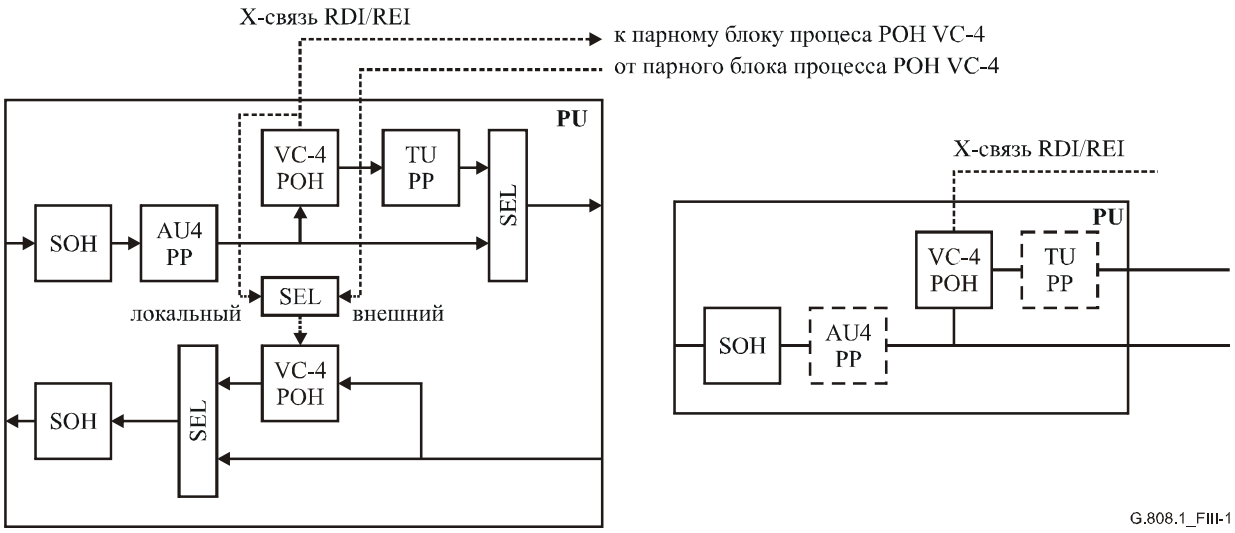


Рисунок III.1/G.808.1 – Подробная (слева) и упрощенная (справа) схемы блока порта (только основные функции)

III.1 Анализ

Рассмотрим в качестве примера случай защиты MS 1+1 (рисунок III.2). Для этой цели используются два блока порта, оба с аппаратными средствами, выполняющими обработку SOH, AU PP, VC-4 POH и TU PP, в то время как защитная коммутация реализуется в блоке коммутации путем переключения всей группы сигналов LOVC.

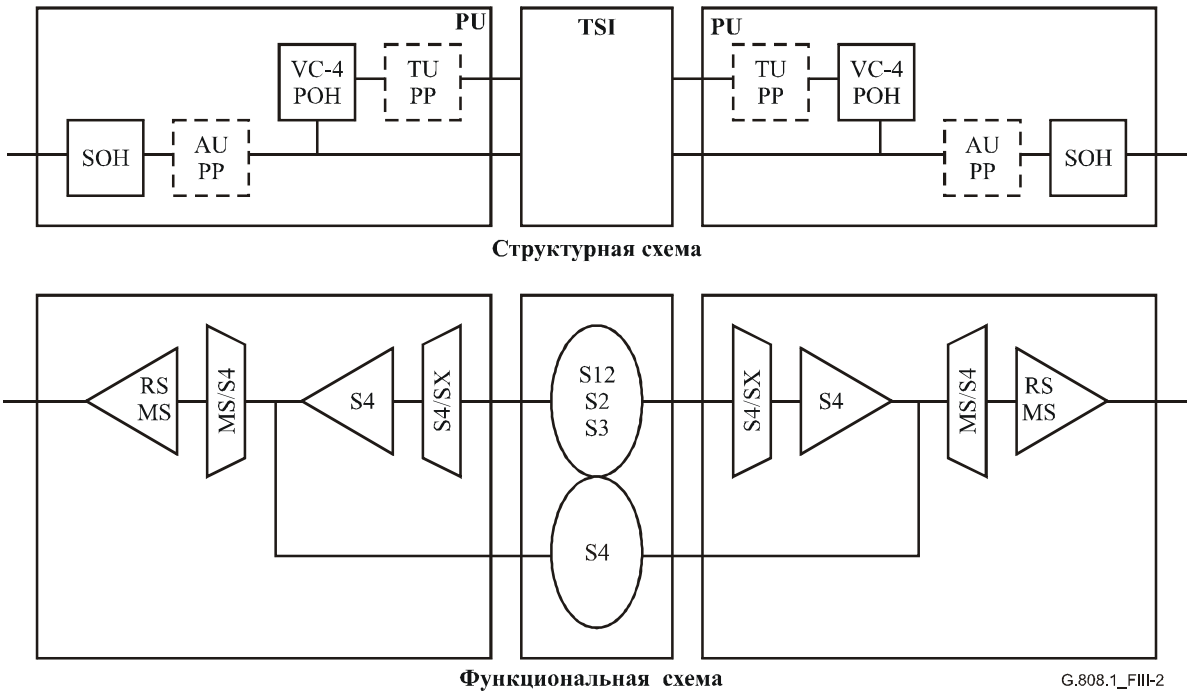
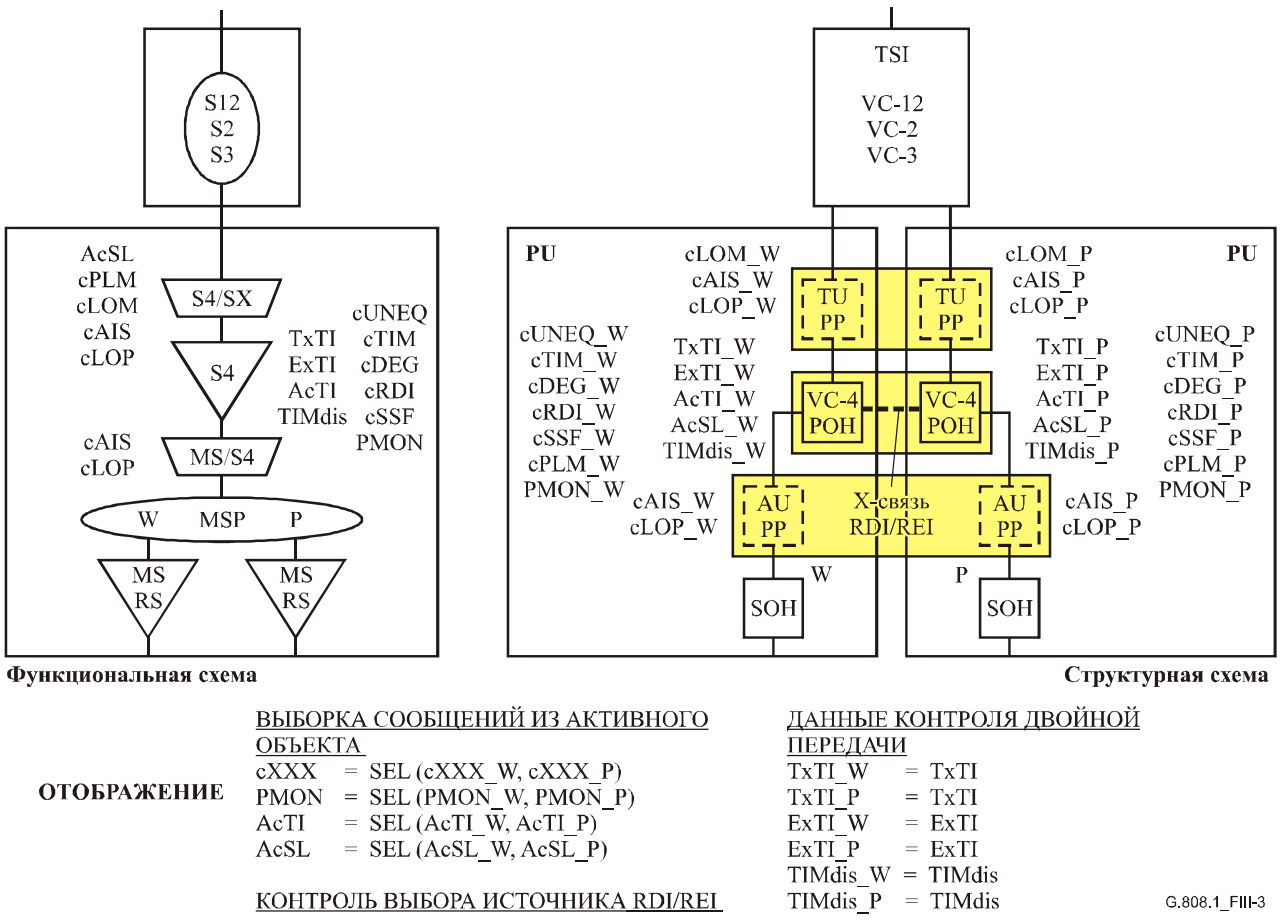


Рисунок III.2/G.808.1 – Отображение структурной схемы в функциональной: основная операция

Согласно функциональной модели, налицо чрезмерный объем функциональных возможностей (рисунок III.3); т. е. обработка SOH, как ожидается, будет производиться дважды, тогда как обработка AU PP, VC-4 POH и TU PP должна выполняться только один раз.



ОТОБРАЖЕНИЕ

ВЫБОРКА СООБЩЕНИЙ ИЗ АКТИВНОГО ОБЪЕКТА

cXXX = SEL (cXXX_W, cXXX_P)
PMON = SEL (PMON_W, PMON_P)
AcTI = SEL (AcTI_W, AcTI_P)
AcSL = SEL (AcSL_W, AcSL_P)

КОНТРОЛЬ ВЫБОРА ИСТОЧНИКА RDI/REI

ДАННЫЕ КОНТРОЛЯ ДВОЙНОЙ ПЕРЕДАЧИ

TxTI_W = TxTI
TxTI_P = TxTI
ExTI_W = ExTI
ExTI_P = ExTI
TIMdis_W = TIMdis
TIMdis_P = TIMdis

G.808.1_FIII-3

Рисунок III.3/G.808.1 – Отображение структурной схемы в функциональной: защита MS

За счет программного обеспечения сетевой элемент NE может предоставлять ожидаемые функциональные возможности; он скрывает резервные процессы AU PP, VC-4 POH и TU PP от администратора.

Для интерфейсов передачи также требуется маскировка; на двух интерфейсах STM-N ожидается вывод одного и того же сигнала (сигналов) AU4, VC-4 и TU.

В наиболее простой реализации будут выводиться "различные" AU и TU. Различие связано с фактическим значением указателя; они не должны быть одинаковыми в рабочем и защитном сигналах STM-N.

Тот факт, что значения указателя AU/TU могут быть различными, не оказывает влияния на работу сети; т. е. это "несоблюдение", в строгом смысле, не имеет последствий, следовательно, для этого не требуется компенсации.

Вместе с тем при обработке POH VC-4 ситуация иная. Здесь нужно удостовериться в том, что сигналы RDI и REI, которые выводятся через оба интерфейса STM-N, идентичны; т. е. процесс контроля POH VC-4 в активном блоке порта STM-N должен отправить свои сигналы RI_RDI/RI_REI на процессы генерации POH VC-4 на обоих блоках порта (рабочем и защитном).

Аналогичным образом, это требуется, когда защита SNC VC-4 выбрана вместо защиты MS (рисунок III.4).

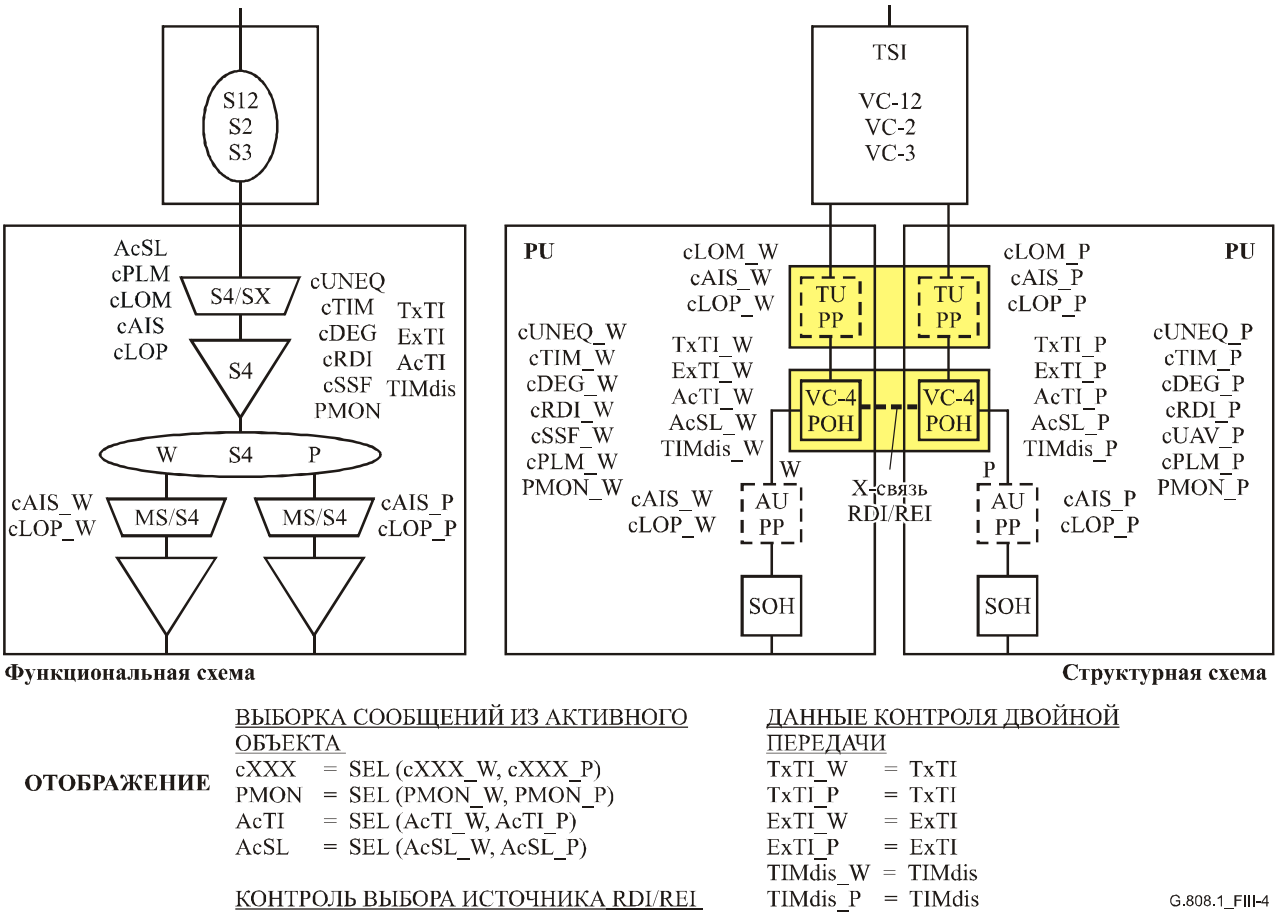


Рисунок III.4/G.808.1 – Отображение структурной схемы в функциональной: защита SNC/I VC-4

В случае, когда X-связь RDI/REI не реализована, не будет возможности добавить контроль эффективности по Рекомендации МСЭ-Т G.826 в сетях, в которых работают вышеупомянутые схемы защиты. Рекомендация МСЭ-Т G.826 требует поддержки двунаправленного (базирующегося на услугах) контроля качества. Для этого требуется, чтобы использовалась информация отдаленного конца. Эта информация отдаленного конца должна представлять ошибки/неисправности, обнаруженные на маршруте сигнала, по которому фактически транспортируется информация клиента.

При однонаправленной коммутации на каждом конце участка защиты независимо производится выбор между рабочим и защитным каналом/SNC. Если в направлении A → Z выбирается рабочее подключение SNC VC-4, а в направлении Z → A – защитное подключение SNC VC-4, то информация отдаленного конца, извлекаемая на каждом конце, передается генератором POH VC-4 на резервный блок порта; т. е. это сигнал, который не выбирается на этом конце. Если при этом (в данный момент) используются свои местные сигналы RI_RDI/RI_REI (вместо сопровождающих сигналов RI_RDI/RI_REI), то отдаленный конец будет принимать информацию, которая не относится к фактически выбранному VC-4.

Регистрируемые данные двунаправленного контроля характеристик (в этом случае) представляют неправильную информацию; т. е. ими нельзя пользоваться.

Конечно, та же самая проблема существует и для регистрируемых данных однонаправленного контроля (базирующегося на обслуживании) на отдаленном конце.

В случае NE для маршрутизации на скорости 64 кбит/с с интерфейсами STM-N та же проблема будет иметь место на уровне VC-12.

ПРИМЕЧАНИЕ. – На рисунках III.3 и III.4 проблема представлена только применительно к RDI/REI. Эти рисунки не показывают завершение тандемного подключения/сегмента или функции ненарушающего контроля, которые требуются для управления защитной коммутацией.

Добавление IV

Пример защиты (1:1)^n

В настоящем Добавлении дается пример защитной коммутации (1:1)n (для n = 3) в сети ATM. В этом случае имеются три рабочих объекта, маршрутизация которых выполнена различным образом. Они защищены одним защитным объектом, который, при нормальном функционировании, транспортирует избыточный трафик. Защитный объект должен иметь достаточную полосу пропускания, чтобы транспортировать наибольший из трех сигналов нормального трафика или сигнал избыточного трафика. Каждый из рабочих объектов является виртуальным маршрутом ATM, чей размер и виртуальный идентификатор маршрута (VPI) показаны на рисунке IV.1.

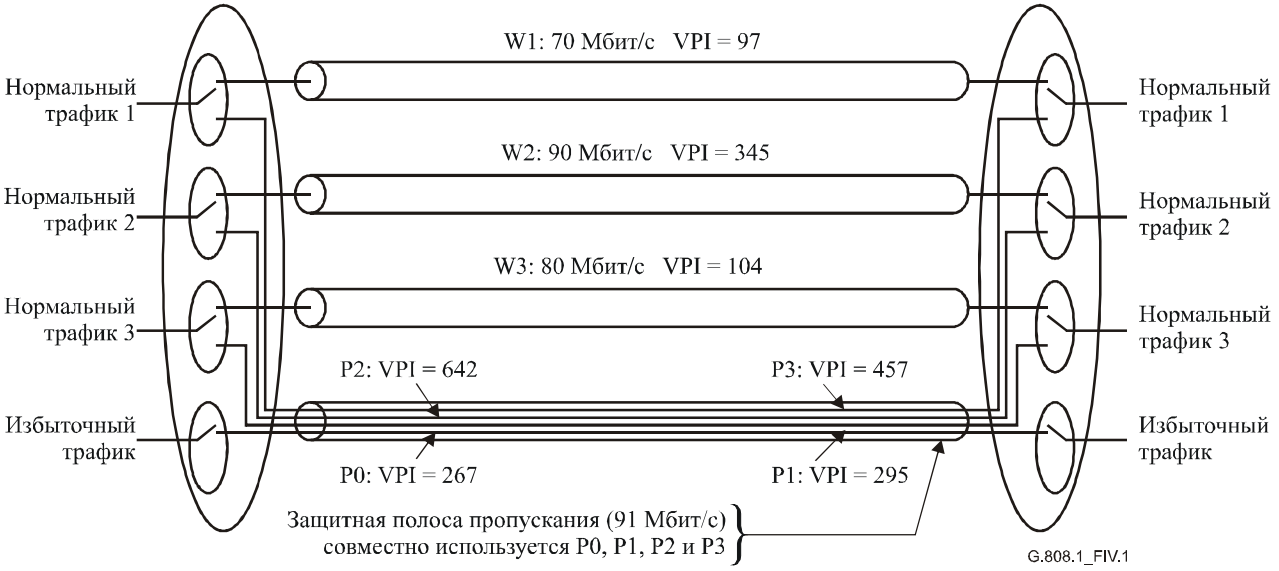


Рисунок IV.1/G.808.1 – Пример защиты (1:1)^n

В этом примере требуется скорость 90 Мбит/с плюс ячейки OAM для P0 (включает OAM VP-APS), P1, P2 и P3, чтобы обеспечить защитную коммутацию. Для однонаправленной коммутации может использоваться 1-этапный протокол, поскольку, когда условие отказа обнаруживается, все, что необходимо, – это чтобы сигнал передавался от конца Z к A для инициализации переключения в мосте. Неправильного подключения не может происходить, так как сигнал, который находится в защитном объекте, однозначно идентифицируется своим VPI.

Добавление V

Примеры живучести инверсных мультиплексированных каналов

V.1 Живучесть, обеспечиваемая LCAS

Используя способность инверсного мультиплексированя VCAT + LCAS где Y = Y-Xv и Z = Y-Xc, а IMG эквивалентна VCG, приводится следующий пример.

AI транспортируется с использованием виртуальной группы сцепления (VCG) X элементами (VC_n_Xv, ODUk_Xv), распределенными по N маршрутов, где:

- Все элементы, принадлежащие к VCG, имеют одинаковую полосу пропускания.
- Полоса пропускания VCG пропорциональна количеству активных элементов.
- N = число маршрутов ($1 \leq N \leq X$), каждый из которых содержит одно или несколько сетевых подключений в пределах VCG.
- X = число элементов в VCG, которые требуются для транспортировки AI в полосе пропускания клиента + обеспечения избыточной/защитной пропускной способности Z ($X \geq 1$, $Z \geq 0$).
- X_{ACT} = фактически транспортируемая полезная информация ($0 \leq X_{ACT} \leq X$); из-за отказа на одном или нескольких каналах полоса пропускания одного или нескольких элементов VCG не будет использоваться для транспортировки AI.

Для транспортировки сигнала 10 Мбит/с требуется VC-12-5v. В этой VCG установлены пять индивидуальных каналов VC-12, маршрутизация двух из них выполнена по маршруту 1 и трех VC-12 – по маршруту 2 (рисунок V.1). В этом случае полоса пропускания, обеспечивающая живучесть, составляет 2 × VC-12, или 40%, а полоса пропускания, не обеспечивающая живучесть, – 3 × VC-12, или 60%. Если бы был добавлен один дополнительный VC-12 (E=1) и маршрутизирован через маршрут 1, то полоса пропускания, обеспечивающая живучесть, составила бы 3 × VC-12, или 60%, а незащищаемая полоса пропускания – 2 × VC-12, или 40%.

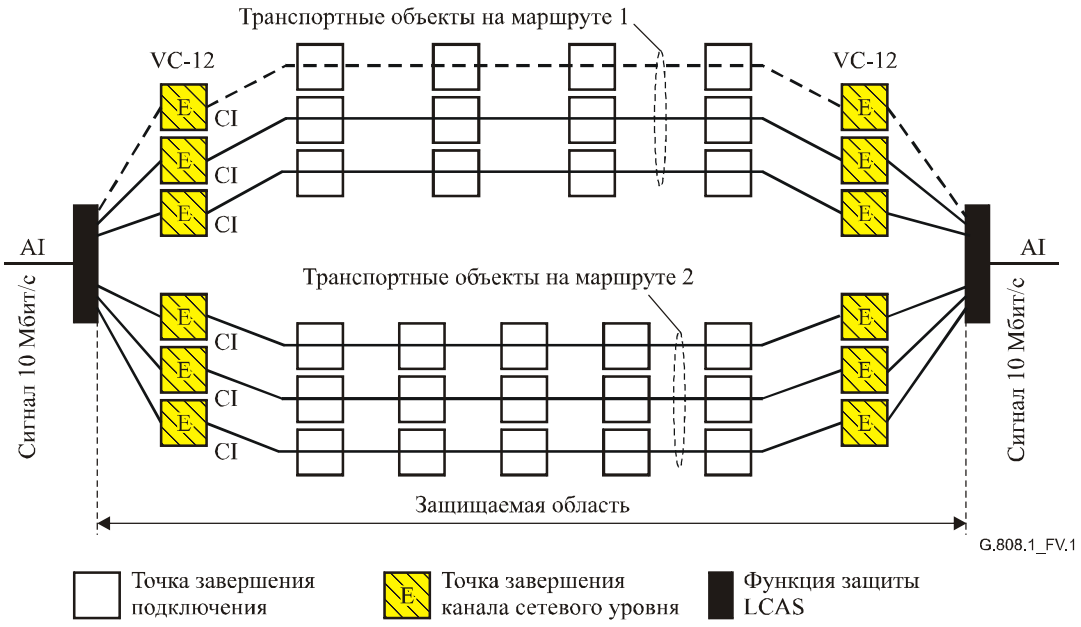


Рисунок V.1/G.808.1 – Пример живучести LCAS для передачи сигнала 10 Мбит/с через VC-12-(X+E)v (X=5, E=0,1)

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	**Системы и среда передачи, цифровые системы и сети**
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2007 г.